Band 15 / 2015

Vernetzte Unsicherheit – Hybride Bedrohungen im 21. Jahrhundert

Anton Dengg und Michael Schurian (Hrsg.)

Schriftenreihe der
Landesverteidigungsakademie

www.bundesheer.at

SCHUTZ und HILFE

Schriftenreihe der
Landesverteidigungsakademie

Anton Dengg und Michael Schurian (Hrsg.)

Vernetzte Unsicherheit – Hybride Bedrohungen im 21. Jahrhundert

15/2015
Wien, Juli 2015

Impressum:

Medieninhaber, Herausgeber, Hersteller:
Republik Österreich / Bundesministerium für Landesverteidigung und Sport
Rossauer Lände 1
1090 Wien

Redaktion:
Landesverteidigungsakademie
Institut für Friedenssicherung und Konfliktmanagement
Stiftgasse 2a
1070 Wien

Schriftenreihe der Landesverteidigungsakademie

Juli 2015
ISBN 978-3-902944-71-9

Druck:
HDruckZ-ASt Stift 4574/15
Stiftgasse 2a
1070 Wien

Besonderer Dank gebührt allen Mitwirkenden, die zur Erstellung dieser Publikation beigetragen haben.

„In allen Schlachten zu kämpfen und zu siegen,
ist nicht die größte Leistung.
Sondern sie besteht darin, den Widerstand des Feindes
ohne einen Kampf zu brechen."

Sun Tsu

Inhaltsverzeichnis

Vorwort

Die militärische, aber letztlich gewaltlose Einnahme der Halbinsel Krim durch russische Spezialverbände hat ein neuartiges Bedrohungsphänomen aufgezeigt, das in dieser Ausprägung zwar theoretisch denkbar war, aber als politisch nicht realisierbar erschien. Dabei sind es weniger die einzelnen Komponenten der „Operation Krim", sondern deren spezifische Komposition unter Missachtung völkerrechtlicher Bestimmungen und besonderer Abstützung auf alte und neue Massenmedien. Der damit entfachte Propagandakrieg, der bis heute anhält, macht es Beteiligten wie Beobachtern schwer, sich einen klaren Überblick über die tatsächlichen Geschehnisse, über Ursachen und Wirkung der Ereignisse zu verschaffen.

Viele Experten sehen das Vorgehen Russlands gegenüber der Ukraine als Bestätigung für die These von einer hybriden Kriegführung, die neben direktem und indirektem Militäreinsatz auch viele andere Maßnahmen (inklusive Cyber-War) vorsieht, um auf einen Gegner einzuwirken und ihn zur Aufgabe zu zwingen. Auch diese Idee scheint nicht neu zu sein, denn schon der chinesische Kriegstheoretiker Sun Tsu hat einen „Sieg ohne Kampf" als die beste Strategie eingestuft. All das greift aber in der heutigen Zeit mit den zur Verfügung stehenden Mitteln und Möglichkeiten zu kurz, um die Bandbreite von Risiken, Gefahren und Bedrohungen in vollem Umfang zu erfassen. Die dabei zu Tage tretenden Erscheinungsformen stellen gewissermaßen eine neue Form der „Enthegung" des Krieges dar, da sowohl die Angreifer als auch deren Absicht und die tatsächliche Zielsetzung im Dunkeln bleiben können. Humanitäres Völkerrecht und andere internationale Regelungen greifen nicht oder werden negiert, das wahre Ausmaß einer „Attacke mit modernen Mitteln" auf einen Staat und dessen Funktionsfähigkeit können erst sehr spät und abrupt erkennbar werden.

Anton Dengg und die Mitautoren dieses Bandes haben sich im Rahmen eines Projektes mit der Thematik einer hybriden Machtprojektion intensiv auseinandergesetzt. Sie gehen dabei über die enge, doch eher militärisch dominierte Vorstellung von hybrider Kriegführung hinaus und stellen ein Konzept vor, das die gesamte Bandbreite eines möglichen Bedrohungsspektrums zu erfassen trachtet. Dabei leisten sie auch Pionierarbeit im Terminologiebereich, indem sie die wesentlichen, relevanten Phänomene definieren und darauf hinweisen, dass nicht jeder Hackerangriff staatsbe-

drohlich ist, sondern eine von jedem Staat festzulegende strategische Schwelle überschritten werden muss.

Aus den Beiträgen und Länderstudien ist ersichtlich, dass zwar ein gewisses Bewusstsein zur Problematik hybrider Bedrohungen vorhanden ist, die Vorstellungen und Lösungsansätze auf nationaler Ebene aber eher diffus oder eindimensional erscheinen. Die Intention der vorliegenden Arbeit ist daher, einen Beitrag zu Bewusstseinsbildung, Problemerfassung und hinsichtlich möglicher Schutz- und Gegenmaßnahmen auf strategischer Ebene zu leisten. Besonders hilfreich kann dabei die von Anton Dengg und Michael Schurian entworfene Graphik sein, in der die Spektren des Bedrohungspotentials dargestellt werden. Diese ist aber wohl auch als Denkanstoß für weiterführende Überlegungen zu verstehen.

Walter Feichtinger
Leiter IFK

Kurzfassung

Gesellschaften vernetzen sich in nahezu allen Lebensbereichen in einem immer höheren Ausmaß; nicht zuletzt gefördert von technologischen Entwicklungen. Neben positiven treten dabei auch negative Effekte auf – Systeme werden verletzungsanfälliger. Dadurch verändert sich auch das Bedrohungsbild und es wird von einer zunehmenden Zahl an Einflussfaktoren geprägt. In aktuellen Konflikten, wie z.B. dem Ukrainekonflikt, zeigt sich diese Palette an unterschiedlichen Faktoren deutlich.

In internationalen Publikationen[1] werden unterschiedliche staatliche Handlungsoptionen bei gegenwärtigen Kampfhandlungen thematisiert. Dabei spricht man von hybrider Kriegsführung (Hybrid Warfare).

Dieses Buch verfolgt einen wesentlich breiteren Ansatz und beschreibt die über Kampfhandlungen hinaus anwendbaren staatlichen Möglichkeiten zur Machtprojektion. Als Beispiel dient der derzeitige Ukrainekonflikt, der nicht nur mit konventionellen – nämlich militärischen – Mitteln, sondern auch mit einer Fülle von unterschiedlichen Machtinstrumenten geführt wird. Infolge dieser Vielzahl staatlicher Machtprojektionsoptionen zur Beeinflussung der Handlungsfähigkeit anderer Staaten ergeben sich bestimmte Bedrohungsfelder. Technologische Errungenschaften und deren offensive Einsatzmöglichkeiten verstärken die Optionen von Staaten, hybride Mittel einzusetzen. Das „Worst Case" Szenario für den Zielstaat ist ein Vorgehen gegen ihn auf mehreren Ebenen.

Wie, wann und durch wen Macht in Form von Soft- und Hard Power gegenwärtig und zukünftig projiziert werden kann, steht im Fokus dieser Publikation. Es werden sicherheitspolitische Dokumente von zwei Referenzstaaten auf deren Sensibilisierung gegenüber hybriden Bedrohungen untersucht.

Einen wesentlichen Teil dieser Arbeit stellt das Aufzeigen von Handlungsoptionen zur Bewältigung von hybriden Bedrohungen dar.

---

[1] Z.B. Frank G. Hoffman: Hybrid Warfare and Challenges. In: JFQ, issue 52, 1st quarter 2009. <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-52.pdf>, abgerufen am 22.06.2015.

Beispiele aus gegenwärtigen Spannungs- und Konfliktregionen untermauern schließlich die theoretischen Ausführungen zur Thematik „hybride Bedrohungen“. Die Abbildungen dienen zur Veranschaulichung komplexer Zusammenhänge.

Abstract

Societies grow more and more connected in all spheres of life; not least due to the technologic achievements. Apart from positive, also negative effects appear – systems become prone to failure. Thereby also the image of threats changes and is influenced by a growing number of factors. In current conflicts, for example the Ukraine, this spectre of different factors becomes apparent.

In international publications[1] different governmental options of choice in contemporary combat operations are dealt with. The notion of Hybrid Warfare has been coined.

This book, however, takes a much broader approach and describes potentially applicable possibilities of a state to exert power beyond mere combat operations. As an example the current Ukraine-conflict is well at hand because it is not thought with conventional – military – means, but rather with a variety of different instruments of power projection. From this variety of options to exert influence over another state's capability to take decisions, different images of threats result. Technologic achievements and their offensive possibilities amplify the options of states to apply hybrid methods. The "worst case scenario" for the target state is a hostile advancement on different layers.

How, when and by whom either soft or hard power is projected in the present or the future lies at the core of this publication. Security policies of two reference states are examined with regards to their view on hybrid threats.

An integral part of this book is the highlighting of options of choice to deal with hybrid threats.

Examples taken from current tension- and conflict-regions eventually underpin the theoretic remarks on „hybrid threats". Images visualise complex linkages.

---

[1] See, e.g. Frank G. Hoffman: Hybrid Warfare and Challenges. In: JFQ, issue 52, 1st quarter 2009. <http://ndupress.ndu.edu.g/Portals/68/Documents/jfq/jfq-52.pdf>, accessed on 22.06.2015.

1 Einleitung und Theorie

1.1 Überlegungen zum Begriff „Strategische Bedrohung“

Thomas Pankratz

Der Begriff der „strategischen Bedrohung“ ist zweifelsohne einer der zentralen Begriffe in der strategischen wie auch sicherheitspolitischen Diskussion. Umso bemerkenswerter ist es daher, dass sich in einschlägigen Lexika oder Handbüchern, im Gegensatz zu „Bedrohung“, keine Begriffsfassungen finden lassen. Im Folgenden werden nun einige Überlegungen angestellt, diesen Begriff zu umreißen. Ausgangspunkt ist das Phänomen Bedrohung, die Orientierung der Argumentation erfolgt anschließend über die zentralen Elemente der Strategie, insbesondere über die strategischen Ziele des Staates. Dieser Ansatz impliziert, dass sich die Argumentation nicht über die Bedrohungen an sich, sondern über die Perspektive des bedrohten Akteurs begründet. Diese Überlegungen sind nicht abschließend zu sehen, sondern sollen vielmehr Gedankenanstöße zur Reflexion über einen oft verwendeten, jedoch kaum näher hinterfragten Begriff geben.

Zentrales Element im strategischen Denken[1] ist, neben der Formulierung von Zielen und den Mitteln[2], mit denen diese Ziele erreicht werden sollen, die Analyse der sogenannten strategisch relevanten Umwelt.[3] In dieser sind die Ziele, aber auch mögliche Ressourcen und Wege ebenso verortet, wie andere Akteure und deren Ziele und Mittel. Somit inkludiert die strategisch relevante Umwelt nicht nur Herausforderungen, sondern auch potentielle Bedrohungen. Im Endeffekt geht es im strategischen Denken darum, sich in dieser strategisch relevanten Umwelt zu positionieren und diese zu beeinflussen.

Bedrohungen können auf zwei grundlegende Weisen dargestellt werden. Zum einen, indem bestimmte Phänomene als Bedrohungen benannt werden, wie dies z.B. in der Europäischen Sicherheitsstrategie von 2003 oder in der Österreichi-

---

1 Als Strategisches Denken kann die zielgerichtete und erfolgsorientierte Kalkulation im Sinne von Abwägen der Elemente Ziele, Mittel und Umwelt verstanden werden.

2 Mittel umfassen in diesem Ansatz sowohl Wege als auch Ressourcen (Instrumente).

3 Strategisch relevante Umwelt bezeichnet hier den aus der Verdichtung entstandenen Ausschnitt aus der Gesamtumwelt, den der jeweilige Akteur für relevant hält.

schen Sicherheitsstrategie von 2013 geschieht. Bei diesem Ansatz erfolgt zumeist keine explizite Erläuterung, warum diese Phänomene eine Bedrohung darstellen. Die Explikation wird als bekannt vorausgesetzt bzw. erfolgt implizit. Zum anderen, indem danach gefragt wird, wie und wodurch sich etwas als Bedrohung manifestiert. Auf diesen Punkt wird im Folgenden näher eingegangen.

Grundsätzlich kann als Bedrohung die Gefährdung der Sicherheit[4] eines Akteurs[5] durch einen anderen Akteur verstanden werden.[6] Etwas näher ausdifferenziert, sind hierbei in idealtypischer Weise mehrere Dimensionen denkbar:

- Wahrnehmung einer Gefährdung bei gleichzeitigem Vorhandensein einer tatsächlichen Gefährdung;
- Wahrnehmung einer Gefährdung ohne Vorhandensein einer tatsächlichen Gefährdung;
- Keine Wahrnehmung einer Gefährdung bei Vorhandensein einer Gefährdung.

Inwieweit andere Akteure[7] nun tatsächlich eine Gefahr für einen anderen Akteur darstellen, hängt von verschiedenen Faktoren ab, die sich in drei Dimensionen widerspiegeln: Eine Dimension ist die Fähigkeit bzw. das Potential (die Potentiale) eines Akteurs, einen anderen tatsächlich gefährden zu können. Die zweite Dimension ist die Absicht (Intention), dies auch zu tun. Hieraus kann abgeleitet werden, dass wenn eine dieser Dimensionen Null ist, von einem Akteur für einen anderen[8] keine objektive Bedrohung ausgeht bzw. ausgehen kann.[9] Eine

---

4 Sicherheit wird hier alle Gesellschafts- und Politikbereiche umfassend verstanden.

5 Individuum, Gruppe, Gesellschaft, Staat, Staatengemeinschaft.

6 Diese Gefährdung kann ausgehen von einem anderen Akteur oder einem Phänomen wie etwa der Umwelt. Hier wird auf Bedrohungen, die von Akteuren ausgehen, eingegangen.

7 Es können dies ein Akteur oder mehrere Akteure sein. Zum Teil können diese benannt werden, d.h. es ist bekannt, um wen es sich handelt; zum Teil können diese jedoch nicht konkret benannt werden.

8 Dies bezieht sich nur auf diese Interaktion. Für andere Akteure kann hingegen sehr wohl eine Gefährdung ausgehen.

9 So kann z.B. Staat A Staat B mit der „nuklearen Auslöschung“ drohen, d.h. er verfügt über die Intention dies zu tun bzw. gibt diese Intention vor, wenn jedoch seine Fähigkeiten hierzu nicht in der Lage sind, ist für Staat B in der gegebenen Situation keine

dritte Dimension der Gefährdung eines Akteurs durch einen anderen kann darin gesehen werden, dass letzterer über bestimmte Potentiale verfügt, um den ersteren gefährden zu können, nicht aber über die entsprechende bewusste Absicht, sich jedoch ein von ihm gesetztes Verhalten auf indirekte, nicht beabsichtigte Weise gefährdend auf den ersten Akteur auswirkt.[10]

Hinsichtlich des potentiell bedrohten Akteurs sind ähnliche Überlegungen anzustellen. Hierbei sind für diesen nicht nur die Potentiale und Absichten anderer Akteure an sich wichtig, sondern vor allem die Fähigkeit, diese zu erkennen und auch in entsprechender Weise zu deuten. Bei dieser Interpretation spielen eine Reihe von zum Teil bewussten, zum Teil auch unbewussten Faktoren[11] eine Rolle, die sich unter dem Begriff „Strategische Kultur" zusammenfassen lassen. Dies bedeutet, dass die Wahrnehmung, d.h. die Analyse des strategisch relevanten Umfelds, als subjektiver konstruktivistischer Akt zu sehen ist. Dies führt dazu, dass die Interpretation der Umwelt nicht als statisches Moment zu sehen ist, sondern sich für den jeweiligen Akteur, bedingt durch innere und äußere Einflüsse, ändern kann und auch wird, sodass Bedrohungen zu unterschiedlichen Zeitpunkten unterschiedlich interpretiert werden. Diese Unterschiede in der Interpretation führen weiteres dazu, dass unterschiedliche Akteure diese Umwelt verschieden interpretieren und in weiterer Folge das Verhalten anderer Akteure in unterschiedlicher Weise als bedrohlich interpretieren. Die strategische Kultur bestimmt jedoch nicht nur die Interpretation der Umwelt, sondern auch, ob, wie und inwieweit der Akteur auf diese reagieren kann bzw. will. Dies ist jedoch nicht nur eine Frage der Mittel bzw. des Könnens und Wollens der Bereitstellung derselben, sondern auch eine Frage der Formulierung von Zielen.

Als Zwischenergebnis kann nunmehr festgehalten werden, dass eine Bedrohungssituation mindestens zwei Akteure voraussetzt, wovon sich zumindest einer durch die Absichten und Potentiale eines anderen Akteurs in seiner Sicherheit bedroht fühlt oder auch tatsächlich bedroht wird. Die empfundene

---

Gefährdung vorhanden. Umgekehrt kann beispielsweise ein mit anderen Staaten alliierter Staat über die Potentiale verfügen, jeden dieser Staaten anzugreifen, wenn jedoch, bedingt durch die Allianz, keine Absicht vorhanden ist, ergibt sich wiederum, dass für die alliierten Staaten keine Gefährdung vorhanden ist.

10 So beispielsweise durch sein Verhalten gegenüber Dritten, durch einen Unfall udgl.

11 Z.B. historische Erfahrungen, geo(politische) Faktoren, Einstellungen und Haltungen der politischen Elite sowie der Bevölkerung, Besonderheiten des politischen Systems.

Bedrohung kann, muss aber nicht mit der Realität übereinstimmen. Gleiches gilt auch umgekehrt. Eine vorhandene Bedrohung, kann, muss aber nicht vom Akteur als solche empfunden bzw. als solche erkannt werden.

Von diesen Überlegungen ist nun darauf überzuleiten, was als „strategische Bedrohung" verstanden werden kann. Dies ist im engen Zusammenhang mit den strategischen Zielen eines Akteurs, in unserem Fall des Staates, zu sehen.

Grundsätzlich können zwei Dimensionen strategischer Ziele des Staates herausgefiltert werden, die in Macht- und in Gestaltungsziele unterteilt werden können. Beide hängen eng zusammen, wobei jedoch Machtziele in zeitlicher Konsequenz Gestaltungszielen vorgeordnet sind. Machtziele beziehen sich auf die eigene Positionierung im Systemumfeld, d.h. insbesondere die Positionierung gegenüber anderen Akteuren sowie auf die Fähigkeiten und Kapazitäten der Durchsetzbarkeit der eigenen Interessen gegenüber anderen. Gestaltungsziele sind Ideen, wie und auf welche Weise die Umwelt zum eigenen Nutzen strukturiert werden kann und soll. Diese implizieren somit auch die Interessen und Werte des jeweiligen Akteurs. Transponiert man nun diese Überlegungen auf den Staat, so kann folgendes abgeleitet werden:

- Grundvoraussetzung zur Positionierung gegenüber anderen Akteuren ist die Existenz des Staates. Als oberstes strategisches Machtziel ist somit der Fortbestand des Staates (Existenz an sich) zu verstehen, wobei „Staat" hier primär dem völkerrechtlichen Ansatz folgend als sich aus den drei Elementen Staatsvolk, Staatsgebiet sowie Staatsgewalt zusammensetzendes Objekt verstanden wird.
- Damit in engen Zusammenhang stehend, ist die Wahrung der Souveränität nach außen und auch nach innen zu verstehen, die somit unter die Dimension Gestaltungsziele zu subsumieren ist. Diese Souveränität kann als Handlungsvollmacht bzw. Deutungshoheit über die Ausgestaltung des eigenen gesellschaftspolitischen Systems und der dahinterstehenden Werte verstanden werden. Während erstere Dimension unabhängig vom gesellschaftspolitischen System des Staates zu sehen ist, ist diese zweite Dimension zwar abhängig von dieser ersten Dimension, aber variabel. Dies kann z.B. bedeuten, dass für westlich orientierte Staaten der demokratisch verfasste, liberale pluralistische Rechtsstaat,

der sich an den Grundbedürfnissen und Grundrechten des Einzelnen orientiert, im Mittelpunkt der zu schützenden politischen Werte[12] steht, für diktatorisch ausgerichtete Systeme hingegen der absolute Machterhalt der politischen Elite oder/und die unbedingte Durchsetzung der eigenen Ideologie.

Abgeleitet von den Ausführungen zum Begriff Bedrohung, kann nun festgestellt werden, dass strategische Bedrohungen jene Bedrohungen sind, die entweder die Existenz des staatlichen Systems bedrohen oder/und in Opposition zur Hoheit über die Ausgestaltung des gesellschaftspolitischen Systems stehen.

Diese Überlegungen mögen auf den ersten Blick klar erscheinen. Differenziert man diese Überlegungen etwas näher aus, ergeben sich jedoch mehrere diskussionswürdige Punkte. So kann beispielsweise argumentiert werden, dass mögliche Bedrohungen, die sich gegen die drei zentralen Elemente des Staates richten, grundsätzlich als strategische Bedrohungen zu verstehen sind. Es kann jedoch auch argumentiert werden, dass ein bestimmter Umfang einer Bedrohung gegenüber einem oder allen Elementen vorliegen muss, um die Existenz des Staates als solches zu gefährden; d.h. nur beim Überschreiten einer bestimmten Schwelle wäre von einer strategischen Bedrohung zu sprechen. Es scheint jedoch schwierig, dieses Ausmaß sowohl qualitativ als auch quantitativ benennen zu können.[13] Letztlich wird es an der politischen Führung liegen, dieses Ausmaß zu beurteilen aber auch zu bewerten. Hierbei wird nicht nur die Fähigkeit der Elite zur Beurteilung und Bewertung entscheidend sein, sondern auch deren Bereitschaft, d.h. das Wollen, dies zu tun.

Ähnliches gilt für die zweite Dimension, diejenige der Deutungs- und Gestaltungshoheit. Auch hier könnten wiederum alle Bedrohungen, die in Opposition zu den eigenen Werten, Interessen und letztlich Zielen stehen, als strategische Bedrohungen verstanden werden. Es kann aber auch wie oben argumentiert werden, dass eine bestimmte Schwelle einer Bedrohung gegeben sein muss, um

---

[12] Zu den gesellschaftspolitische Ziele Österreichs siehe beispielsweise Bundeskanzleramt Österreich, Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten. Wien 2013, S. 9.

[13] Ausgenommen beispielsweise dem Fall, dass ein Staat von einem anderen Akteur besetzt wird, die Bevölkerung durch nichtkonventionelle Systeme als Gesamtes bedroht oder die Staatsgewalt ausgeschalten wird.

von strategischer Bedrohung sprechen zu können. Ein essentieller Punkt hierbei ist, dass es zunächst notwendig ist, diese Werte und Ziele entsprechend zu formulieren und auch als „hochrangige Staatsziele" zu benennen. Auch hier liegt es wieder an den politischen Entscheidungsträgern, dies zu beurteilen und zu bewerten. Entscheidend, und im Gegensatz zu diktatorisch ausgerichteten Systemen, ist in westlichen Systemen, dass diese Beurteilung und Bewertung von zumindest einem Großteil der politisch Verantwortlichen (und somit auch der Opposition), insbesondere aber auch Bevölkerung mitgetragen wird.[14]

Zusammengefasst kann festgestellt werden, dass nicht jede potentielle Bedrohung von sich aus eine strategische Bedrohung darstellt und dass es nicht „die" strategische Bedrohung gibt. Es kann jedoch generell gefolgert werden, dass unter „strategischen Bedrohungen" solche Bedrohungen zu verstehen sind, die die Existenz des Staates gefährden. Da dieses strategische Ziel des Staates einigermaßen klar festmachbar ist, ist die Bedrohung desselben augenscheinlicher, unmittelbarer und auch nachvollziehbarer. Dennoch gibt es hier Interpretationsspielraum. Interpretationsspielraum ist auch bei Bedrohungen gegeben, welche die gesellschaftspolitischen Ziele, die von Werten und Interessen abgeleitet werden, gefährden, und somit als strategische Bedrohungen bezeichnet werden können. Bei dieser Dimension scheint, da Werte und Interessen und somit auch deren Bedrohungen mittelbarer sind, der Interpretationsspielraum jedoch größer.

Letztlich trägt die politische Elite die Verantwortung. Verantwortung dafür, dass sie die strategischen Ziele des Staates formuliert. Dies soll und muss in demokratisch orientierten Systemen zum Wohle der Bevölkerung geschehen; auch in dem Sinn, dass diese Ziele, aber auch die dahinterstehenden Werte, der Bevölkerung entsprechend vermittelt werden. Weiters sollte Verantwortung dafür getragen werden, die strategisch relevante Umwelt entsprechend und in offener Weise zu beurteilen und zu bewerten und schließlich auch die Verantwortung dafür, diejenigen Maßnahmen zu ergreifen, um mögliche Bedrohungen, insbesondere solche, die auf die strategischen Ziele des Staates gerichtet sind, abwehren zu können. Die Formulierung von strategischen Zielen ohne die entsprechenden

---

[14] Dies bedeutet jedoch auch, dass der Bevölkerung Werte und Interessen und somit auch die strategischen Ziele des Staates nicht nur bekannt, sondern auch bewusst sein müssten.

Mittel zur Verfügung zu stellen, kann weder als erfolgsorientiert noch nachhaltig bezeichnet werden.

In demokratisch orientierten Staaten ist daher allgemein, nicht nur vom akademischen Standpunkt aus, sondern auch, und insbesondere aus Sicht des Staatsbürgers, die Fähigkeit, der Wille und auch der Mut der politisch Verantwortlichen zum strategischen Denken und in weiterer Folge zum strategischen Handeln zu fordern. Es ist dies die ureigenste Aufgabe der Politik.

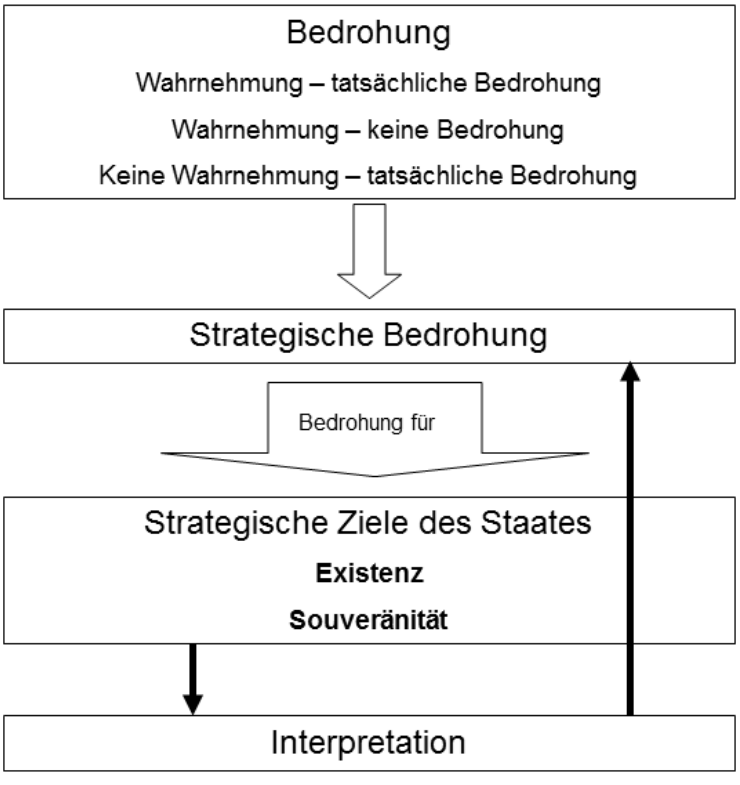


Abbildung 1: Strategische Bedrohung
Thomas Pankratz

1.2 Zum Begriff der Hybriden Bedrohungen

Anton Dengg
Michael N. Schurian

1.2.1 Einleitung

Bis ca. Ende des 20. Jahrhunderts konnten Konflikte relativ einfach beschrieben werden: Ein Staat oder Staatenverbund setzte seine Machtmittel (zumeist militärische) gegen einen anderen Staat ein. Der Kampf war gegen einen klar identifizierten Feind ausgerichtet. Im Kalten Krieg standen sich zwei ideologisch konträre Machtblöcke gegenüber und versuchten durch ein militärisches Wettrüsten den jeweils anderen zu dominieren. Bedingt durch neue Waffensysteme (z.B. Interkontinentalraketen oder Langstreckenbomber) veränderten sich strategische Überlegungen und militärische Ausrichtungen. Mit sogenannten Stellvertreterkriegen versuchte man politischen Einfluss zu gewinnen beziehungsweise zu erweitern. Hierzu wurden unterschiedliche Mittel und Methoden angewandt. Regionale Akteure wurden in deren Konflikten von „Paktvertretern" mit unterschiedlichen Instrumentarien unterstützt. Propagandamaßnahmen stellten einen wesentlichen Faktor in der medialen „Gut kontra Böse"-Inszenierung dar. Auseinandersetzungen wurden dabei großteils Ebenen-konform (Staat gegen Staat, Streitmacht gegen Streitmacht) ausgetragen. Mit dem Zerfall des Warschauer Paktes löste sich die bipolare Weltordnung auf und damit auch ein überschaubares und relativ kalkulierbares Konfliktbild.

Die folgende Entwicklung von neuen Technologien, insbesondere der Informations- und Kommunikationstechnologien sowie der sozialen Netzwerke, ermöglichte Staaten einen breiteren Handlungsspielraum, um Machtprojektion auf vielfache Art und Weise gegen andere Staaten auszuüben. Dabei spielt nicht nur der zeitliche Faktor, sondern vor allem – wie an Beispielen von Cyberattacken ersichtlich – die verdeckte Anwendung staatlicher Machtprojektion eine besondere Rolle. Primäres Ziel ist, sich nicht als Aggressor zu erkennen zu geben, sondern die Zielerreichung, den anderen Staat im eigenen Sinne zu beeinflussen. Dadurch bleibt möglicherweise ein positives internationales Image unangetastet, und/oder man eröffnet die Möglichkeit, die Schuld für eine aggressive Handlung einem anderen Staat zuzuschreiben. Insbesondere im Cyberbereich sind derartige Aktivitäten zu beobachten. „Die Geschwindigkeit und Nichtvorher-

sehbarkeit von Angriffen machen es nahezu unmöglich, die Herkunft des Gegners und dessen Motive in eigens vorbereitendes Handeln einzubeziehen“[1], konstatieren deutsche Sicherheitsexperten. Des Weiteren führen die Experten aus, dass die „[...] Möglichkeit „Cyber-Angriffe“ im Nachhinein zu bestreiten, [..] bereits heute zum strategischen Kalkül einer neuen, computergestützten Auseinandersetzung auch zwischen Staaten [gehört].“[2] Der 2008 vorherrschende bewaffnete Konflikt zwischen Georgien und Russland zeugt von ähnlicher hybrider Machtprojektion unter Zuhilfenahme des Cyberraumes.

Die Auseinandersetzung im gegenwärtigen Ukraine-Konflikt lässt einen weiteren Einsatz hybrider Methoden durch nicht einem Staat zuzuordnende bewaffnete Gruppierungen erkennen. Speziell diese Form der Machtprojektion dürfte zukünftig vermehrt Nachahmer finden. Der Ukraine-Konflikt offenbart, dass sich die Fähigkeit und Intention der Machtprojektion durch hybride Mittel als Trend herauskristallisieren könnte.

Hybride Methoden lassen sich aber nicht nur bei der Machtprojektion von Staaten, sondern ebenso bei Terrororganisationen verorten. Der im letzten Jahrzehnt vorherrschende Terrorismus, welcher nicht auf staatliche Unterstützung angewiesen ist[3], bietet mit seinen innovativen Taktiken und Methoden sogar Großmächten die Stirn. Die westliche Gemeinschaft bemüht sich zwar, Lösungskonzepte zu finden, wirksame Gegenstrategien zur Eindämmung des globalen Terrorismus wurden aber noch nicht entwickelt. Religiöse Fanatiker bestimmen mit ihren über das Internet medial verbreiteten grausamen Taten nach wie vor das Kriegsbild. Die vielen Jahre internationaler Kriseninterventionen, wie beispielsweise in Afghanistan und im Irak, zeigen zukünftige Herausforderungen bei der Entwicklung brauchbarer sowie langfristiger Lösungskonzepte gegen hybride Mittel und Methoden.

---

1 Bundesministerium der Verteidigung – Der Bundesminister: Verteidigungspolitische Richtlinien. Berlin, 27.05.2011, S. 3. <http://www.bmvg.de/portal/a/bmvg/!ut/p/c4/LYsxEoAgDATf4gdIbcv1MYBzcQbMDgQ8ftSONtssUsrddQ3iDdk9YlmWnaM4XXhauIq9pPLybB65wRDdF6FQzZ2R47PxdqtcTHGAXlU_q72byv9tgQFK91xGj6tRgx1/>, abgerufen am 05.01.2015

2 Ebd., S. 3.

3 Vgl. Bauer, Alain: Hybridization of Conflicts. In: PRISM 4, No. 4. <http://cco.dodlive.mil/files/2014/04/Hybridization_of_Conflicts.pdf>, abgerufen am 15.07.2014, S. 57.

Bisher waren sicherheitspolitische Expertisen eher auf konventionelle Kampfführung und entsprechende Gegenstrategien ausgerichtet. Die angeführten Beispiele führen die Vielschichtigkeit der Machtprojektionsmöglichkeit vor Augen, was auch unter Experten zu Diskussionen über hybride Bedrohung führt. Vor dem Hintergrund weltweiter Vernetzung und der grenzüberschreitenden Wirkungsmächtigkeit ökologischer sowie ökonomischer Risiken sind viele Staaten einer neuartigen Form von Bedrohung ausgesetzt. Diese können nicht mehr ausschließlich durch die Institution Militär abgewehrt werden. Genau hier setzt das Projekt des Instituts für Friedenssicherung und Konfliktmanagement der Landesverteidigungsakademie (IFK/LVAk) an und versucht eine Bewusstseinsbildung in dieser Thematik zu fördern.

1.2.2 Methodik

Grundlage dieser Arbeit bildete das 2011-2012 am IFK behandelte Projekt „Strategien hybrider Machtprojektion am Beispiel USA, Russland, China und Indien". Daraus entwickelte sich das Folgeprojekt „Hybride Bedrohungspotentiale und daraus resultierende sicherheitspolitische Ableitungen für Kleinstaaten".

Bei der Begrifflichkeit „Kleinstaat" wurde auf die Unterscheidungsmerkmale von Jeanne A.K. Hey zurückgegriffen. Hey unterscheidet drei Kategorien von Kleinstaaten:

a) „Mikrostaaten mit weniger als einer Million Einwohner (z.B. in der Karibik und im Indischen Ozean),
b) industrialisierte europäische Kleinstaaten (z.B. Belgien, Niederlande, Schweiz und Österreich), [...], sowie
c) unterentwickelte Kleinstaaten der Dritten Welt (z.B. in Afrika, Asien und Lateinamerika) [...]"[4].

[4] Hey, Jeanne A.K.: Refining Our Understanding of Small State Foreign Policy. In: Hey, Jeanne A.K. (Hrsg.): Small States in World Politics. Explaining Foreign Policy Behavior. Boulder, Colorado 2003, S. 185-195; zitiert nach Wilhelm, Andreas: Außenpolitik. Lehr- und Handbücher der Politikwissenschaft; München 2006, S. 109.

Für die weiterführende Bearbeitung des Projekts wählte man die Kategorie „industrialisierte europäische Kleinstaaten" aus. Schließlich wurden in einem weiteren Arbeitsprozess die Staaten Slowakei und Schweden herausgefiltert. Grund für diese Selektion war, dass diese Staaten einerseits betreffend Struktur, Heeresgröße und Auslandsengagement Österreich ähneln und somit eine Vergleichsgröße darstellen. Andererseits unterscheiden sie sich durch ihre Zugehörigkeit zu diversen Bündnissen (UNO, NATO, etc.), was mögliche unterschiedliche staatliche Herangehensweisen bei der Abwehr hybrider Bedrohungen erklärt. Die daraus gewonnenen Ableitungen dienen als Beitrag für weiterführende sicherheitspolitische Diskussionen.

Die theoretische Basis für das Projekt bildete der Soft- und Hardpower-Ansatz von Joseph Nye. Ein Land kann, so Nye, „[...] andere auf drei verschiedene Arten drängen, seinen Interessen zu dienen: durch Zwang, Geld oder Attraktivität"[5]. Mit Hilfe eines empirisch-analytischen Ansatzes wurden im Projekt die Sicherheitsstrategien der Slowakei und Schwedens nach konkreten Inhalten „hybrider Bedrohungen" untersucht.

Zur Gewinnung eines thematischen Überblicks stützte sich die Projektleitung auf Internetrecherchen, Expertengespräche und Workshops. Analysiert wurden unterschiedliche sicherheitspolitische Strategien und Studien hinsichtlich der Begrifflichkeit „hybride Bedrohungen". Erste Ergebnisse zeigten, dass zwar vermehrt Inhalte zu „hybrider Kriegsführung" (*Hybrid Warfare*), jedoch kaum Erkenntnisse zu hybriden Bedrohungen existieren. Das Augenmerk lag neben theoretischen Überlegungen auch auf möglichen Akteurskonstellationen sowie deren Mittel und Methoden, um – falls Hybridität nicht thematisiert wurde – daraus indirekt auf das Vorhandensein hybrider Bedrohungen zu schließen.

Erste Analysen von Krisen- und Konfliktträumen sowie verschiedenen sicherheitsrelevanten Vorfällen zeigten, dass die Begrifflichkeit „hybride Kriegsführung" (*Hybrid Warfare*) zu kurz greift. Eine Veränderung der Politik in einem Staat setzt nämlich nicht zwingend Kriegsführung voraus –

---

[5] Joseph S. Nye, Jr.: Wladimir Putin verliert seine letzte „Soft Power". In: Die Welt Online, 30.12.2014.
<http://www.welt.de/debatte/kommentare/article135880512/Putin-verliert-die-letzte-Soft-Power-die-er-besass.html>, abgerufen am 31.12.2014.

es reicht eine empfindliche Destabilisierung der Wirtschaft oder Gesellschaft. Diese kann ohne offensichtliche Anwendung von militärischer Gewalt geschehen. So wurden z.B. hochkomplexe und mit hohem Aufwand produzierte Computerviren zur Beeinflussung staatlicher Aktivitäten eingesetzt, was der Computervirus *Stuxnet* beweist. Die bewusste Einwirkung auf staatliche Interessen mit nicht-militärischen Mitteln demonstriert nicht nur die neue Variation zur Machtprojektion, sondern ebenso die Intention von Staaten, derartige Formen auch einzusetzen. Der Stellenwert staatlicher Cybergewalt wird durch Edward Snowdens Enthüllungen von National Security Agency (NSA)-Überwachungspraktiken veranschaulicht. Snowden war sich bewusst, dass „[...] er durch seine Arbeit die Staatsmacht vergrößert [...]“[6] hatte, folgerte Laura Poitras, U.S.-Journalistin und Filmemacherin.

Als weiteres Beispiel indirekter, nicht-militärischer Intervention sind Unterstützungsmaßnahmen in Form militärischer Ausbildungstätigkeiten für Rebellen in Syrien durch britische Elite-Kämpfer[7] zu nennen. „Insgesamt sollen bereits mehr als 300 Rebellen im Irak an der syrischen Grenze ein Trainingslager absolviert haben. Die Ausbildung werde von Ex-Mitgliedern der SAS (Special Air Service), einer Spezialeinheit der britischen Armee, geleitet“[8], so ein „Spiegel Online“-Bericht 2012. Mit derartigen Handlungen beeinflussen Staaten/Regierungen nicht nur die Vorgänge in Konfliktregionen. Sie üben damit auch Einfluss auf das Handeln der betroffenen Staaten aus. Alle in den Beispielen genannten Aktivitäten sind somit als Teil hybrider Machtausübung zu werten.

Im Zuge verschiedener Expertengespräche und Workshops zeigte sich die Notwendigkeit einer Definition von „hybrider Bedrohung“. Zu diesem Zweck entwickelte das IFK eine Arbeitsdefinition, die in einem Workshop mit Exper-

---

6 Seibel, Alexandra: Die ganze Existenz aufs Spiel setzen. Interview mit der U.S.-Journalistin und Filmemacherin Laura Poitras, die im Juni 2013 Edward Snowden zusammen mit Glenn Grenwald, Reporter beim Guardian, in Hongkong traf; In: Kurier, 29.12.2014, S. 21.

7 Salloum, Raniah: Britische Elite-Kämpfer bilden Rebellen aus. In: Spiegel Online, 23.07.2012. <http://www.spiegel.de/politik/ausland/syriens-rebellen-werden-im-angeblich-im-ausland-trainiert-a-845923-druck.html>, abgerufen am 27.08.2014.

8 Ebd.

ten aus unterschiedlichen interdisziplinären Bereichen diskutiert wurde. Ein kleinerer Expertenkreis finalisierte schließlich die im Kapitel „Die Begrifflichkeit ‚hybride Bedrohung' (Kapitel 1.2.5)" angeführte Arbeitsdefinition.

Um die Komplexität „hybrider Bedrohungen" zu vereinfachen, wurden unterschiedliche Abbildungen und Übersichten angefertigt. Damit sollte sowohl die Begrifflichkeit von hybriden Bedrohungen als auch mögliche Interdependenzen erklärt werden. Einen weiteren Versuch der Komplexitätsreduktion stellt die entwickelte tabellarische Darstellung[9] von „Offensiv"-Akteuren mit deren offensiven Mitteln einerseits und entsprechenden „Defensiv"-Akteuren mit notwendigen defensiven Mitteln andererseits dar.

Schließlich analysierten einzelne Experten nach vorgegebenen Kriterien sicherheitspolitische Strategien und Berichte auf das Vorhandensein hybrider Bedrohungen bzw. auf entsprechend abzuleitende Inhalte. Beispiele zu bereits erfolgten hybriden Machtprojektionen auf unterschiedlichen Ebenen bildeten schließlich den Abschluss des Projekts, um den theoretischen Ansatz zu veranschaulichen.

1.2.3 Zielsetzung des Projekts

Eine intensive Beschäftigung mit der Thematik „hybride Bedrohungen" verdeutlicht, dass diese in der sicherheitspolitischen Forschung kaum verankert ist. Daher setzte sich das IFK zum Ziel, das Phänomen „hybride Bedrohung" zu untersuchen, wissenschaftlich fundiert zu betrachten und schließlich ins öffentliche Bewusstsein zu rücken. Dabei ist nicht nur das Wissen über derartige Bedrohungen entscheidend, sondern insbesondere die Kenntnis notwendiger Gegenstrategien. Angestrebtes Ziel des Projekts war es, sicherheitspolitische Konzepte ausgewählter Kleinstaaten hinsichtlich ihrer Einschätzung aktueller Bedrohungen zu analysieren und daraus Ableitungen zu entwickeln. Im Fokus des Projekts stand u.a. die Frage, inwieweit hybride Bedrohungsmöglichkeiten auf gesamtstaatlicher Ebene in den Referenzstaaten (Slowakei und Schweden) erfasst werden. Des Weiteren wurde analysiert, über welche Strategien und Konzepte

---

[9] Entwickelt von Bachora/Dengg/Schurian; siehe Abbildung 3.

internationale Sicherheitsorganisationen wie z.B. die North Atlantic Treaty Organization (NATO) verfügen, um hybriden Bedrohungen zu begegnen. Schließlich konzentrierte man sich auf die Frage nach den wahrgenommenen Wechselwirkungen zwischen der Beteiligung am internationalen Konflikt- und Krisenmanagement (IKKM) und den mit hybriden Bedrohungen verbundenen Risiken im Entsendestaat. Dabei lag der Fokus auf der Frage nach den staatlichen Konsequenzen im Rahmen einer gesamtstaatlichen Sicherheitsvorsorge.

Letztendlich mündeten Erkenntnisse und Rückschlüsse, insbesondere in puncto Bedrohungsbilder sowie möglicher Schutz- und Abwehrmaßnahmen, in Ableitungen für Kleinstaaten. Die daraus resultierenden Erfahrungen bzw. *Lessons Learned* sollen als Anhalt für die österreichische sicherheitspolitische Beratung dienen. Damit wird der 2014 erschienenen Teilstrategie des österreichischen Bundesministeriums für Landesverteidigung und Sport Rechnung getragen, wonach es heißt, dass künftig „[...] Konflikte im europäischen Umfeld vermehrt mit hybriden Methoden ausgetragen werden“[10].

1.2.4 Allgemeine Betrachtungen von Bedrohungsbildern

Der Gedanke, dass Konfliktakteure – seien es staatliche oder nicht-staatliche – jedes mögliche Mittel und jede Methode zur Zielerreichung einsetzen, ist keinesfalls neu. Bereits Clausewitz stellte fest, dass jede Zeit ihr eigenes Konzept des Krieges auszutragen hat[11]. Kriegsführung als kulturelles Phänomen ist stets ein Reflex der Zivilisation, eingebunden in den technologischen Standard der jeweiligen Zeit und Gesellschaft. Daran scheint sich bis heute nichts geändert zu haben.

Neuartig bei der gegenwärtigen Bedrohung sind die veränderten Rahmenbedingungen, in denen sich Staaten und deren Streitkräfte zu Beginn des 21. Jahrhunderts befinden: Globalisierung und Entgrenzung strapazieren territorial definier-

---

10 BMLVS: Teilstrategie Verteidigungspolitik, S. 5. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf>, abgerufen am 13.11.2014

11 Clausewitz, Carl von: Vom Kriege. Achtes Buch, Drittes Kapitel. B. Reclam 1994 (1832), S. 312.

te Konzepte wie z.B. Souveränität oder Landesverteidigung. Eine globale Bevölkerungsexplosion, die mit einem ebenso exponentiellen Anstieg an zu befriedigenden Bedürfnissen sowie Ressourcenverbrauch einhergeht, drängt Volkswirtschaften in einen Wettbewerb um knapper werdende Rohstoffe, wobei die Technologierevolution diese noch verstärkt. Informationen, Meinungen und Kapital zirkulieren weltweit, nahezu ohne Zeitverzug. Die globale mediale Vernetzung sowie die Möglichkeit permanenter Kommunikation mittels der IKT-Technologie (damit auch Beeinflussungsmöglichkeiten, ob bewusst oder unbewusst) ermöglichen den internationalen Vergleich verschiedener Lebenswelten als auch Lebensstandards und damit unterschiedlicher „Freiheitsformen", die die jeweilige Gesellschaft ihren Mitgliedern ermöglicht oder vorenthält. Das Ergebnis dieses Vergleichs ist, neben anderen Ursachen und Motiven, ein Grund für Migrationsströme, insbesondere nach Europa.

Gesellschaften, Märkte, insbesondere der einzelne Mensch vernetzten sich in einem immer höheren Ausmaß. Dadurch sind Staaten sowohl mächtiger, als auch verletzlicher. Die Sicherheit und Stabilität von Staaten, der Wohlstand von Gesellschaften und das Wohlergehen von Individuen hängen demzufolge von der Funktionstüchtigkeit komplex gekoppelter Systeme ab. Als exponiertes Beispiel dient das Energienetz oder der bargeldlose Zahlungsverkehr. Sind diese gekoppelten Systeme erst einmal funktional beeinträchtigt, wirkt sich dies negativ auf Staaten, Märkte und Gesellschaften aus. Daraus ergibt sich die Frage nach den möglichen Ausprägungen von Einflussnahmen auf Akteure. Wie findet zukünftig eine Konfliktaustragung statt? Welche Bedrohungen kommen in einer komplex vernetzten Welt auf uns zu?

Es ist davon auszugehen, dass feindliche hybride Machtprojektionen – wie im IFK-Modell dargestellt (siehe Abbildung 2 „Hybride Bedrohungspotentiale und Strategien" weiter unten) – hybride Gegenreaktionen, ersichtlich durch entsprechende Strategien, hervorrufen. Dabei ist zu berücksichtigen, dass defensive Gegenreaktionen auch umgekehrt und als Offensivstrategien einsetzbar sind.

Eine Erkenntnis aus der Analyse von Strategie- und Bedrohungsanalysen ist, dass sich unterschiedliche staatliche Sicherheitsexpertisen oftmals in ihren sicherheitspolitischen Bedrohungsszenarien ähneln. Ein Blick in Sicherheitsstrategien großer Staaten bzw. Staatenbündnissen, wie z.B. der EU, zeigt deutliche Übereinstimmungen bei sicherheitspolitischen Herausforderungen. Dies kann zweierlei bedeuten: Entweder reagieren jene Staaten unabhängig auf ähnliche

reale Bedrohungsszenarien oder sie lehnen sich an Bedrohungsszenarien von Großstaaten an und generieren entsprechende Ableitungen für ihren Bereich (siehe Abbildung 2). Damit würden sich für Kleinstaaten aber zwei Herausforderungen ergeben:

a) einerseits müssten sie sich gegen die von Großstaaten analysierten (hybriden) Bedrohungsszenarien wappnen; und
b) andererseits Strategien gegen mögliche (hybride) Offensivstrategien von Großstaaten (sowie von nichtstaatlichen Akteuren) entwickeln.

Machtausübungskategorien – wie Politik, Ökonomie, Ökologie, Cyber, Kultur, Medien, und Streitkräfte – auf dem Boden, auf See, in der Luft und im Weltraum spielen hierbei eine signifikante Rolle. Insbesondere technologische Entwicklungen ermöglichen zunehmend auch nicht-staatlichen Akteuren (wie z.B. Konzernen) entweder in Teil- oder allen Kategorien, Staaten durch hybride Machtausübung zu beeinflussen. Einflussmöglichkeiten auf die kritische Infrastruktur sind hier hervorzuheben.

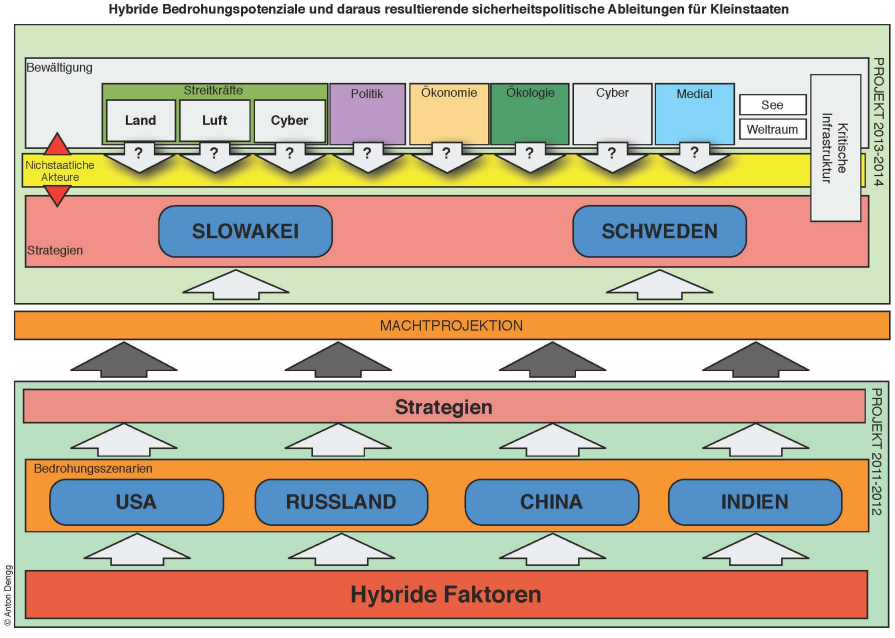


Abbildung 2: Hybride Bedrohungspotentiale und Strategien
Anton Dengg

Es ist davon auszugehen, dass vor allem Kleinstaaten auf Bedrohungsbilder von großen Staaten zurückgreifen. Nur so lässt sich erklären, dass sich diese in ihren Bedrohungsanalysen und Strategien nahezu gleichen. Dabei ist jedoch zu berücksichtigen, dass sich Kleinstaaten in Zeiten zunehmender politischer und wirtschaftlicher Globalisierung an den globalen sicherheitspolitischen Gegebenheiten orientieren müssen und sich daher Ähnlichkeiten in den Bedrohungsanalysen erklären lassen. Die Komplexität dieses Umstandes zeigt – abgesehen von den vielen Vorteilen, welche die Globalisierung mit sich bringt – auch Gefahren und Bedrohungen für Staaten und Gesellschaften auf: mit der steigenden infrastrukturellen Vielschichtigkeit wächst neben der Abhängigkeit auch die Verwundbarkeit. Damit ist die Sicherheit von Gesellschaften ebenso gefährdet wie diejenige jedes Individuums. Der Staat als Souverän des legitimierten Machtapparats hat daher Schutzvorkehrungen zu treffen. Doch wie soll/muss ein Staat reagieren? Welche Gegenmaßnahmen sind wann zu ergreifen?

1.2.5 Die Begrifflichkeit „hybride Bedrohung"

Seit geraumer Zeit sucht man nach Antworten auf die Herausforderungen von „neuen" oder „asymmetrischen Kriegen". Die Intention, mit dem Begriff „hybride Bedrohung" eine neue Kategorie in die Forschungsdebatte einzuführen, bedarf zunächst einer Erklärung. Wo wird dieser Begriff diskutiert und welche neuen Erkenntnisse lassen sich daraus überhaupt gewinnen bzw. gibt es daraus resultierende Gegenmaßnahmen?

Grundsätzlich ist festzuhalten, dass es keine einheitliche Begriffsdefinition zu „Hybriden Bedrohungen" gibt. Im angloamerikanischen Raum findet sich vermehrt die Bezeichnung *Hybrid Warfare*. Dabei wird der Kampf mit konventionellen militärischen wie unkonventionellen Elementen mit entsprechenden Mitteln und Methoden (z.B. mit nicht-militärischen Kräften, Guerillas, terroristischer und krimineller Taktik) geführt.

Unter „Bedrohung" versteht das *Wörterbuch Sicherheitspolitik*

> „[...] die Wahrnehmung einer existenziellen Gefährdung eines Staates, einer Staatengemeinschaft oder eines Bündnisses durch die Politik eines anderen Staates, einer Staatengemeinschaft, oder die, meist gestützt auf überlegene militärische Machtmittel, Gefahren für deren Sicherheit, Souveränität und Integrität[...]"[12].

Dabei kann diese Bedrohung zunächst eine lediglich subjektive Einschätzung einer latenten Gefährdung staatlicher Sicherheit sein. Ob sich die Bedrohung tatsächlich realisiert, hängt von den Fähigkeiten und der Intention des Gegners ab. Erst die Befähigung, die sich mit einer Schädigungsabsicht verbindet, stellt eine konkrete Bedrohung dar. Dabei kann sich der Vorsatz abrupt ändern, während der Aufbau von adäquaten Möglichkeiten die Bereitstellung von Ressourcen und insbesondere einen gewissen zeitlichen Vorlauf benötigt. Kurzum: Eine Bedrohung setzt sich aus Können *und* Wollen zusammen, aus der Befähigung und der Intention. Während der Kapazitätenaufbau einige Zeit in Anspruch nimmt und beobachtet werden kann, gestaltet sich die Feststellung einer Schädigungsabsicht weitaus schwieriger. Der Wechsel der Politik kann

---

[12] Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald; Schreiner/Karl H. und Bruzek, Oliver: Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000, S. 38.

abrupt erfolgen und unversehens wird aus einem strategischen Partner eine aktuelle Bedrohung. Dies konnte am Ukraine-Konflikt, der die Europäische Union (EU) überraschte, beobachtet werden.

Der Begriff der „Hybridität" stammt aus der Biologie bzw. ursprünglich aus der Landwirtschaft. Dort bezeichnet der Begriff eine Mischform von zwei vorher getrennten Systemen. Der Duden definiert das „Hybrid" hingegen als eine Mischung aus zwei oder mehreren Komponenten. Ein Beispiel aus der Tierwelt ist etwa das Maultier, eine Kreuzung aus Pferd und Esel, deren Züchtung wesentliche Vorteile der beiden Tiere hervorheben sollte. Ein neues „Produkt" war entstanden. Die Kombination von zwei oder mehreren ursprünglich eigenständigen Elementen lässt hier etwas Neues entstehen. Dabei bezieht sich das Neue nicht nur auf die innere Zusammensetzung, sondern wirkt sich auch maßgeblich auf seine Umwelt aus. Für die Konzeption der „hybriden Bedrohung" bedeutet dies, dass bisher erkannte Bedrohungsformen miteinander neu kombiniert werden. Letztlich erfolgt durch die Neukonfiguration bestehender Konfliktphänomene und Bedrohungsformen eine Erweiterung des Bedrohungsspektrums.

Es lässt sich somit festhalten, dass hybride Bedrohungen eine Synthese – von bislang isoliert betrachteten Konfliktbildern – darstellen. Als solche gibt es nicht *die* hybride Bedrohung, sondern unterschiedliche Bedrohungen, die aus divergierenden Variationen alternierender Kombinationen entstehen und so wechselweise Effekte und Stoßrichtungen erzeugen. Hybride Bedrohungen sind jedenfalls im Plural zu denken. Demzufolge sind Lösungsansätze, Schutz- und Abwehrmechanismen in entsprechender Vielfalt zu entwickeln.

Hybride Bedrohungen setzen sich konzeptuell aus mehreren Elementen konventioneller Bedrohungsbilder zusammen. Die militärische Durchführungsform (*Hybrid Warfare*) ist daher nur als eine Teilmenge im hybriden Bedrohungsspektrum zu betrachten. Hoffmann bezieht sich in einem Artikel zu Hybrid Warfare auf die National Defense Strategy (NDS) 2005, wonach hybride Kriegsführung eine Mischung von traditionellen,

irregulären, terroristischen und disruptiven Bedrohungen darstellt.[13]

Das Konzept der Hybriden Bedrohungen geht über jenes des *Hybrid Warfare* hinaus, da es auch nicht-militärische Mittel berücksichtigt. In konzeptioneller Hinsicht stellt dieses Bedrohungsbild eine Reaktion auf das sich seit dem Zusammenbruch des Ost-West-Gegensatzes abzeichnende Diffuser-werden von Konflikten dar. Hoffmann schreibt:

> "[...] our greatest challenge in the future will come not from a state that selects one approach, but from states or groups that select from the whole menu of tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography and aims."[14]

Hybride Bedrohungen sind somit gekennzeichnet von der Anwendung konventioneller und irregulärer Taktiken, von dezentraler Planung und Ausführung, der Präsenz nicht-staatlicher Akteure und dem Einsatz von Hochtechnologie. Die Kombination verschiedener Taktiken und Methoden führt zu einer „Arbeitsteilung" von staatlichen Einheiten und nicht-staatlichen Gruppierungen bzw. zur Etablierung neuartiger innovativer Formationen, die imstande sind, alle Aktivitäten durchzuführen.

2010 beschäftigte sich das United States Government Accountability Office (GAO) in Washington mit hybrider Kriegstaktik, welche mit hoher Wahrscheinlichkeit von gegenwärtigen sowie zukünftigen Gegnern genutzt wird. Demnach werden U.S.-Truppen mit Bedrohungen wie

> „[...] non-state- and state-sponsored adversaries, including computer network and satellite attacks; portable surface-to-air missiles; improvised explosive devices; information and media manipulation; and chemical, biological, radiological,

---

13 Hoffman, Frank G.: Hybrid Warfare and Challenges. In: JFQ, issue 52, 1st quarter 2009, S. 35. <http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fsmallwarsjournal.com%2Fdocuments%2Fjfqhoffman.pdf&ei=4z0YVMzZKsTuyQOnsYCgBQ&usg=AFQjCNGcQFhNuLAoKd3Hvk_2zv9uzNm8sQ&bvm=bv.75097201,d.bGQ>, abgerufen am 16.09.2014.

14 Hoffmann, Frank G.: Hybrid Threats. Reconceptualizing the Evolving character of Modern Conflict. In: Strategic Forum, No. 240, April 2009, S. 5.

nuclear, and high- yield explosive devices"[15]

konfrontiert. Trotz dieser Erkenntnis hat das Department of Defense (DoD) keine offizielle Definition von hybrider Bedrohung und „[...] has no plans to do so because DOD does not consider it a new form of warfare."[16] Mehrere U.S.-Experten aus der Politik und dem Militär bekräftigten daraufhin, dass sie für die immer komplexeren Konflikte den Begriff „Hybride Warfare" in ihren Doktrinen nicht verwenden.[17]

Im besagten GAO-Papier wird eine Arbeitsdefinition von „Hybrid Threat" des Joint Irregular Warfare Centers als Beispiel erwähnt. Darin wird "Hybrid Threat" charakterisiert als:

> „An adversary that simultaneously and adaptively employs some fused combination of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors."[18]

2011 legte die U.S. Army den Begriff „Hybrid Threat" in deren „Operations Doctrine" fest. Darunter wird verstanden: "The diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects."[19] Auch wenn der GAO-Definitionsversuch der IFK Arbeitsdefinition nicht unähnlich ist, zeigt sich insbesondere bei jenem der U.S. Army, dass im U.S.-Kontext hybride Bedrohungen eher als militärische Kampfhandlungen verstanden werden.

---

15 GAO, United States Government Accountability Office: Subject: Hybrid Warfare. GAO-10-1036R Hybrid Warfare. Washington, DC 10.09.2010, S. 1. <http://www.gao.gov/new.items/d101036r.pdf>, abgerufen am 29.09.2014.

16 Ebd., S. 2.

17 Ebd., S. 2.

18 Working definition derived by U.S. Joint Forces Command, Joint Irregular Warfare Center, 2008-2009. In: GAO, United States Government Accountability Office: Subject: Hybrid Warfare. GAO-10-1036R Hybrid Warfare. Washington, DC 10.09.2010, Enclosures, S. 18. <http://www.gao.gov/new.items/d101036r.pdf>, abgerufen am 29.09.2014.

19 U.S. Army: Field Manual 3-0 Operations C-1. GPO, Washington, DC Februar 2011, S. 1ff. In: MAJ Brian P. Fleming, United States Army: The Hybrid Threat Concept. Contemporary War, Military Planning and the Advent of Unrestricted Operational Art. Report. 17.05.2011, S. 2. <https://www.hsdl.org/?view&did=700828>, abgerufen am 16..09.2014.

Einen weiteren möglichen Ansatz eines europäischen Definitionsversuches lieferte 2013 der European Council on Security and Defence:

> „The world as a whole faces increased volatility, complexity and uncertainty. A multipolar and interconnected international system is changing the nature of power. The distinction between internal and external security is breaking down. Complex layers of governance and new patterns of interdependence empower new players and give rise to new challenges "[20]

Aus den oben genannten unterschiedlichen Definitionen lässt sich erkennen, dass zu Beginn des Projekts die Entwicklung einer für alle teilnehmenden Experten akzeptablen und allgemein verständlichen Arbeitsdefinition von „hybrider Bedrohung" erforderlich war. Im Laufe des Forschungsprojektes wurde schließlich folgende Arbeitsdefinition entwickelt:

„Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen."[21]

Dieser Arbeitsdefinition ist hinzuzufügen, dass Bedrohungshandlungen eine strategische Schwelle überschreiten müssen, um als hybride Bedrohung zu gelten. Das ist dann der Fall, wenn durch eine feindliche Aktivität die Handlungs- und Entscheidungsfreiheit eines angegriffenen Staates in substanzieller Weise eingeschränkt wird. Die Ausformung dieser Einschränkung kann von Fall zu Fall unterschiedlich sein und, je nach Auswirkungen, von jedem Staat anders

---

[20] High Representative/Head of the EDA on the Common Security and Defence Policy: Preparing the December 2013 European Council on Security and Defence. Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy. Brüssel 15.10.2013. <http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf>, abgerufen am 06.10.2014.

[21] Arbeitsdefinition entwickelt durch das Institut für Friedenssicherung und Konfliktmanagement der Landesverteidigungsakademie (Dengg/Feichtinger/Schurian) in Anlehnung an: Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald/Schreiner, Karl H. und Bruzek, Oliver. Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000.

interpretiert werden. Was bleibt ist die Frage nach der Identifikation einer strategischen Schwelle. Ein Ansatz dazu ist: Diese wird überschritten, wenn zumindest zwei Sektoren hybrider Bedrohungen betroffen beziehungsweise zu deren Abwehr mindestens zwei Ministerien involviert sind.

Aus dem bisher Gesagten ist ersichtlich, dass das IFK den Begriff „hybride Bedrohungen" in seinem arbeitsdefinitorischen Ansatz umfassender und detaillierter interpretiert als dies in anderen Begriffsdefinitionsversuchen zu finden ist.

In der internationalen Publikationslandschaft werden „hybride Bedrohungen" – nach dem Verständnis des IFK – kaum diskutiert. Thematisiert wird – wie erwähnt – hybride Kriegsführung (*Hybrid Warfare*), die sich nach Ansicht der Autoren dieser Zeilen eher auf Hard Power (sprich dem Kampf mit Waffen und Kampfmitteln) beschränkt. Erste Anzeichen (die NATO beschäftigt sich z.B. mit „Hybrid Threats") lassen ein Umdenken bei Experten erkennen, wonach man zunehmend über *Hybrid Warfare* hinausgeht. Unterschiede in der Definition liegen vermehrt im unterschiedlichen Verständnis von „Krieg". Ist Smart Power „Krieg"? Ab welcher Schwelle ist bei Hard Power von „Krieg" zu sprechen? Oder: Welche Dimension von terroristischen Aktivitäten muss vorherrschen, um einen „War on Terror" auszurufen?

Da der Kriegsbegriff umstritten ist, wird hier von einer näheren Erläuterung Abstand genommen. Festgelegt wurde allerdings, dass die Bezeichnung „Krieg" nur dann zulässig ist, wenn eine Auseinandersetzung mit erheblicher Waffengewalt unter Involvierung von zumindest zwei Staaten ausgetragen wird. Damit trifft bei hybrider Bedrohung die Bezeichnung Krieg nicht zu, weil mehrere Arten von auch nicht mit physischer Gewaltanwendung verbundenen Machtprojektionen angewandt werden.

2011 organisierte die NATO Allied Command Transformation (NATO ACT) unter Teilnahme von ca. 100 Experten – zusammengesetzt aus dem privaten Sektor sowie Sachkundigen aus der NATO – ein einwöchiges Szenarien-Experiment zur Thematik „Countering Hybrid Threats". Auffallend ist eine offensichtliche Trendumkehr von *Hybrid Warfare* zu „Hybrid Threats". Diese NATO-Simulation verdeutlicht den nunmehr breiteren Verständnisansatz. Die NATO beschreibt Terrorismus, Migration, Piraterie, Korruption, ethnische Konflikte als Teil der hybriden Bedrohung. Sie sieht in einer Orchestrierung von Diplomatie, politischer Interaktion, humanitärer Hilfe, sozialem Druck, ökonomischer Entwicklung und einer geschickten Medienkampagne sowie dem Ein-

satz militärischer Kräfte eine hybride Bedrohung als "[...] those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives"[22]. Der arbeitsdefinitorische Ansatz von „hybrider Bedrohung" des IFK grenzt somit stark an jenen der NATO. Weitere offizielle NATO-Ansätze zur Handhabung hybrider Bedrohungen, die über das Szenarien-Experiment hinausgehen, sind – zumindest offiziell – nicht erkennbar.

1.2.6 Interessensdurchsetzung als Zweck einer hybriden Bedrohung

Für Clausewitz ist Krieg ein „[...] Akt der Gewalt, um den Gegner zur Erfüllung unseres Willens zu zwingen"[23]. Folglich ist Krieg eine Interessensdurchsetzung. Gleichzeitig muss hingegen nicht jede Form der Interessensdurchsetzung Krieg sein.

Ein Akteur kann durch den konzertierten Einsatz von Instrumenten aus seinem „Werkzeugkasten" der hybriden „Kampfmittel" die Durchsetzung und Sicherung seiner Interessen anstreben. Ein hybrides Vorgehen gegen einen Zielstaat mit nicht-militärischen Mitteln dürfte eher dann erfolgen, wenn eine direkte (militärische) Konfrontation wenig lohnend erscheint oder dem internationalen Ansehen schaden könnte. Die eigentliche Interessensdurchsetzung – Schwächung des Gegners – kann ebenso durch die Anwendung anderer Mittel und Methoden (als militärischen) erreicht werden.

Um die hybride *Bedrohung* von anderen umfassenden Politik-Ansätzen zu unterscheiden, sind Kriterien erforderlich, die in einer Analyse erlauben, den koordinierten Einsatz von Instrumenten unterschiedlicher Bedrohungsfelder nach seinen schädlichen und nach seinen fördernden Auswirkungen zu differenzieren.

---

[22] Miklaucic, Michael: NATO Countering the Hybrid Threat. <http://www.act.nato.int/nato-countering-the-hybrid-threat>, abgerufen am 15.09.2014.

[23] Clausewitz, Carl von: Vom Kriege. In: Von Clausewitz, Sun Tzu: Vom Kriege und die Kunst des Krieges. Meisterwerke der Strategie. Bearbeitung: MaxiBucks. 1. Auflage, 2011; iBooks Store; Hochformat S. 22.

Ein solches Unterscheidungsmerkmal ist die stabilisierende Wirkung durch ein mehrdimensionales Vorgehen. Das Engagement Österreichs in Bosnien-Herzegowina (BiH) ist z.B. eine Politik der mehrdimensionalen Interessensdurchsetzung, die im Zielstaat (BiH) den Sicherheitssektor[24], das Justizwesen[25] und die Wirtschaft[26] betrifft. Die Intention ist jedoch nicht die Anwendung einer hybriden Bedrohung, sondern einen Beitrag zu leisten, „[...] um dem Balkan-Staat auf seinem Weg in eine friedliche und demokratische Zukunft zu helfen“[27]. Eine hybride Bedrohung würde mit dem gleichen umfassenden Ansatz vielmehr das Gegenteil beabsichtigen: interne Destabilisierung, Desintegration, öffentliche Furcht und Unruhe, ökonomische Volatilität, diplomatische Isolierung zur Durchsetzung eigener Interessen. Eine hybride Bedrohung ist daher als Form der negativen Anwendung von Gewalt zu bezeichnen.

1.2.7 Gewalt

Gewalt ist eng mit dem Begriff Macht verknüpft, woraus eine Bedrohung (oftmals subjektiv empfunden) abgeleitet werden kann. Der Gewaltbegriff ist ein täglicher Begleiter in der Nachrichtenwelt. Artikel in Tageszeitungen zeigen die Verwendung des Gewaltbegriffs wie z.B.: die Gewalt der Milizen; Brennstäbe werden mit Gewalt herausgezogen; wenn Journalisten Gewalt ausgesetzt sind; es wird von einem gewaltsamen Zwischenfall berichtet; kirchlicher Gewalt; da wird jemandem unter Androhung von Gewalt erpresst. Die Bezeichnung „Gewalt“ wird demnach oftmals in verschiedenen Zusammenhängen verwendet.

Gewalt ist

---

[24] Vgl. Kugelweis, Pierre: Universität Graz und Streitkräfte blicken gemeinsam auf Bosnien-Herzegowina. In: Der Soldat; Ausgabe Nr. 23/2010, 01.12.2010. <http://www.dersoldat.at/universitaet-graz-und-streitkraefte-blicken-gemeinsam-auf-bosnien-herzegowina?PHPSESSID=66m5qg8qftiuu6kuj0tdh2f7g6>, abgerufen am 19.10.2015.

[25] Ebd.

[26] Bundesministerium für Europa, Integration und Äußeres, Republik Österreich: Außen- und Europapolitischer Bericht 2013; S. 87; <http://www.bmeia.gv.at/fileadmin/user_upload/Zentrale/Publikationen/AEPB/Aussen_und_Europapolitischer_Bericht_2013.pdf>, abgerufen am 19.01.2015

[27] Österreichisches Bundesheer: Bundesheer in Bosnien. <http://www.bundesheer.at/ausle/eufor/index.shtml>, abgerufen am 19.01.2015.

„[...] in der Politik im weiter definierten Sinne Sammelbezeichnung für Bestrebungen individueller oder kollektiver Akteure, die darauf gerichtet sind, öffentlich-politische Anliegen unter Androhung oder Einsatz von physischem oder psychischem Zwang gegen Leib und Leben oder mittels verdeckter Gewalt (»strukturelle Gewalt«) zu beeinflussen oder zu prägen."[28]

Clausewitz sieht die physische Gewalt als Mittel, um dem Feind den eigenen Willen aufzuzwingen. Die Fachliteratur unterscheidet verschiedene Arten von Gewalt: *physische*, *psychische*, *institutionelle*, *strukturelle* und *kulturelle* bzw. *symbolische* Gewalt[29]. Dabei zielt nach Bonacker und Imbusch die direkte *physische Gewalt* auf Schädigung, Verletzung oder Tötung anderer Personen ab, während sich die *psychische Gewalt* auf Worte, Bilder, Symbole, Einschüchterung und Angst abstützt.[30] *Institutionelle Gewalt* intendiert hingegen dauerhafte Abhängigkeits- und Unterwerfungsverhältnisse[31], was mit Soft Power zu vergleichen ist. „Prototyp institutioneller Gewalt in der Moderne ist der Hoheits- und Gehorsamsanspruch, mit dem der Staat dem Einzelnen gegenübertritt."[32] Gewalt wird dabei von staatlichen Sicherheitsinstitutionen ausgeübt. Bonacker und Imbusch schließen in ihrer Kategorisierung Galtungs Begriff zu *struktureller Gewalt* ein, was der Vollständigkeit halber erwähnt wird. Gewalt ist in der sozialen Struktur einer Gesellschaft immanent und stets präsent. Vereinfacht gesagt handelt es sich dabei um eine Ausprägungsform der sozialen „Ungerechtigkeit"[33].

---

28 Schmidt Wolfgang: Wörterbuch zur Politik. Stuttgart 1995, S. 367.

29 Vgl. Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden. In: Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung. Wiesbaden 2006, S. 86.

30 Ebd., S. 86f.

31 Ebd., S. 87.

32 Waldmann, Peter: Politik und Gewalt. In: Nohlen, Dieter/Schultze, Rainer-Olaf (Hrsg.): Politische Theorien, München 1995, S. 431. Zitiert nach: Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden. In: Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung. Wiesbaden 2006, S. 87.

33 Galtung, Johann: Gewalt, Frieden, Friedensforschung. In: Senghaas, Dieter (Hrsg.), Kritische Friedensforschung, Frankfurt am Main 1971, S. 62. Zitiert nach: Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden. In: Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung. Wiesbaden 2006, S. 88.

Bonacker und Imbusch verwenden auch Galtungs Begriff der *kultureller Gewalt*. Darin sind jene Aspekte von Kultur enthalten, „[...] die zur Rechtfertigung oder zur Legitimierung direkter, illegitimer, institutioneller oder struktureller Gewalt benutzt werden können“[34]. Bei *symbolischer Gewalt* wird Gewalt als sprachliches beziehungsweise kulturelles Ausdrucksvermögen begriffen.[35] Darunter fällt z.B. Beschimpfung, Diskreditierung, Demütigung oder Rufmord. Obwohl Bonacker/Imbusch sich auf den Menschen beziehen, wird diese Form der Gewalt nicht in Hinblick auf eine Gesellschaft, eine ethnische, religiöse oder andere Gemeinschaft behandelt. Der Unterschied zur *psychischen Gewalt* liegt eher in deren Zielsetzung. Während *psychische Gewalt* auf Einschüchterung und Angst abzielt, spielt bei der *symbolischen Gewalt* die Herabsetzung des Gegenübers eine entscheidende Rolle.

Anwendung von Gewalt kann daher zweierlei Ziele verfolgen. Entweder wird Gewalt zur Erringung oder zum Erhalt von Macht angewandt. Dies leitet zum Begriff der *Macht* über.

1.2.8 Macht

Als Macht bezeichnet der U.S.-Amerikaner Robert Kagan „[...] die Fähigkeit, andere zu veranlassen, das zu tun, was man will, und sie von dem, was man nicht will, abzuhalten.“[36] Dabei muss nicht immer Gewalt angewandt werden. Die Ausübung von Macht, insbesondere durch den Einsatz anderer als militärischer Mittel – durch hybride Methoden – spiegelt sich in der Sicherheitsstrategie der Veriningten Staaten von Amerika (USA) wider: „While the use of force is sometimes necessary, we will exhaust other options before war whenever we can, and carefully weigh the costs and risks of action against the costs and risks of inaction.”[37] Joseph Nye definiert Macht als die Möglichkeit, das Verhalten

---

34 Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden. In: Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung. Wiesbaden 2006, S. 89.

35 Ebd., S. 89.

36 Kagan, Robert: Die Demokratie und ihre Feinde. Wer gestaltet die neue Weltordnung? München 2008, S. 20.

37 President of the United States: National Security Strategy. Washington Mai 2010, S. 22. <http://nssarchive.us/NSSR/2010.pdf>, abgerufen am 17.06.2013.

anderer zu Gunsten des eigenen Vorteils zu beeinflussen.[38] Macht kann, so Nye, dann ausgeübt werden, wenn man im Besitz erforderlicher Möglichkeiten oder entsprechender Ressourcen ist, um angemessenen Einfluss auszuüben.[39] Somit kann eine Bedrohung lediglich von jenen Akteuren ausgehen, die neben dem Willen auch die notwendigen Mittel besitzen, um Macht anzuwenden. Für Nye kann – wie bereits angemerkt – Macht durch zweierlei Bereiche ausgeübt werden: durch Hard und Soft Power. Später kommt bei Nye eine Dritte hinzu, die eine Mischung aus den erwähnten darstellt: Smart Power. Hard Power beschreibt Nye als eine Anreiz/Drohungs-Taktik („Karotte und Stock")[40], während Soft Power als Überzeugungsarbeit zum Streben nach als ideal angesehenen Werten beschrieben werden kann. Soft Power wird erfolgreich angewendet, wenn ein Akteur von den eingesetzten Argumenten überzeugt wird und diesen nacheifert, was sich in Robert Kagans Definition widerspiegelt. Soft Power beruht auf kulturellen und politischen Idealen sowie auf Außenpolitik, wenn diese als legitim angesehen wird, so Nye. Smart Power hingegen ist „[...] the ability to combine hard and soft power into a successful strategy."[41]

1.2.9 Hybride versus bisherige Kriegführung

Inwiefern geht nun hybride Bedrohung über bisherige Bedrohungsbilder hinaus? Die Hybridität als Distinktionsmerkmal muss sich folglich von anderen Bedrohungsbildern abheben, wenn das Konzept nicht zu einer inhaltslosen Begriffsverwirrung verkommen will. Daher sind hybride Bedrohungen von anderen Konfliktbildern, wie dem konventionellen, dem totalen und dem asymmetrischen Krieg, abzugrenzen.

---

38 Vgl. Nye, Joseph S. Jr.: Soft Power. The Means to Success in World Politics. PublicAffairs 2004, S. 2.

39 Ebd., S. 3.

40 Ebd., S. 5.

41 Nye, Joseph S. Jr.: Smart Power. The Blog. <http://www.huffingtonpost.com/joseph-nye/smart-power_b_74725.html>, abgerufen am 29. September 2014.

Hybride Bedrohungen versus konventioneller Krieg

Konventioneller Krieg ist „[...] kollektive organisierte Gewalt unter Einschluss des Staates“[42], insbesondere Armeen, die in einer „offenen“ Schlacht gegen Streitkräfte anderer Staaten kämpfen. Die Gewalttätigkeit als wesentliches Charakteristikum von Kriegen findet sich im Synonym „bewaffnete Konflikte“.

Bei hybrider Bedrohung muss nicht zwangsläufig Waffengewalt eingesetzt sein. Sie kann sich durchaus ohne physische Gewaltanwendung zeigen, muss aber eine Kombination von nicht-gewalttätigen Praktiken mit beinhalten, um als hybride Bedrohung eingestuft zu werden.

Hybride Bedrohungen versus totale Kriege

In einem totalen Krieg kommt es, unter einer zentralisierten Verwaltung und straffen Organisation, die die militärische Schlagkraft maximieren soll, zum Einsatz aller Mittel. Eine größtmögliche Anzahl an Menschen wird mobilisiert, um mit Soldaten einerseits und der Waffen- und Versorgungsgüterproduktion andererseits am Krieg teilzunehmen. Hauptzweck des totalen Krieges ist die Entfaltung maximaler militärischer Gewalt, um den Gegner zu besiegen beziehungsweise physisch auszuschalten. Der totale Krieg strebt einen Sieg als Ziel an, welches in der Ausschaltung des Gegners besteht. Er verabsolutiert sich von seinem politischen Zweck und läuft Gefahr in einer unheilvollen Eigendynamik überzuschwappen. Im totalen Krieg ersetzt die „Grammatik des Krieges die Logik der Politik“[43]. Militärische Übermacht steht einer politischen Ohnmacht gegenüber.

Hybride Bedrohungen haben insofern eine Ähnlichkeit mit dem totalen Krieg, als dass mehrere Instrumente (Wirtschaft, öffentliche und veröffentlichte Meinung, Gesetzgebung, etc.) zur Schädigung eines Gegners eingesetzt werden. Konfliktakteure, die planen, eine Kontroverse auf hybride Weise auszutragen,

---

42 Vgl. Bonacker, Thorsten/Imbusch, Peter: Zentrale Begriffe der Friedens- und Konfliktforschung: Konflikt, Gewalt, Krieg, Frieden. In: Imbusch, Peter/Zoll, Ralf (Hrsg.): Friedens- und Konfliktforschung. Eine Einführung. Wiesbaden 2006, S. 107ff.

43 Hofmeister, Heimo: Theorie des Terrorkrieges. In Gustenau, Gustav (Hrsg.): Zur Theorie des Terrorismus (4/02). Wien 2002, S. 10.

laufen Gefahr, dass sich durch Gegenreaktionen der Konflikt aufschaukelt (z.B. durch Multiplikatoreffekte[44]) und damit verschärft. Im Gegensatz zum totalen Krieg zielen hybride Bedrohungen nicht auf eine vollständige Vernichtung des Gegners und die Auslöschung von lebensnotwendigen Strukturen ab. Vielmehr sind hybride Bedrohungen als Überforderungsstrategien auf verschiedenen Ebenen in mehreren Bereichen zu werten, die insgesamt zu einem multiplen Institutionenversagen führen.

Hybride Bedrohungen versus asymmetrische Kriege

Symmetrische Kriege (auch als „westfälische Kriege" bezeichnet) sind bewaffnete Konflikte zwischen zwei homogenen Gewaltakteuren. Dabei stehen sich zwei Gewaltakteure gegenüber, die hinsichtlich ihres rechtlichen Status, der Ausbildung ihrer Streitkräfte, der verwendeten Technologie, den eingesetzten Taktiken gleich – kurzum: symmetrisch – aufgestellt sind. Ein Merkmal der Symmetrie liegt in der Ausübung militärischer Operationen, die einem speziellen Berufsstand vorbehalten ist, deren Angehörige als Kombattanten gelten.

Asymmetrische Kriege hingegen sind von einer Entschleunigung der Konfliktdynamik, der Heterogenität der Akteure und einer normativen Ungleichheit[45] gekennzeichnet. Asymmetrische Kriegsführung wird von unterschiedlichen Akteursgruppen bestimmt. Diese können von konventionellen Streitkräften über paramilitärische Freiwilligenverbände, private Militärdienstleister bis zu organisierten kriminellen und transnational agierenden Terroristen reichen. Die Unterscheidung zwischen Kombattant und Nicht-Kombattant, sowie zwischen Front und Hinterland verschwimmt.

Hybride Bedrohungen können sich in Teilbereichen mit asymmetrischer Kriegsführung überlagern. Ein asymmetrisch agierender Gewaltakteur kann zum Ausgleich seiner z.B. militärischen Unterlegenheit mehrere andere Mittel in verbundener Weise auf unterschiedlicher Ebene (sprich hybrid) gegen einen Zielstaat einsetzen. Der Initiator einer solchen Bedrohung wird also seine Angriffe gegen

---

44 Nähere Erklärung dazu siehe in diesem Beitrag weiter unten.

45 Erklärung: Während sich staatliche Streitkräfte eines Rechtsstaates an das Humanitäre Völkerecht zu halten haben, fühlen sich eventuell Kämpfer eines nicht-staatlichen Akteurs eventuell kaum daran gebunden.

Bereiche richten, in denen ein signifikantes Ungleichgewicht der Kräfte und Ressourcen zu seinen Gunsten vorliegt (was einer militärischen Taktik ähnelt). Er wird Operationen in physischen und virtuellen Räumen ausführen, in denen er bei geringstem Ressourceneinsatz die erhoffte Wirkung erzielt. Technische Überlegenheit ist ein Stützpfeiler in dieser asymmetrischen Kriegsführung.

1.2.10 Hybride Bedrohungsfaktoren

Die Möglichkeiten einen Staat zu beeinflussen sind vielfältig. Sie erhöhen sich mit der Komplexität von Abläufen und dem technologischen Fortschritt. Hybridität stellt kein neues Phänomen dar. Neue Herausforderungen ergeben sich jedoch durch gegenwärtige Technologien und moderne Kommunikationsstrategien, verbunden mit globaler Vernetzung. Letztere ermöglicht einem Akteur eine bisher unbekannte Vielfalt von Mitteln und Methoden zur Beeinflussung eines Gegenübers.

Neben den positiven Aspekten, welche neue Technologien für Gesellschaften mit sich bringen (z.B. im Cyberbereich durch interdisziplinäre Vernetzungen), ergeben sich auch negative Wechselwirkungen. Erst der Ausfall und damit das Fehlen einzelner Technologiebereiche zeigt z.B. die Abhängigkeit und schließlich die Verletzbarkeit unserer Infrastruktur. Fällt ein System aus, treten Folgewirkungen lawinenartig, mit teils dramatischen Auswirkungen, zu Tage. Der gegenwärtig vielzitierte *Black Out* im Bereich der Stromwirtschaft gilt als bestes Beispiel. Besonderes Kennzeichen dabei: Ein weitreichender Stromausfall muss nicht ausschließlich durch technisches Gebrechen zustande kommen. Dies kann ebenso infolge einer von Menschenhand herbeigeführten Ursache, wie z.B. in Form eines technischen „Fehlers" in der Ausrüstung, erfolgen. Spezifikum dabei: die körperliche Anwesenheit des Saboteurs ist nicht mehr an den Anschlagsort gebunden – Attacken können aus Distanz über den Cyberraum erfolgen. Von langer Hand geplante Angriffe mit zeitlich abgestimmten Abläufen inklusive ähnlicher Vorgehensweisen wie beispielsweise beim Computerschädling *Stuxnet*[46] sind vorstellbar. Vergleichbare Vorfälle sind für die gesamte auf Informations-Technologie (IT) basierende Infrastruktur nicht auszuschließen.

---

[46] Bei *Stuxnet* handelte es sich um einen Computer-Wurm, der auf hoch spezialisierte Industrieanlagen in kritischen Infrastrukturen abzielte. (Siehe Karnouskos, Stamatis:

Globalisierung verpflichtet zum verantwortungsvollen Agieren insbesondere in sicherheitspolitischen Belangen. Beiträge zur Durchführung eines staatlichen bzw. internationalen Konflikt- und Krisenmanagements (IKKM) stellen hierzu ein wesentliches Element dar. Damit soll nicht nur Sicherheit in Konfliktzonen geschaffen, sondern auch Rückwirkungen auf den eigenen Staat verringert und im besten Fall verhindert werden. Die größte Herausforderung dabei ist die zunehmende Zahl an Protagonisten neben Mitteln und Methoden. Die Konflikte in Syrien oder in der Ostukraine verdeutlichen dies. Regulären Sicherungskräften stehen vermehrt Kämpfer nicht-staatlicher Akteure wie etwa von national radikalen religiösen Gruppierungen, verschiedenen ethnischen Milizen, Guerillas, Söldnern, ideologisch überzeugten Unterstützern und Angehörigen anders-staatlicher Streitkräfte ohne entsprechender Kennzeichnung gegenüber. In solchen Situationen kann von einem Gewaltmonopol keine Rede sein. Vielmehr ist es naheliegend von einem „Gewaltoligopol“[47] und in weiterer Folge gar von einem „Gewaltpolypol“ zu sprechen. Diese Zustände beschreibt eine deutsche Tageszeitung im Juni 2014:

> „Besonders alarmiert ist die Nato durch die neu entwickelte „Subversionsstrategie“[48] Russlands. Sie wird bisher intern als „hybride Kriegsführung“ bezeichnet. Laut Nato-Analysen besteht die neue militärische Taktik Moskaus darin, bestimmte Gebiete mit Militärexperten – im Nato-Jargon „kleine grüne Männchen“ genannt – zu infiltrieren, die Aufständische wie jene in der Ostukraine beraten, aufwiegeln und im Gebrauch von militärischem Gerät schulen.“[49]

Im Artikel wird ein hoher NATO-Offizier mit den Worten „Sie destabilisieren, ohne selbst einen regulären Schuss abzugeben“[50] zitiert. Demzufolge etabliert

---

Stuxnet Worm Impact on Industrial Cyber-Physical System Security. SAP Research, Germany. <http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf>, abgerufen am 18.02 2015.

47 Gewaltoligopol ist als Gegenbegriff zum Gewaltmonopol zu verstehen. „Sicherheit“ wird grundsätzlich vom Staat gewährleistet während insbesondere in Krisenregionen oftmals mehrere Gruppierungen ihrem Klientel gegenüber postulieren für deren Sicherheit zu sorgen.

48 Schlitz, Christoph B.: Die Nato zittert vor Russlands neuer Strategie. In: Die Welt, 25.06.2014. <http://www.welt.de/politik/ausland/article129431400/Die-Nato-zittert-vor-Russlands-neuer-Strategie.html>, abgerufen am 26.06.2014.

49 Ebd.

50 Ebd.

sich eine Form der psychologischen Kampfführung gepaart mit Unterstützungsmaßnahmen wie z.B.: Militärische Ausbildung und Unterweisung, Materialbereitstellung, mediale Propagandaunterstützung und/oder der „Zurverfügungstellung" subversiver Kräfte. Diese Methode ist durchaus geläufig und wurde in ähnlicher Form von westlichen Mächten bereits eingesetzt. So wurde z.B. von Gert Sommer in einem Buchbeitrag berichtet: „Offiziell begann der Libyen-Krieg zwei Tage nach der Vereinten Nationen (UNO) Resolution 1973 (17.03.2011). Die direkten Vorbereitungen für diesen Krieg begannen aber anscheinend früher."[51] Sommer bezieht sich dabei auf einen Bericht des britischen Sunday Mirror vom 23. März 2011, wonach „Hundreds of British soldiers have been operating with rebel groups inside Libya for three weeks"[52].

Diese Methode stellt somit eine neue Qualität dar, weil freiwillige Kämpfer durch einen anderen Staat organisiert werden, was offiziell allerdings geleugnet wird. Damit verschwimmt eine klare Differenzierung zwischen Freund und Feind bzw. zwischen Kombattant und Nicht-Kombattant.

Noch schwieriger fällt diese Differenzierung bei Cyberattacken aus. Dabei ergibt sich nicht nur die Herausforderung der territorialen Ortung des Ausgangspunktes von Angriffen, sondern auch bei der Zuweisung zu einem determinierten Akteur. Sollte der Ursprung des Anschlags tatsächlich rückverfolgbar sein, stellt sich dennoch die Frage, ob dieser Akteur in Wahrheit Urheber der Aktivität ist. Oder stützt sich ein anderer Akteur lediglich auf dessen Infrastruktur ab? Dadurch wird die Analysearbeit sicherheitspolitischer Experten erschwert, ebenso wie entsprechende Gegenreaktionen. Gerade bei der Cyberproblematik stellt sich die Frage, ab welcher Ebene Staaten für deren Verteidigung zu sorgen haben, um als sicherheitspolitisch verlässlicher Partner zu gelten. Werden vom Territorium eines Staates durch einen Akteur Cyberattacken gegen einen ande-

---

51 Sommer, Gert: Der Libyen-Krieg: Reflektionen zu Gaddafi und anderen Beteiligten. In: Becker, Johannes M./Daxner, Michael und Sommer, Gert (Hrsg.): Der Libyen-Krieg. Das Öl und die „Verantwortung zu schützen". In: Schriftenreihe zur Konfliktforschung, Band 26. Berlin 2013, S. 206 .

52 The Mirror: Crack SAS troops hunt Gaddafi weapons inside Libya. 20.03.2011. <http://www.mirror.co.uk/news/uk-news/crack-sas-troops-hunt-gaddafi-117405>, abgerufen am 19.01.2015. In: Sommer, Gert: Der Libyen-Krieg: Reflektionen zu Gaddafi und anderen Beteiligten. In: Becker, Johannes M./Daxner, Michael und Sommer, Gert (Hrsg.): Der Libyen-Krieg. Das Öl und die „Verantwortung zu schützen". In: Schriftenreihe zur Konfliktforschung, Band 26. Berlin 2013, S. 206.

ren Staat ausgeführt, stellt sich die Frage, ob in Zukunft eine Regelung von Nöten sein wird, der zufolge der Staat, von dessen Territorium aus die Attacke geführt wird, aufgrund seiner zu geringen Absicherungsmaßnahmen zur Verantwortung zu ziehen ist.

Ähnliche Herausforderungen ergeben sich bei sozialen Netzwerken wie z.B. Facebook und Twitter. Diese nehmen gegenwärtig einen zentralen Platz in der Informationsweitergabe (Kenntnisstand) über eine Krisenregion ein. Die weitreichenden Zugangsmöglichkeiten zu verschiedenen sozialen Medien durch nahezu jede Nutzerin und jeden Nutzer bieten auch Gelegenheiten für Propagandamaßnahmen. Medienmeldungen, wonach Konzerne für eine positive Darstellung in verschiedenen Online-Foren bezahlt haben[53], geben Einblicke in entsprechende Möglichkeiten. Daraus ergeben sich in moralischer und rechtlicher Hinsicht enorme Herausforderungen wie z. B.: Werden über Online-Medien bewusst Informationen lanciert, um von Staaten ein politisches Handeln einzufordern? Müssen/Dürfen infolgedessen Staaten auf soziale Netzwerke Einfluss nehmen, um entsprechend gegenzusteuern? Sind Staaten für die instrumentalisierte Verbreitung radikaler Propaganda und Falschmeldungen über Server, die sich auf deren Staatsgebieten befinden, verantwortlich und somit haftbar? Das zunehmende Aufkommen von Tablets und Smartphones steigert signifikant diesbezügliche rechtliche Herausforderungen und könnte so insbesondere auf intra-staatliche Konflikte Einfluss nehmen. Für den Beobachtungszeitraum 2013 zeigt das Konfliktbarometer des Heidelberger Instituts für Internationale Konfliktforschung (HIIK) in ihrer Studie 414 Konflikte[54], wovon 337 sogenannten „intrastate conflicts" und lediglich 77 „interstate conflicts" zuzuordnen waren. Könnten zukünftig Cybermöglichkeiten diese Konflikte verstärken bzw. deren Anzahl erhöhen?

---

53 ÖBB, ÖVP und Bank Austria zahlten für positive Internet-Forenbeiträge. In: Die Presse Online. 06.11.2014. <http://diepresse.com/home/techscience/internet/4587699/OBB-und-Bank-Austria-zahlten-fur-positive-InternetForenbeitraege>, abgerufen am 10.11.2014.

54 Heidelberg Institute for International Conflict Research (HIIK): Conflict Barometer 2013. Februar 2014. <http://hiik.de/de/downloads/data/downloads_2013/ConflictBarometer2013.pdf>, abgerufen am 10.04.2014.

1.2.11 Allgemeine Überlegungen zu „Hybride Bedrohungspotentialen und daraus resultierende sicherheitspolitische Ableitungen für Kleinstaaten"

Das neue Informationszeitalter bietet eine Reihe außergewöhnlicher Perspektiven, die vor einigen Jahren als schier unmöglich galten. Die rasante Verbreitung von Smartphones mit ihren technischen Möglichkeiten wie z.B. der Global Positioning System (GPS)-Verfolgung, Speicherung und Versendung von Film-, Fotomaterial bzw. Informationen lassen eine nahezu verzugslose weltweite Informationsbereitstellung verschiedenster Aktivitäten durch jeden Nutzer und Nutzerin zu. Als Beispiel ist die U.S. Spezialoperation zur Ergreifung Osama Bin Ladens im Mai 2011 zu nennen, bei welcher der Helikoptereinsatz in Abbottabad, Pakistan, von einem Twitter-User in Realzeit online gestellt wurde[55]– allerdings ohne zunächst einen Zusammenhang mit Al Qaida und Osama Bin Laden herstellen zu können.

Als weiteres Beispiel dienen gepostete Opferzahlstatistiken oder Durchhalteparolen. „Spiegel Online" berichtete von syrischen Oppositionsgruppen, die über Twitter von mehr als 650 Todesopfern aufgrund eines Chemiewaffeneinsatzes schilderten.[56] Da derartige Informationen im rasanten Medienzeitalter schwer überprüfbar sind, könnten sie zu politischen Fehlinterpretationen und staatlichen Überreaktionen führen.

Durch ähnliche Meldungen ergibt sich eine weitere Herausforderung: Die Überprüfbarkeit des Wahrheitsgehalts von Internetmeldungen, woraus sich – bei entsprechender Intention – eine Bedrohung ergeben kann.

Eine andere analoge – im hybriden Bereich angesiedelte – Bedrohung ergibt sich aus der Veröffentlichung eines angeblichen Fehlverhaltens durch staatliche Sicherheitsakteure. So wurden persönliche Daten betreffend der Protagonisten, inklusive Daten von deren Familienangehörigen, verbreitet. Der Zweck dieser

---

55 Siehe hiezu Osama bin Laden killed: Pakistani man live tweets deadly raid. In: The Telegraph, 02.05.2011.<http://www.telegraph.co.uk/technology/twitter/8487686/Osama-bin-Laden-killed-Pakistani-man-live-tweets-deadly-raid.html>, abgerufen am 29.09.2014.

56 Reuter, Christian: Bürgerkrieg in Syrien: Aktivisten werfen Assad Giftgaseinsatz mit Hunderten Toten vor. In: Spiegel Online, 21.08.2013. <http://www.spiegel.de/politik/ausland/aktivisten-in-syrien-neuer-giftgasangriff-von-assads-armee-a-917699.html>, abgerufen am 09.10.2014.

Aktivitäten – die Daten wurden in einer Art Steckbriefform in Umlauf gebracht – kann als Aufforderung zu Lynch- oder Selbstjustiz oder zur Bloßstellung der handelnden Person gewertet werden. Als Beispiel dient der Pfefferspray-Einsatz eines Polizisten bei der sogenannten Occupy-Protestaktion in New York.[57] Die Personalien dieses Ordnungshüters wurden von der *Anonymous*-Gruppierung im Internet verbreitet. Er wurde beschuldigt, den Reizstoff gegen eine friedliche Demonstrantin eingesetzt zu haben. In ähnlicher Art und Weise veröffentlichte 2011 *Anonymus* persönliche Daten (Name, Adresse, Geburtsdaten) von 25.000 österreichischen Beamten des Innenministeriums über einen Twitter-Account.[58] Generell ist nicht auszuschließen, dass bei einer hybriden Machtprojektion mittels medialer Mittel bewusst Druck auf Sicherheitskräfte/Sicherheitsministerien und Politiker ausgeübt wird.

Ein weiterer Aspekt in gegenwärtigen und zukünftigen hybriden Bedrohungsszenarien ist die immer einfachere Übertragung digitalisierter und als „Geheim" klassifizierter Informationen an nicht autorisierte Personen oder Institutionen. Die Veröffentlichung von Geheiminformationen wie z.B. durch Wikileaks oder den U.S. Amerikaner Edward Snowden Anfang 2013 demonstrieren, inwieweit in der gegenwärtigen IT-Welt Einzelpersonen in bereits unteren und mittleren Führungsebenen Zugang zu umfassendem Geheimwissen erlangen und sie auch entsprechend nützen. Derartige, mit anderen hybriden Taktiken orchestrierte Veröffentlichungen könnten in sicherheitspolitischer Hinsicht eminente Auswirkungen auf einen Staat haben.

Auch in der EU werden offensichtlich Methoden von Soft- und Hard Power zur Durchsetzung politischer Zielsetzungen – bewusst oder unbewusst – angewandt. Als die Schweiz ihre Personenfreizügigkeit nicht auf Kroatien ausdehnte, reagierte im Februar 2014 die EU und kündigte der Schweiz den Zugang zum

---

57 McVeigh, Karen: Occupy Wall Street activists name officer over pepper spray incident. In: The Guardian, 26.09.2011.<http://www.theguardian.com/world/2011/sep/26/occupy-wall-street-police-named>, abgerufen am 30.09.2014.

58 Proschofsky, Andreas: Anonymous veröffentlicht Daten von Polizisten. In: Der Standard Online, 26.09.2011. <http://derstandard.at/1317018455940/Pwnyzei-Anonymous-veroeffentlicht-Daten-von-Polizisten>, abgerufen am 30.09.2014.

EU-Forschungsprogramm „Horizon 2020“ sowie das Studentenaustauschprogramm Erasmus auf.[59]

Aus den genannten Beispielen ist ersichtlich, dass für entsprechende Gegenmaßnahmen im gesamten Spektrum der hybriden Bedrohungen spezielle Methoden erforderlich sind, um weder taktisch, operativ, noch strategisch ins Hintertreffen zu geraten.

1.2.12 Akteure, Zielsetzung und Methoden bei Hybriden Bedrohungen

In diesem Abschnitt werden die einzelnen Elemente der Definition der Hybriden Bedrohung näher kommentiert.

(1) Gefährdung eines Staates oder eines Staatenbündnisses

Methoden einer hybriden Bedrohung zielen auf die Verwundung substanzieller Schutzgüter eines Staates ab. Neben der territorialen Integrität und der politischen Souveränität zählen dazu auch ein funktionierendes Wirtschaftsleben, der soziale Frieden und die öffentliche Ordnung.

Territoriale Integrität bezieht sich auf die Achtung des Staatsgebietes und geht über den physischen Lebensraum hinaus. Zum Staatsgebiet zählen Landgebiete, Gewässer, küstennahe Meeresabschnitte und der Luftraum. Ungeklärt ist, ob und inwiefern der Cyberraum – der fünfte Raum – zum Staatsgebiet hinzugerechnet werden muss. Kann ein Angreifer den virtuellen Cyberraum eines Staates und damit die territoriale Integrität überhaupt verletzen? Unter politischer Souveränität lässt sich die Willensbildungsfreiheit und Willensäußerungsfreiheit der politischen Gemeinschaft verstehen. Sind beispielsweise Störungen von Wahlen und Volksabstimmungen durch die Verbreitung falscher Nachrichten, die geeignet sind, den Wahlausgang zu beeinflussen, als Angriffe auf die öffentliche Willensbildungsfreiheit und damit auf die politische Souveränität (Propa-

---

[59] Studenten und Forscher fordern Beteiligung an EU-Programmen. In: Online Tagesanzeiger, 04.03.2014. <http://www.tagesanzeiger.ch/wissen/bildung/Studenten-und-Forscher-fordern-Beteiligung-an-EUProgrammen/31353020/print.html>, abgerufen am 30.09.2014.

gandaschlacht) zu verstehen? Ebenso sind der Aufbau und die Förderung der bewaffneten Opposition oder lokaler Sezessionsbewegungen als Gefährdung des Staates zu werten.

Aber wie sieht es mit dem Umfang und der Intensität solcher Bedrohungen aus? Nicht jede Drohgebärde ist sicherheitspolitisch relevant. Ergo muss eine *strategische Schwelle* für Bedrohungshandlungen überschritten werden. Dies kann nur dann der Fall sein, wenn der Staat in seiner Handlungs- und Entscheidungsfreiheit in substanzieller Weise eingeschränkt wird. Es ist davon auszugehen, dass derartige intensive Bedrohungen gegen substantielle staatliche Schutzgüter, die Bewältigungskapazitäten eines einzigen Staatsressorts übersteigt, was den Ruf nach Kooperation erhöhen würde.

(2) Wer ist der Akteur einer hybriden Bedrohung?

Eine hybride Bedrohung kann grundsätzlich sowohl von einem Staat als auch einem nicht-staatlichen Akteur ausgeübt werden. Als Beispiele für letztere dienen sowohl Terrororganisationen als auch transnational operierende Konzerne. Dabei muss der Akteur das entsprechende Vermögen (Fähigkeiten, Ressourcen, Wissenskomponente, objektives Element) und die Intention (Politik, Willenskomponente, subjektives Element) zu solch einer bewussten Handlung zum Ausdruck bringen. Somit ist eine hybride Bedrohung rein auf einen Akteur bezogen und von anderen Risikoquellen, wie z.B. Klimawandel, Überalterung, Staatsfragilität, Migration, etc. abzugrenzen.

Wie eingangs beschrieben, ist für den Einsatz einer hybriden Bedrohung eine Kombination zweier Komponenten nötig: einerseits die Fähigkeit und andererseits der Wille zum Einsatz bestimmter Mittel und Methoden. Fehlt einer dieser Bausteine, liegt keine hybride Bedrohung vor. So kann zwar ein Staat die Fähigkeiten und organisatorischen Voraussetzungen (Ressourcen, Personal, Finanzierung, Kooperationsmechanismen, Entscheidungsregeln etc.) aufbauen, fehlt jedoch die Absicht, diese Fähigkeit gegen einen anderen Staat einzusetzen, kann nicht von einer „Bedrohung“ gesprochen werden. Im Gegenzug könnte ein Staat die Absicht verfolgen, koordinierte Mittel gegen einen anderen Staat einzusetzen. Fehlt ihm jedoch die Fähigkeit dazu, liegt ebenfalls (noch) keine hybride Bedrohung vor. Die Absicht wird, abhängig vom jeweiligen Akteur, als „frommer Wunsch“ oder als konkretes Vorbereitungsstadium zu bewerten sein. In

diesem Zusammenhang sind ebenso Konzerne als nicht-staatliche Akteure mit entsprechendem Machtpotential zu nennen. Denkbar wäre, dass private Konzerne einerseits eigenständige Machtinteressen verfolgen, andererseits vom Staat politische Zielvorgaben erhalten.

Die nachfolgende vom Projektteam erarbeitete Übersicht dient der vereinfachten Darstellung offensiver und defensiver Akteure bei hybriden Bedrohungen und den jeweiligen Mitteln und Methoden. Dieser Bedrohung werden mögliche staatlich aktive Defensivkräfte gegenübergestellt.

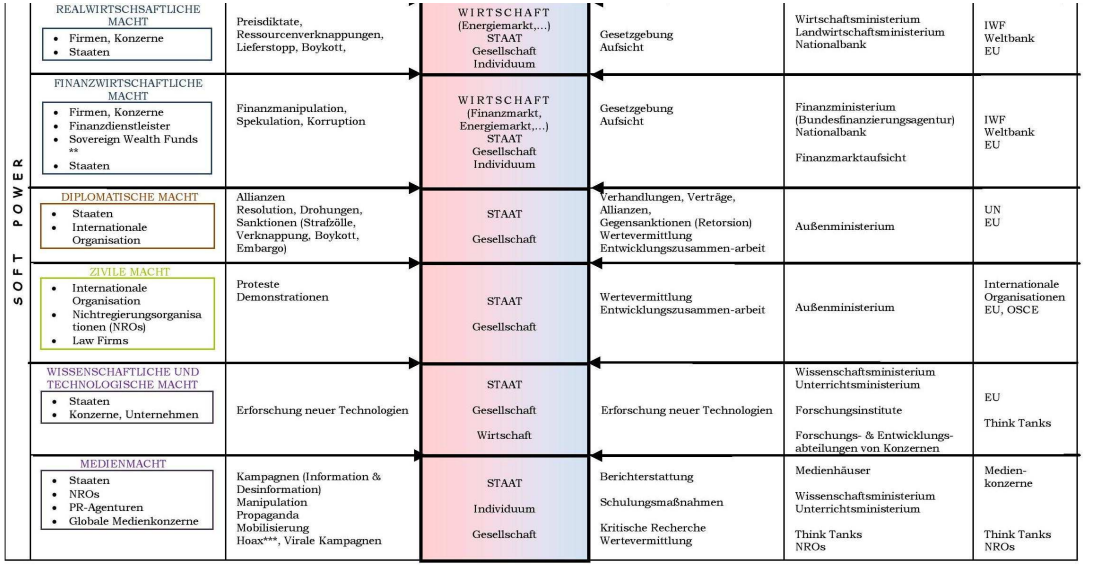
Dabei ist zu bedenken, dass mehrere Protagonisten bei hybriden Bedrohungen unterschiedlich auftreten können und – wie eingangs dieser Arbeit bei der Arbeitsdefinition erwähnt – zumindest zwei staatliche Akteure auf der Defensivseite involviert sein müssen, damit von hybrider Bedrohung gesprochen werden kann. Zu erwähnen ist, dass diese Übersicht nicht als abgeschlossene Akteursdarstellung zu betrachten ist, sondern lediglich als Hilfestellung bei der Analyse einer hybriden Bedrohung dient.

Abbildung 3: Akteurs-Übersicht *Michael Schurian*

Beilage ./**A** **Akteurs-Übersicht** Stand: 26.06.2015

Hybride Bedrohung

	Offensivakteure	**Offensive Mittel und Methoden (Beispiele)**	**Bedrohungsobjekte**	**Defensiv- und Präventivmittel und -methoden (Beispiele)**	**Defensivakteure**	
					national	**inter-national**
	Gleichzeitiges, systematisches, zielgerichtetes Zusammenwirken		RAUM, Dimension		Gleichzeitiges, systematisches, zielgerichtetes Zusammenwirken	
HARD POWER	STAATSGEWALT • Land-, Luft-, See-, Weltraum- und Spezialstreitkräfte • Polizei, Spezialeinsatzkräfte • Nachrichtendienste • Justiz	Militärische Operationen ABC-Waffen Putsch* Überwachung, Kontrolle, Ordnung, Ermittlung, Festnahme, Verwahrung Aufklärung/Spionage, Manipulation, Sabotage Strafverfolgung, Verurteilung, Strafvollzug	STAAT Individuum Gesellschaft	Militärische Operationen, Verteidigung, PsyOps, Sicherungsmaßnahmen, Kontrolle, Herstellen der Ordnung, Ermittlung, Verwahrung Informationsgewinnung, Analyse, Beratung, Abwehr Strafverfolgung, Verurteilung, Strafvollzug	STAATSGEWALT • Verteidigungsministerium (Streitkräfte, Abwehramt) • Innenministerium (Polizei, Spezialeinsatzkräfte) • Nachrichtendienste • Justiz, Justizwache	NATO Interpol, Europol Eurojust UN EU
	CYBERGEWALT • Hacker, Cracker • O.K. („Phishing"), • Staatliche Institutionen	Datenüberwachung, Datenmanipulation, Sabotage	STAAT Gesellschaft Wirtschaft	Gesetzgebung Spezialsoftware Ausbildung von Experten Schulungen	CYBERGEWALT • Staatliche Sicherheitskräfte • Infrastruktur-Ministerium • Wissenschafts-Ministerium • Unterrichts-Ministerium • IT-Unternehmen	Interpol, Europol EU
	PRIVATISIERTE GEWALT • O.K. (Mafia, Schlepper) • Söldner, Private Militär- & Sicherheitsfirmen • Milizen (War Lords) • Piraten	Illegaler Handel Korruption Sabotage, Anschläge, Tötung Kaperung, Geiselnahmen, Erpressung	STAAT Individuum Wirtschaft	Überwachung, Kontrolle, Ermittlung, Festnahme, Verwahrung, Analyse, Beratung militärische Operationen polizeiliche Maßnahmen Informationspolitik	Innenministerium Verteidigungsministerium Bundeskanzleramt Medien	Interpol, Europol NATO EU
	VOLKSGEWALT • Extremisten (pol./rel./ethn.) • Aufständische, Revolutionäre • Rebellen, Unzufriedene, Sozial Benachteiligte, Armutsgefährdete, Marginalisierte	Verhetzung, Demonstrationen, Gewalttätige Unruhen, Aufstand, Revolution Rebellion Social Media	STAAT Gesellschaft Individuum	Aufklärung, Wertevermittlung Bildungsarbeit Gesetzgebung, Kontrolle, Überwachung, Festnahme Sozialpolitik, Integration	Innenministerium (Verteidigungsministerium) Sozialministerium Unterrichtsministerium NROs Zivilgesellschaft	OSCE EU Kirchen NROs
	TERRORGEWALT • Terroristen • Terrororganisation/ -gruppierungen (pol./rel./ethn.)	Anschläge, Tötungen Massenvernichtungswaffen ABC-Waffen Korruption	STAAT, Individuum Gesellschaft Wirtschaft	Observation, Militär. Operationen, Strafverfolgung Entwicklung Einfrieren von Vermögenswerten	Innenministerium Verteidigungsministerium Justiz Außenministerium Finanzmarktaufsicht Gesundheitsministerium	NATO EU



* **Putsch**: Gewaltakt meist kleiner Gruppen mit dem vorrangigen Ziel des Sturzes einer Regierung und Übernahme der Regierungsgewalt (*Wörterbuch Sicherheitspolitik mit Stichworten zur Bundeswehr*; 4. Vollst. Überarb. Auflage; Hamburg, Berlin, Bonn: Mittler (2000).

** **Sovereign Wealth Fund**: Staatsfonds, in denen Regierungen Kapital für unterschiedliche Zwecke (auch strategische Ziele) anlegen.

*** **Hoax**: Falschmeldung, die über Email, soziale Netzwerke oder andere Medien verbreitet wird.

Grafik: Mag. Michael Schurian, IFK

(3) Worin besteht das Potential eines Akteurs?

Das Potential eines Akteurs entsteht aus der Gesamtheit all seiner Fähigkeiten, Ressourcen und Sozialverbindungen. Eine hybride Bedrohung besteht in der Entfaltung dieses Potentials durch den kombinierten Einsatz unterschiedlichster Mittel und Methoden. Als Mittel kommen zunächst – aber nicht ausschließlich – jene der staatlichen Gewalt in Betracht: Streitkräfte und Nachrichtendienste, um grenzüberschreitend aktiv zu werden, Polizeikräfte und Justiz, um gegen im eigenen Staatsgebiet aufhältige Angehörige des anzugreifenden Zielstaates vorzugehen. Aufgrund weltumspannender Informations- und Kommunikationsnetzwerke ist ein Cyberangriff als ein potentielles Offensivmittel zu werten.

Ebenfalls grenzüberschreitend ist der Bereich der Ökonomie, der dank der Globalisierung zu größerer Produktvielfalt und vermehrten wechselseitigen Nutzen geführt hat – aber ebenso mit größerer Dependenz einhergeht. In diesem Zusammenhang muss beispielsweise an die Energieversorgungssicherheit gedacht werden. Viele Staaten sind vom Import fossiler Energieträger aus politisch instabilen Regionen oder vom strategischen Einkauf knapper Ressourcen (z.B. „seltene Erden") abhängig. Zwischen Russland und der Ukraine flammte in regelmäßigen Abständen ein Konflikt über Erdgaslieferungen auf, was stets zu politischen Spannungen zwischen den beiden Ländern führte.[1]

Spekulationen auf die heimische Währung sind eine Möglichkeit, um die Ökonomie eines Staates zu beeinflussen. Ähnlich verhält es sich bei genmanipuliertem Saatgut. So wirft z.B. Greenpeace dem U.S.-Konzern Monsanto vor, mit von ihm gehandelten genmanipulierten sterilen Samen für Abhängigkeit zu sorgen. Das Problem dabei: Bisher behielten Bauern einen Anteil der Ernte für die Aussaat im nächsten Jahr zurück. Dies ist mit dem genmanipulierten Saatgutprodukten des Vorjahres nicht mehr möglich, da diese nicht mehr zur erneuten Aussaat geeignet sind. Bauern sind somit gezwungen, Saatgut zuzukaufen.[2] Es ist nicht auszuschließen, dass derartige Praktiken auch mit staatlichem Interesse zu Machtprojektionszwecken genutzt werden.

---

1 Vgl. Mangott, Gerhard: Russland, Ukraine und die Gasversorgung der EU. 12.09.2014. <http://www.gerhard-mangott.at/?p=3598>, abgerufen am 14.11.2014.

2 Greenpeace: Steriles Saatgut als Geldquelle. 21.02.2006. <http://www.greenpeace.de/themen/landwirtschaft/gentechnik/steriles-saatgut-als-geldquelle>, abgerufen am 19.02.2015.

Bei potentiellen Fähigkeiten und Ressourcen eines Akteurs gelten folgende zwölf Dimensionen von Gewalt und Macht und stellen folglich das außenpolitische Instrumentarium eines Staates dar:

Militärische Gewalt

Hierbei kommen insbesondere Armeen und Spezialeinsatzkräfte zum Einsatz. Militär kann sowohl „offen" als auch „verdeckt" eingesetzt werden. Vor allem der verdeckte Kampf (engl. covert operations) könnte zukünftig in Zusammenhang mit hybriden Bedrohungen einen noch größeren Stellenwert haben. Dabei handelte es sich im Kalten Krieg um ein in der Öffentlichkeit kaum beachtetes Phänomen. „Speznas"-Kräften (russische Spezialeinsatzkräfte) wurde nachgesagt, sie hätten in einem möglichen Konfliktfall verdeckte militärische Einflussnahme durchgeführt. Aber es finden sich ebenso kongruente westliche Beispiele aus der jüngeren Geschichte. Wie angesprochen berichtete der britische „Mirror" Anfang 2011 in seiner Online-Ausgabe: „Hundreds of British SAS soldiers have been operating with rebel groups inside Libya for three weeks."[3] Von den Streitkräften der USA sind ähnliche Intentionen bekannt. So wird in der einschlägigen U.S.-Literatur von „covert operations", „black operations" oder von „clandestine operations" gesprochen. Eine „clandestine operation" ist in den USA definiert als eine

> „[...] operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities."[4]

Im Central Intelligence Agency (CIA)-Sprachgebrauch versteht man unter einer „clandestine operation" eine „[...] mission, with negative particulars, not attribu-

---

3 Crack SAS troops hund Gaddafi weapons inside Libya. In: The Mirror, 20.03.2011. <http://www.mirror.co.uk/news/uk-news/crack-sas-troops-hunt-gaddafi-117405>, abgerufen am 06.10.2014.

4 Department of Defense: Dictionary of Military and Associated Terms. Joint Publication 01-02. 08.11.2010, S. 56. <http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf>, abgerufen am 06.11.2014.

table to the organization carrying it out“[5]. Juristische Herausforderungen, die sich in diesem Zusammenhang mit der Begrifflichkeit Kombattant und Nicht-Kombattant ergeben, werden hier aber nicht weitergehend diskutiert. Es wird jedoch darauf hingewiesen, dass „Unschärfen“, die sich z.B. gegenwärtig mit bewaffneten Kräften in der Ost-Ukraine ergeben, zukünftig eine gängige Methode zur Beeinflussung politischer Vorgänge in einem Land werden könnte.

Politische und justizielle Gewalt

Die Gesetzgebung und – in Folge – der Justizapparat könnte zum Nachteil eines anderen Staates, dessen Wirtschaft und seiner Bürger eingesetzt werden (Ermächtigungsgesetze, rückwirkende Enteignung ohne Investitionsersatz, Haftbeschlüsse, etc.). Die missbräuchliche Vollziehung von Gesetzen gegenüber natürlichen oder juristischen Personen sowie die mögliche politische Einflussnahme auf die Gesetzgebung in einem anderen Staat veranlasst manche Autoren von „Lawfare“, einem „Kofferwort“ aus *Law* (engl. „Gesetz“) und *Warfare* (engl. „Kriegsführung“), zu sprechen.[6]

---

5 Smith, Thomas W.: Encyclopedia of the Central Intelligence Agency. New York 2001, S. 31. <http://books.google.at/books?id=1Jc9wBsImOIC&printsec=frontcover&dq=encyclopedia+of+the+central+intelligence+agency&hl=de&sa=X&ei=SXkyVIiUD6P9ywObuYDQAQ&ved=0CCAQ6AEwAA#v=snippet&q=%22black%20operation%22&f=false>, abgerufen am 06.10.2014.

6 Vgl. <http://www.thelawfareproject.org/what-is-lawfare.html>, abgerufen am 22.10.2014.

Gewalt durch Informationsdienste

Informationsdienste könnten neben Aufklärung und Informationsbeschaffung zur Manipulation von Informationen, Propaganda und Sabotage genutzt werden. So verweist beispielsweise die „Frankfurter Allgemeine" im Juni 2014 diesbezüglich auf Unterlagen von Edward Snowden: „Der britische Geheimdienst GCHQ [Government Communications Headquarters] verfügt über umfangreiche Möglichkeiten, Online-Umfragen zu beeinflussen, Web-Inhalte und E-Mail-Absender zu fälschen."[7] Ob westliche Informationsdienste derartig manipulative Maßnahmen tatsächlich einsetzen ist spekulativ.

Cybergewalt

Cyberangriffe können in verschiedenen Formen – z.B. mittels Viren, Identitätsdiebstahl (Phishing), Datenüberwachung und -manipulation, Unterdrückung von Web-Diensten, die Veränderung von Inhalten einer Webseite etc. – eingesetzt werden. Hier wird nochmals auf das Beispiel der theoretischen Möglichkeit des britischen Informationsdienstes GCHQ zur Beeinflussung des Internetverkehrs mittels entsprechender Software Inhalte von Video-Websites zu entfernen etc. verwiesen (siehe oben).

Privatisierte Gewalt

Private Militär- und Sicherheitsfirmen, paramilitärische Freiwilligenverbände, Milizen aber auch Piraten und kriminelle Organisationen verfolgen zwar eigenständige Ziele, könnten jedoch in einer strategischen Partnerschaft mit dem Offensivakteur beiderseitige Vorteile erzielen. Während für die organisierte Kriminalität (OK) sowie Warlords eine permanente Unsicherheitssituation und damit ein schwacher Staat eher von Vorteil zwecks Erwirtschaftung von Profit ist, könnte ein aggressiver Nachbarstaat die durch die OK verursachte Unsicherheit nützen, um den angegriffenen Staat weiter für die Zielsetzung des Angreifers zu schwächen.

---

7 Frankfurter Allgemeine: Britischer Geheimdienst kann Internet manipulieren. Online-Ausgabe, 14.07.2014. <http://www.faz.net/aktuell/politik/weitere-snowden-enthuellungen-britischer-geheimdienst-kann-internet-manipulieren-13046387.html>, abgerufen am 30.12.2014.

Volksgewalt

Zu dieser Gruppe zählen insbesondere bewaffnete Aufständische, politische oder religiöse Extremisten, eine mobilisierbare Masse von Unzufriedenen und marginalisierte Minderheiten, die – quasi als „fünfte Kolonne" – die Interessen eines offensiven Akteurs umsetzen. Eine erfolgreiche Instrumentalisierung dieser Volksgewalt von in einem anderen Land tätiger Akteure kann als wesentliches Werkzeug zur Aufwiegelung der Bevölkerung dienen. So könnte sich z.B. eine Privatfirma, die sich nach dem Vorbild der in Belgrad beheimateten Organisation „Canvas" organisiert, Schulungen und Trainings über „strategic nonviolent conflicts"[8] anbieten. Dabei ist die Abstützung auf eine ähnliche Zielsetzung wie bei „Canvas" vorstellbar:

> „[...] rather to spread the word of „people power" to the world than to achieve victories against one dictator or another. Our next big mission should obviously be to explain to the world what a powerful tool nonviolent struggle is when it comes to achieving freedom, democracy and human rights."[9]

Eine deutsche Tageszeitung bezeichnete einen der Leiter von Canvas, den Serben Srđa Popović, als jenen, der „Revolution als Business"[10] betreibt. Sind diese Ziele bei Canvas möglicherweise hehr, so ist eben nicht auszuschließen, dass ähnliche Firmen weniger uneigennützige Ziele verfolgen, um Staaten dies als Methode hybrider Bedrohung in Form von „Covert Operations" zu ermöglichen.

Terroristische Gewalt

Terrorattacken oder spektakuläre Sabotageakte, die eine hohe Zahl ziviler Opfer in Kauf nehmen bzw. auf diese bewusst abzielen, bezwecken die Minimierung der Widerstandskraft einer Gesellschaft. Dabei kann ein Staat Terrororganisatio-

---

8 CANVAS: Who we are. <http://www.canvasopedia.org/who-we-are>, abgerufen am 10.10.2014.

9 Ebd.

10 Scheffer, Ulrike: Der Serbe Srdja Popovic betreibt Revolution als Business. In: Tagesspiegel, 14.03.2011. <http://www.tagesspiegel.de/politik/widerstandsguru-der-serbe-srdja-popovic-betreibt-revolution-als-business/3946482.html>, abgerufen am 10.10.2014.

nen passiv fördern – in dem er terroristische Aktivitäten zwar nicht aktiv fördert, aber auch nicht unterbindet – oder aktiv unterstützen.

Diplomatische Macht

Den Einsatz diplomatischer Möglichkeiten kann ein staatlicher Akteur nützen, indem er beispielsweise bestehende Allianzen erschüttert und den Zielstaat zunehmend von der internationalen Gemeinschaft isoliert. Der EU-Ansatz am Beispiel der Schweiz wurde bereits erwähnt. Auch wenn hier nachvollziehbare Motive im Vordergrund standen, sind bei hybriden Bedrohungen von Staaten ähnliche Vorgangsweisen vorstellbar.

Realwirtschaftliche Macht

Der Lieferstopp von Rohstoffen und Energieträgern (Gas), der Einkauf strategischer Ressourcen, *Land Grabbing,* die Kontrolle von Verkehrswegen können als realwirtschaftliche Formen der Machtprojektion verstanden werden. Aber auch ein gesellschaftlicher Einfluss wird insbesondere durch den E-Commerce-Bereich wesentlich erleichtert. Finanztransaktionssysteme, Großhändler oder der damit einhergehende Datenstock von Kunden haben ungeahnte Machtprojektionspotenziale zur möglichen Schwächung des Wirtschaftsstandortes eines Staates. Als Beispiele sind Online-Konzerne wie Amazon oder der chinesische Gegenpart Alibaba zu nennen. Letzterer ist mittlerweile größer als Amazon und eBay zusammen und erwirtschaftet bemerkenswerte Profite.[11]

Finanzwirtschaftliche Macht

Handelshemmnisse, Wechselkursbeeinflussung, die gezielte Verschuldung anderer Länder sowie der strategische Einsatz von Staatsfonds (*Sovereign Wealth Funds*) sind Beispiele für die ökonomische Beeinflussung des Gegners. Medienberichte aus April 2013 zeigen bereits durchgeführte Versuche einer elektronisch gesteuerten kurzzeitigen Einflussnahme auf Finanzmärkte. Die U.S.-Nachrichtenagentur Associated Press (AP) berichtete, dass über Twitter gefälschte Informationen über eine Explosion, die den U.S.-Präsidenten im Weißen Haus verletzt hätte, lanciert wurden. Mehr als 1,9 Millionen Menschen sol-

[11] Alibaba: After the Float. In: The Economist, 06.09.2014, S. 60.

len den AP-Nachrichten auf Twitter gefolgt sein. Ergebnis war, dass aufgrund dieser Nachricht in drei Minuten der US Börsenbarometer Index S&P 500 um 0,8 Prozent fiel, was einen Wertverlust von 136,5 Millionen US Dollar bedeutete.[12] Waren die Auswirkungen auch nur von kurzer Dauer (die Börse erholte sich rasch wieder), zeigen sie dennoch, was mit Hilfe sozialer Medien auf dem Finanzsektor möglich scheint. Dabei kann ein krimineller Hintergrund nur ein Motiv darstellen. Ebenso sind strategische machtpolitische Szenarien denkbar. Weitere, ähnlich ausgefeilte Methoden im Bereich von Finanzspekulation mit der Absicht, einen Staat zu schädigen, zu destabilisieren oder willfährig zu machen, sind daher nicht unwahrscheinlich.

Wissenschaftliche und technologische Macht

Auch wenn ein *Brain-Drain* möglicherweise nicht bewusst zum Zwecke der Ausübung von hybrider Bedrohung eingesetzt wird, findet dieser bereits seit Jahrzehnten statt. Dabei werden Akademiker mit Zukunftspotential im Forschungs- und Unternehmensbereich vom Ausland abgeworben, was in den Medien oft als „Abzug der Gehirne" bezeichnet wird. Dabei entsteht durch die Abwanderung dieser Experten für die dafür verantwortlichen Staaten ein zweifacher Vorteil. Einerseits wird damit – sollte dies bewusst gesteuert werden – einem Staat dessen (zukünftige) Eliten entzogen, andererseits verschafft man sich auch einen technologischen Fortschritt, da die abgewanderten Experten Wissen für ihren „neuen" Staat generieren. Des Weiteren hätte dies zusätzlich ökonomische Nachteile für jene Staaten, denen „abgewanderte" Patente verloren gehen.

Zum Bereich der wissenschaftlichen Macht kommt ein weiterer Aspekt hinzu: Finanzierungen aus dem Ausland ermöglichen oftmals erst die Einleitung von Forschungsprojekten. Als Beispiel können U.S.-finanzierte Forschungsprojekte in Österreich genannt werden. In einem Interview in einer österreichischen Tageszeitung informiert Tim Lawrence[13] über U.S.-Forschungsinvestitionen. Demzufolge kooperierten 2013 die USA weltweit in 30 Ländern mit verschiede-

---

[12] FBI ermittelt wegen Tweet über Explosion im Weißen Haus. In: Die Presse Online, 24.04.2013. <http://diepresse.com/home/politik/aussenpolitik/1393224/FBI-ermittelt-wegen-Tweet-uber-Explosion-im-Weissen-Haus> abgerufen am 24.04.2013.

[13] Tim Lawrence ist Kommandant beim Air Force Research Laboratory und leitet das dort ansässige Europäische Büro zu Luft- und Raumfahrtforschung (EOARD).

nen Forschungsvorhaben.[14] Nach dem Artikel in der „Wiener Zeitung" belaufen sich die vom U.S.-Militär finanzierten österreichischen Projekte in den letzten fünf Jahren auf nahezu neun Millionen Euro.[15] Würde ein ähnlicher Akteur derartige Investitionen für Zwecke der hybriden Bedrohung einsetzen, ergäbe sich die theoretische Möglichkeit der Einstellung der Forschungsunterstützungen, womit der Erfolg der Forschungsprojekte erheblich gestört wäre. Ein zusätzlicher Nutzen aus Forschungsfinanzierungen ergibt sich durch die Möglichkeit, in Forschungsergebnisse anderer Staaten Einblick zu nehmen.

In diesem Zusammenhang ist ein theoretischer Einfluss der Pharmaindustrie auf das Gesundheitswesen zu erwähnen. Über weltweit agierende Netzwerke könnte Kontrolle über Meinungsbildner und Gesundheitsinstitutionen ermöglicht werden. Kleinstaaten, insbesondere in ärmeren Weltregionen mit dringendem Bedarf an Medikamenten, sind oftmals im besonderen Maße von der Pharmaindustrie anderer Staaten abhängig.[16] Eine entsprechende Interpretation von Gesundheitsstatistiken oder die Wirkung von Medikamenten, verbunden mit dem Wunsch nach höheren Gewinnmargen, könnte sowohl von Konzernen als auch von Staaten – vorausgesetzt die Intention ist vorhanden – für Panikmache instrumentalisiert werden. Das Gesundheitsbedürfnis der Bevölkerung einerseits, in Verbindung mit dem Eigeninteresse der Pharmaindustrie andererseits, könnte unter Umständen einen zusätzlichen Nährboden für eine soziale Destabilisierung eines Staates bieten.[17]

---

14 Figl, Bettina: Mehr als Brustkrebsforschung. In: Wiener Zeitung, 31.07.2014, S. 7.

15 Ebd., S. 7.

16 Anmerkungen von Amin/Brica/Feuchter, TeilnehmerInnen des GALG, 15.-19.09.2014.

17 Anmerkungen von Margreiter/Jancuska, Teilnehmer des GALG, 15.-19.09.2014.

Medienmacht

Liberale Demokratien mit pluralen Gesellschaften leben vom freien Gedankenaustausch. Medien erfüllen dazu die Funktion der Berichterstattung und tragen zur Meinungsbildung bei. Die Beeinflussung und Kontrolle der multimedialen „Konfiguration" einer Gesellschaft ist ein zentraler Machtfaktor, mit dem – jenseits von Waffengewalt – Einfluss auf Staaten und Gesellschaften ausgeübt werden kann. Der Einsatz von Medienmacht zielt auf die öffentliche und veröffentlichte Meinung ab, ob im Cyberbereich, in sozialen Netzwerken oder mittels massenmedialer Berichterstattung durch Wort, Ton, Bild und Film (ebenso Musik und Lebensstil). Daher bedienen sich Akteure oftmals der Medien, wie etwa gegenwärtig die islamistische Terrororganisation „Islamischer Staat".

Die Austragung von Konflikten basiert nicht ausschließlich auf realen Ereignissen, sondern ebenso in deren symbolischer Deutung, Sinngebung, kollektiver Wahrnehmung und deren Kontextualisierung in der Dynamik unterschiedlicher Welterklärungsmodelle. Wahr ist, was *wahr*-genommen wird. Medien sind hierfür die Brücke zwischen Realität einerseits und Kollektiven bzw. Individuen andererseits.

Eine völlig andere Form von Machtausübung im medialen Bereich zeigt sich durch die Trennung von Hauptkommunikationskanälen eines Staates – ähnlich geschehen in Syrien. Mitte 2012 berichtete „Spiegel Online", dass „[...] die arabischen Satelliten dem regimenahen Sender Addounia das Programm abgewürgt [...]"[18] hätten.

Ein zusätzlicher Aspekt im Spektrum medialer Macht offenbart sich durch die Möglichkeit gesteuerter Informationsmeldungen. Wiederum berichtete „Spiegel Online" 2012, dass nach Meldung des syrischen Informationsministeriums westliche Geheimdienste „[...] den Kanal des Staatsfernsehens hacken und das offizielle Programm durch Falschmeldungen ersetzen."[19]

---

[18] Salloum Ranniah: Offensive an der Twitter-Front. In: Spiegel Online, 24.07.2012. <http://www.spiegel.de/politik/ausland/buergerkrieg-in-syrien-offensive-an-der-twitter-front-a-845895-druck.html>, abgerufen am 09.10.2014.

[19] Salloum Ranniah: Offensive an der Twitter-Front. In: Spiegel Online, 24.07.2012. <http://www.spiegel.de/politik/ausland/buergerkrieg-in-syrien-offensive-an-der-twitter-front-a-845895-druck.html>, abgerufen am 09.10.2014.

Alle oben genannten Fähigkeiten und Ressourcen zu einem Bild gebündelt, ergeben folgende Abbildung:

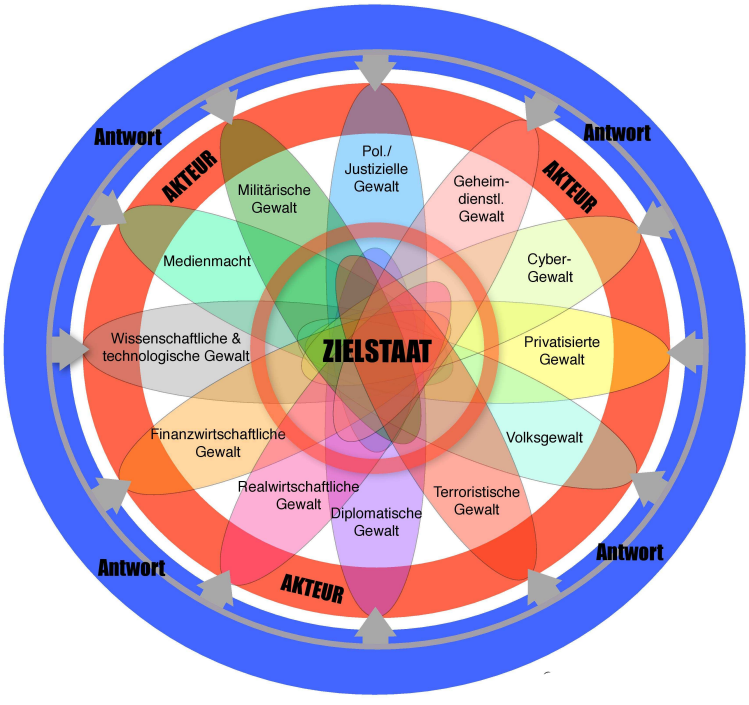


Abbildung 4: Spektren des Bedrohungspotentials
Anton Dengg, Michael Schurian

In Abbildung 4 ist der offensive Akteur, der die hybride Bedrohung initialisiert, als roter, äußerer Ring dargestellt. Der Defensivakteur bzw. der Zielstaat ist im inneren kleinen, roten Ring abgebildet. Beide Ringe sind durch zwölf verschiedenfarbige Ellipsen verbunden. Diese symbolisieren die jeweiligen Fähigkeiten, Handlungsdimensionen und außenwirksamen Instrumente des Akteurs. Aus diesem Spektrum kann dieser wählen, welches Mittel in welcher Kombination die empfindlichste Wirkung beim Zielstaat erzielen wird. Aus der Kombination verschiedenster Aktivitäten gegen unterschiedliche Schwachstellen des Gegners können Synergieeffekte erwachsen, die sowohl die physische als auch psychische Dimension des Konflikts erfassen. Als besonderer Aspekt sind in Abbildung 4 die sich überlappenden bunten Segmente zu nennen. Diese zeigen, dass jedes Segment, koordiniert mit zumindest einem zweiten Element vorherrschen

kann/muss, damit eine hybride Bedrohung entsteht. Zu betonen ist, dass Abbildung 4 lediglich einige Möglichkeiten von hybriden Bedrohungen aufzeigt und nahezu beliebig erweitert werden kann.[20] Der blaue Ring deutet auf die hybride Defensiv-Antwort in Form eines umfassenden staatlichen Sicherheitsansatzes hin.

(4) Wie kann eine hybride Bedrohung eingesetzt werden?

Eine hybride Bedrohung ist ein verbundenes, koordiniertes, konzertiertes, systematisches Zusammenwirken mehrerer Aktivitäten gegen einen Staat zu dessen Nachteil. Mehrere Handlungen (zumindest zwei) wirken auf den Zielstaat. Das erhöht nicht nur die Effektivität, sondern erschwert auch die Abwehr. Die Handlungen können mit Zwang, Druck und Gewalt erfolgen oder auch mithilfe von Propaganda und Embargos.

Da eine hybride Bedrohung auf mehreren Ebenen wirkt, kann von einem mehrdimensionalen Vorgehen gesprochen werden. Besonders einflussreiche Dimensionen sind die Bereiche der Politik und des Rechts, des Militärs, der Ökonomie, der Ökologie, der Sozietät und Kultur, der Technologie, der Wissenschaft sowie das Medienwesen.

Wie ein hybrider Prozess tatsächlich erfolgen kann, hängt vom Zustand des Zielstaates ab. Eine Industrienation ist abhängiger von Energie, Ressourcen und funktionierender Wirtschaft. Hingegen ist ein Schwellenstaat mit schwachen staatlichen Institutionen und internen Machtasymmetrien anfälliger für Korruption und Aufstände. Cyberangriffe sind in einem Land, das kaum über eine flächendeckende IT-Infrastruktur verfügt, wenig Erfolg versprechend. In einem hochtechnisierten Land kann ein solcher Angriff wiederum fatale Auswirkungen auf die (Finanz-)Wirtschaft und öffentliche Ordnung erzielen.

Dabei kann das Bedrohungspotential unmittelbar (direkt) oder mittelbar (indirekt) eingesetzt werden. Direkte Angriffe können über eigene Einheiten, indirekte über Stellvertreter erfolgen. Als indirekter Angriff wäre die Zweckentfremdung eines außenpolitischen Instruments anzusehen. Beispielsweise dient die originäre Funktion der Wirtschaft nicht der Bedrohung, sondern der materiellen

---

[20] Dies wird Gegenstand zukünftiger Forschung sein.

Bedürfnisbefriedung von Menschen, der Erzeugung von Gütern und Erbringung von Dienstleistungen sowie der Zuteilung von Ressourcen.[21]

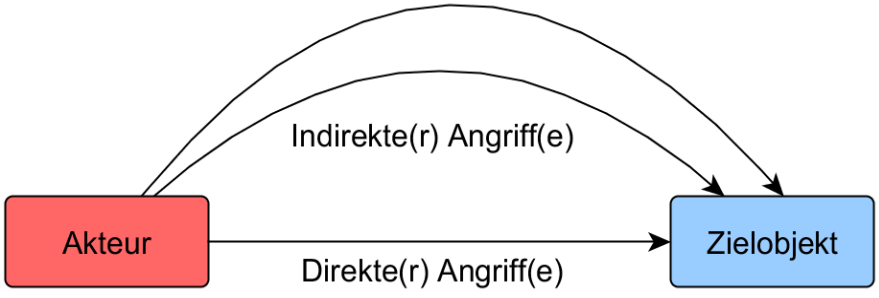


Abbildung 5: Direktes und Indirektes Vorgehen gegen ein Ziel
Michael Schurian

Bewertet man den Einsatz der Staatsgewalt als direktes Vorgehen gegen ein Zielobjekt, und sieht man z.B. in ökonomischen oder medialen Maßnahmen ein indirektes Vorgehen, ergibt sich schematisch folgende Abbildung (Abbildung 6), die das Potential des Akteurs auf direktem und indirektem Weg in sich zusammenfasst:

[21] Wirtschaftlicher Wettbewerb per se ist keine Sicherheitsbedrohung, kann aber dafür eingesetzt werden.

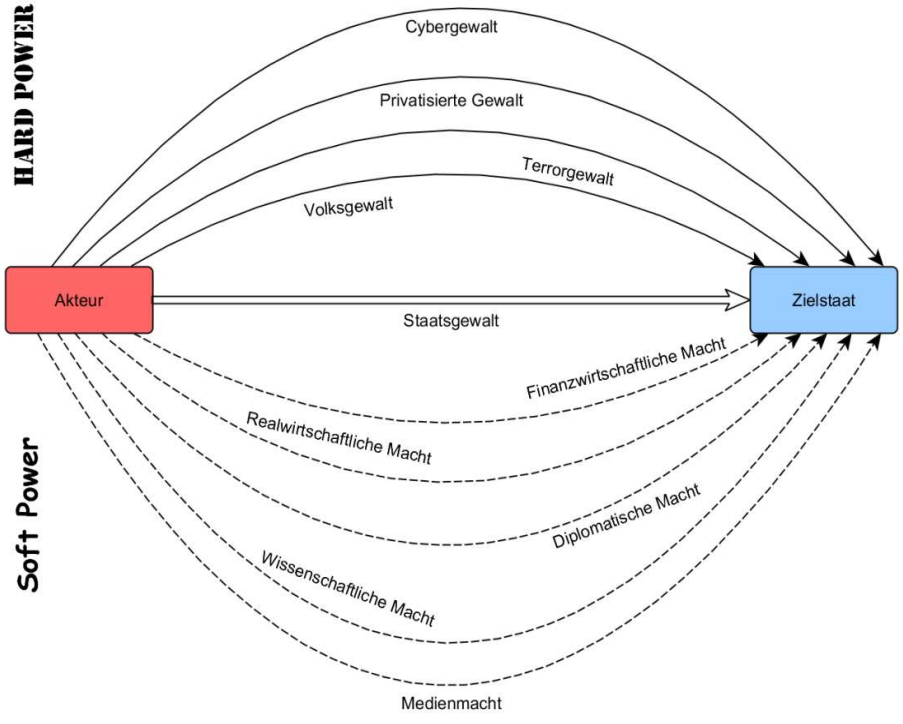


Abbildung 6: Direkte und indirekte Potentiale eines Akteurs
Michael Schurian

(5) Der zielgerichtete Einsatz des Bedrohungspotentials

Die Bedrohungshandlungen müssen geeignet sein, den Zielstaat in seiner Entscheidungsfreiheit zu beschränken und zu einer Verhaltensänderung im Sinne des Bedrohungsakteurs zu bewegen. Isoliert betrachtet mögen einzelne Operationen keinen (oder bloß einen willkürlichen) Zusammenhang aufweisen, weil es zunächst keine Überschneidungspunkte gibt. So hat beispielsweise eine vor der Küste eines Landes abgehaltene Marineübung auf den ersten Blick nichts mit Demonstrationen im Regierungsviertel der Hauptstadt gemein. Erst eine genauere Analyse könnte diese beiden Vorfälle als Machtprojektion eines einzigen Akteurs enttarnen.

(6) Die Mehrdimensionalität

Der mehrdimensionale Einsatz von Fähigkeiten und Ressourcen zum Zwecke der Konfliktaustragung ist das Kernelement hybrider Bedrohungen. Neben direkten Angriffen auf Streitkräfte des Gegners zielt die Strategie der hybriden Bedrohung zusätzlich auf die ökonomischen, infrastrukturellen, sozialen etc. Voraussetzungen des Zielstaats und seiner Allianzen ab. Bei einem so mehrdimensionalen Vorgehen der Konfliktaustragung (siehe hierzu auch den Absatz (5) zielgerichteter Einsatz) stellt sich die Frage nach der Treffsicherheit einer hybriden Bedrohung. Theoretisch ist davon auszugehen, dass nicht alle Auswirkungen vorhersehbar bzw. das Reaktionsmuster des angegriffenen Zielstaates nur schwer zu prognostizieren ist. Der Angreifer sieht sich kontraintuitiven Folgen ausgesetzt. Nicht-intendierte Auswirkungen auf Kollateralobjekte (z.B. Zivilisten, Verbündete, die eigene Exportwirtschaft, etc.) sind in der Lage, der Konfliktdynamik ungeahnte Impulse zu verleihen. Diese Impulse – auch wenn sie ungeahnt und überraschend auftreten – können bei Flexibilität des Akteurs wiederum mit anderen Spektren hybrider Bedrohung für einen weiteren Angriff genutzt werden.

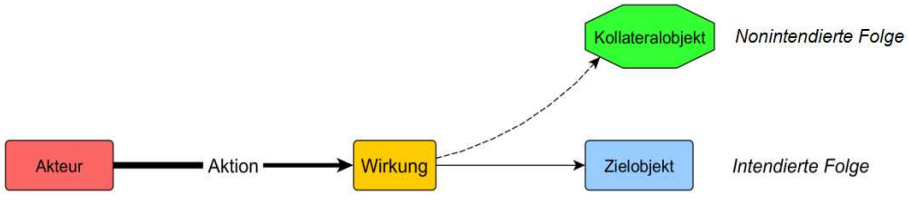


Abbildung 7: Intendierte und non-intendierte Folgen
Michael Schurian

Neben nicht-intendierten Folgen können eine Reihe von Effekten wirken, die ex ante nicht vorherzusehen oder abzuschätzen waren. Ein Terroranschlag richtet sich unmittelbar gegen zivile Staatsbürger und mittelbar gegen deren Staat. Ein Attentat hat aber ebenso Auswirkungen auf die Wirtschaft (Ausbleiben von Touristen, entgangene Gewinne und somit niedrigere Steuereinnahmen, Unsicherheit an den Börsen), auf das Rechtswesen (Ruf nach strengeren Sicherheitsgesetzen, Inkaufnahme der Schwächung bürgerlicher Freiheiten) und auf die Volksgewalt (Solidarisierung mit den Tätern) etc. Diese zusätzlichen Reaktionen wirken als Kreuzeffekte auf den Konflikt ein – sie können die Wirkungen intensivieren oder auf andere Lebensbereiche erweitern. Daher kann ein Terroran-

schlag hybride Wirkungseffekte auslösen, die wiederum hybride Gegenreaktionen bedingen.

Verstärken sich die Auswirkungen, kann man von einem **Multiplikatoreffekt** sprechen. Die mediale Berichterstattung verstärkt – indem sie ihrer ureigenen Aufgabe des Berichtens nachkommt – die mediale Präsenz der Täter. Dies kann beispielsweise zum Ausfall von Umsätzen und somit zu verringerten Steuereinnahmen führen, was wiederum geringere staatliche Ausgaben bewirkt. Sanktionen gegen Zulieferunternehmen (Uranminenabbau, Transport und Nuklear-Entsorgung) können den Druck auf weitere Branchen (Energiewirtschaft) bewirken. Deswegen kommt Medien und deren Berichterstattung höchste Bedeutung zu. Verantwortungsvolle journalistische Recherchearbeit, mit dem Ziel einer objektiven Berichterstattung, ist daher als wesentliche Strategie gegen hybride Bedrohungen zu werten.

Es ist zu befürchten, dass solche Verstärkungen des Initialangriffes einen gewissen Automatismus auslösen, der sich über Kettenreaktionen zu einem Flächenbrand aufheizen kann. Aufgrund der Interdependenz der betroffenen Systeme (Politik-Ökonomie-Soziales-Ökologie-Militär) ist mit nicht-linearen Folgen zu rechnen, welche die Stoßrichtung und die Dosierung des initialen hybriden Angriffs übersteigen.

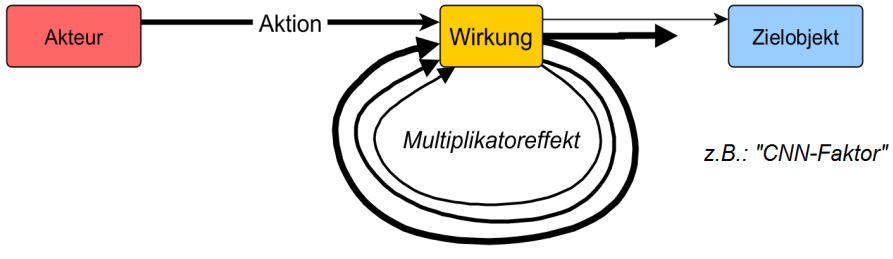


Abbildung 8: Multiplikatoreffekt
Michael Schurian

Während es aufgrund der Konnektivität interdependenter Systeme zu Verstärkungswirkungen gegenüber dem Zielstaat kommen kann, ist auch eine konträre Wirkung möglich. Die Folgen eines hybriden Angriffs könnten also ebenso den Akteur selbst treffen (**Rückkopplungseffekt**) und eine Eigenschädigung be-

wirken. Solche Rückkopplungen gegen den Initiator sind nicht überraschend, da sowohl Akteur als auch Zielobjekt verbunden sind.

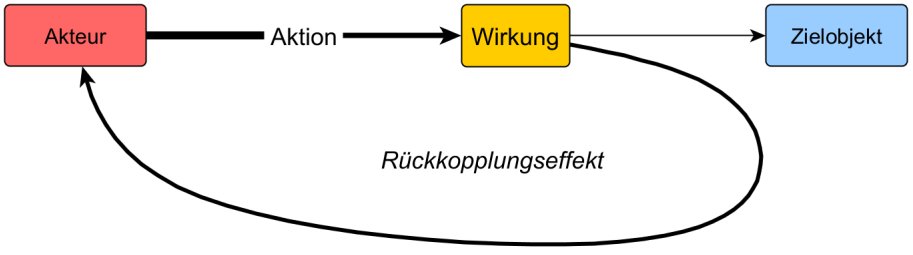


Abbildung 9: Rückkopplungseffekt
Michael Schurian

Der Erfolg einer hybriden Bedrohung hängt ebenso davon ab, ob ein Akteur mögliche Rückkopplungen in seine Planungen einbezieht, sich wappnen und in Folge standhalten kann. Die Ungewissheit über Ausmaß, Stoßrichtung oder Zeitpunkt solcher Effekte ist für den Entwurf wirksamer Resilienz-Konzepte bestimmend.

(7) Zeitliche Abstimmung

Hinsichtlich der temporalen Koordinierung sind parallele und serielle Angriffswellen denkbar. *Parallele Attacken* sind multiple simultane Operationen; sie werden zu einem kurzfristigen und massierten Vorgehen gegen einen Gegner eingesetzt. *Serielle Attacken* sind eine Kette von Operationen, die zeitlich versetzt gesetzt werden. Sie eignen sich als Zermürbungsinstrument, um beispielsweise in den Angriffspausen Verhandlungserfolge zu erzielen, seine Strategie zu evaluieren und gegebenenfalls zu adaptieren. Eine Angriffsserie, deren einzelne Anschläge jeweils unterhalb der Wahrnehmungsschwelle bleiben, dient auch dem Angreifer sich im Verborgenen zu halten.

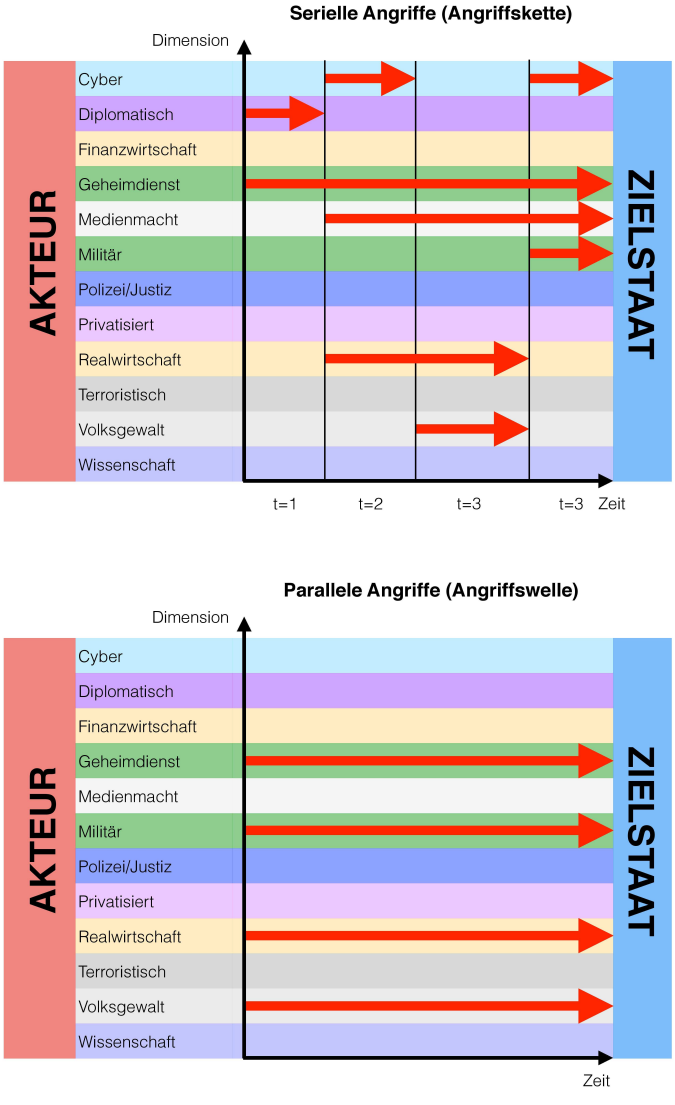


Abbildung 10: Hybride Angriffswellen und Angriffsketten
Michael Schurian

Im Lichte des Kraft-Raum-Zeit-Kalküls bedeutet dies: Hybride Angriffswellen setzen unterschiedliche Kräfte in verschiedenen Räumen gleichzeitig ein. Hybride Angriffsketten verteilen verschiedenartige Kräfte

auf mehreren Ebenen zu unterschiedlichen Zeiträumen. Aufgrund der massiven Möglichkeiten paralleler hybrider Ansätze stellen diese ein Worst-Case-Szenario dar. Ob von einem Akteur eine parallele oder serielle Attacke erfolgt, hängt mit großer Wahrscheinlichkeit von der Größe und Fähigkeiten des Ziellandes ab.

1.2.13 Zusammenfassung

Hybride Bedrohungen sind grundsätzlich nichts Neues. Sie bekommen aber durch globale Vernetzungsprozesse, durch neue mediale Möglichkeiten, insbesondere den sozialen Netzwerken im Cyberraum, eine völlig neue Dynamik und Bedeutung. Die zunehmende Komplexität unserer Infrastruktur, die mittlerweile unser Gesellschaftssystem durchdringt, wird aufgrund der vermehrten Abstützung auf Technik verletzbarer. Hervorzuheben ist die enorme Steigerung der Abhängigkeit von technischen Produkten, was wiederum neue staatliche Machtpotentiale (auch jene von nicht-staatlichen Akteuren) schafft. Herausforderungen ergeben sich insbesondere im Cyberraum, da die Rückverfolgbarkeit der Angreifer kaum gewährleistet ist. D.h., es ist oftmals unmöglich, den „Urheber" von Angriffen beziehungsweise den eigentlichen „Machtausüber" auszumachen. Ist der vermeintliche Urheber ausgemacht, ergibt sich die Herausforderung, die Vorwürfe des Tatbestands zu verdichten und den Verdächtigten als „Attentäter" zu überführen. Es muss nicht jenes Land, von dem eine Cyberattacke ausgeht, auch der Urheber des Angriffes sein. Schwachstellen im Cyberraum eines Staates könnten von Angreifern ausgenutzt worden sein.

Ein mehrdimensionales Vorgehen kommt der Verschleierung von Zielen zugute. Dabei muss dem Aggressor nicht daran gelegen sein, sich in der Öffentlichkeit als Urheber der Machtprojektion zu präsentieren – entscheidend ist die Erreichung von Ziel und Zweck seiner Aktivität[22]. Wesentlich für das Verständnis der Strategie einer hybriden Bedrohung ist, dass ein Akteur seine Maßnahmen zielgerichtet, mehrdimensional und in einem zeitlich abgestimmten Zusammenhang koordiniert und als Art „Mastermind" agiert.

[22] Das Beispiel rund um die Geschehnisse des Virus *Stuxnet* macht dies deutlich.

Ein Aggressor kann einen Zielstaat entweder seriell oder parallel auf vielfache Weise (hybrid) bedrohen. Die angestrebte Wirkung kommt beim angegriffenen Zielstaat nicht immer geplant zur Wirkung. Derartige nicht-intendierte Auswirkungen können der Konfliktdynamik ungeahnte Impulse verleihen, was wiederum große Flexibilität beim Aggressor bedingt. Im Kontext staatlicher Sicherheit ist die Überschreitung einer strategischen Schwelle beim Zielstaat entscheidend.

Das Ausnutzen von Naturkatastrophen sowie eine folgende Anwendung zusätzlicher hybrider Machtprojektionen kann zur verstärkenden Destabilisierung eines staatlichen Gefüges im Sinne des Aggressors führen. Diese Reaktionsfähigkeit hängt entscheidend von der Flexibilität, der Bereitschaft sowie der Möglichkeit des Aggressors ab, seine Macht zu projizieren.

Gegenwärtige Beispiele (wie die Ukraine-Krise spätestens ab 2014) verdeutlichen die Herausforderung hybrider Bedrohungen (entweder von staatlicher oder nicht-staatlicher Seite) für die westliche Gemeinschaft. Dabei spielen rechtliche sowie moralische Aspekte eine große Rolle. Beispiele zeigen, dass sich Staaten bereits hybrider Methoden zur Machtausübung bedienen. Daher gilt es, Gegenmittel zu generieren.

Wesentlich ist, hybride Bedrohungen nicht als isoliert zu betrachtende Konfliktbilder zu werten. Es gibt nicht *die* hybride Bedrohung, da diese aus divergierenden Variationen alternierender Kombinationen besteht und somit wechselweise Effekte und Stoßrichtungen erzeugt. Daher sind auch Lösungsansätze, Schutz- und Abwehrmechanismen in entsprechender Vielfalt zu entwickeln.

Die wesentliche Herausforderung für Staaten besteht darin, gegen sie gerichtete hybride Machtprojektionen in der gesamten Bandbreite zu erkennen und geeignete, akkordierte Gegenmaßnahmen einzuleiten.

1.3 Hybride Bedrohungspotenziale im Lichte der Vernetzung und Systemischen Denkens

Herbert Saurugg

Seit dem Ende des Kalten Krieges vor 25 Jahren haben sich die Bedrohungsbilder und -szenarien wesentlich verändert. Von einer relativ einfach überschaubaren bipolaren Welt sind wir heute in einer hochkomplexen, sehr dynamischen und zunehmend turbulenteren Zeit angelangt. Die Fachwelt verwendet dafür auch den Begriff VUCA[1] - volatil, unsicher, komplex und ambivalent. Diese Entwicklungen betreffen so gut wie allen Lebensbereiche. Gleichzeitig haben sich unsere altbewährten Denkmuster kaum verändert. Doch reicht das aus, um mit den neuen Herausforderungen zurecht zu kommen?

Ein wesentlicher Treiber für die Veränderungen war die exponentiell ansteigende Verbreitung von Informationstechnologien (IT, Computer, IT-Lösungen und vor allem die technische Vernetzung, im speziellen das Internet), die Basistechnologien des 5. Kondratieff-Zykluses. Diese beschreiben zyklische Wirtschaftsentwicklungen in der Dauer von rund 40-60 Jahren, wo je eine Basistechnologie/-innovation[2] die Entwicklungen bestimmt. Demnach befinden wir uns derzeit im abklingenden 5. bzw. im beginnenden 6. Zyklus, also in einer Phase des Umbruches.

1.3.1 Netzwerkgesellschaft

Parallel dazu hat sich seit den 1950er Jahren die Netzwerkgesellschaft zu entwickeln begonnen. Zuerst sehr langsam, nahm mit der breiten gesellschaftlichen Durchdringung mit Informationstechnologien Anfang des 21.

---

1 Englisch: Volatility, uncertainty, complexity and ambiguity.

2 1. Dampfmaschine, Frühmechanisierung, Industrialisierung → Kraft; 2. Eisenbahn → Transport; 3. Elektrotechnik- und Schwermaschinen; Chemie → Verarbeitung; 4. Integrierter Schaltkreis, Kernenergie, Transistor, Automobil → Automatisierung; 5. Informations- und Kommunikations-Technik → Integration, Globalisierung; 6. Wahrscheinlich Psychosoziale Gesundheit, Biotechnologie, Bildung.

Jahrhunderts die Geschwindigkeit deutlich zu. Während die Industriegesellschaft durch Standardisierung, Synchronisierung, Zentralisierung (hierarchische Strukturen) oder durch Konzentration (Massenheere, Massenmedien, Massenproduktion, Arbeit in der Fabrik) gekennzeichnet ist, ist die nun sich etablierende Netzwerkgesellschaft durch genau gegenteilige Kennzeichen charakterisiert.[3] Es kommt zu einer Individualisierung (Produkte, Lebensweise), zur Autokoordinierung (über/durch das Internet, ad-hoc Vernetzungen), zur Dezentralisierung (Energiebereitstellung, bzw. verlieren Nationalstaaten ihre Bedeutung) und zur dynamischen Vernetzung statt Konzentration, was wiederum hierarchische Strukturen in Frage stellt. Die Netzwerkgesellschaft etabliert sich neben der Agrar- und Industriegesellschaft als dritte wesentliche Gesellschaftsform unabhängig von der jeweiligen religiösen oder wirtschaftlichen Weltanschauung.

Der Transformationsprozess von der Agrar- zur Industriegesellschaft, zwischen ca. 1650 und 1750, ist nicht reibungsfrei verlaufen und hat so manches bis dahin gültige Weltbild über den Haufen geworfen. Ähnliche Turbulenzen zeichnen sich auch heute ab. Dabei wird die bisherige Agrar- und Industriegesellschaft nicht vollständig abgelöst, sondern sie entwickelt sich parallel dazu, was zusätzliche Herausforderungen schafft. Konflikte haben daher häufig mit den damit verbundenen unterschiedlichen Wertemustern und Denkweisen zu tun und weniger mit den häufig vorgeschobenen Motiven, wie etwa bei scheinbaren Religionskriegen.

Bemerkenswert ist, dass sich die abzeichnenden Lösungen und Denkweisen der Netzwerkgesellschaft viel stärker mit der Agrar- als mit der Industriegesellschaft decken, was auch mit der vorherrschenden Energienutzung zu tun hat. Die Industriegesellschaft war durch das fossile Zeitalter geprägt, das wahrscheinlich noch weitreichende Nachwirkungen haben wird, wie z.B. beim sich abzeichnenden Klimawandel. Darüber hinaus ist zu erwarten, dass Lösungen der Netzwerkgesellschaft, beispielsweise dezentrale Energieversorgungssysteme oder Produktionsmethoden, auch zu einer positiven Weiterentwicklung in der Agrargesellschaft, etwa in entlegenen Regionen, beitragen können. Damit könnten auch wichtige sicherheitspoli-

---

[3] Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit, Hochschule für Management Budapest 2013.

tische Ziele, wie die Stabilisierung vor Ort, gefördert und leichter erreicht werden. Wenn ein würdiges Leben vor Ort möglich ist, sinkt der Migrationsdruck bzw. das Konfliktpotential. Die durch die Industriegesellschaft geschaffene Chancenungleichheit oder Ressourcenprobleme könnten damit wieder reduziert werden. Das Ende des noch vorherrschenden Wachstumsparadigmas zeichnet sich ab. Es ist auf einer Welt mit begrenzten Ressourcen nicht nachhaltig und wirkt selbstzerstörerisch. Die wesentliche Frage dabei ist noch, wie und ob uns eine Abkehr ohne einer „Schöpferischen Zerstörung“[4] gelingen kann.

Aus dieser Perspektive erscheinen so manche Widersprüchlichkeiten und aktuelle Entwicklungen in einem anderen Licht. Etwa die Auflösung der häufig künstlich geschaffenen Nationalstaaten im arabischen Raum, oder, dass es durch eine dezentrale Energieversorgung zu massiven Machtverschiebungen kommt, die von den etablierten und konzentrierten/zentralisierten Machthabern wahrscheinlich nicht ohne weiteres hingenommen werden. Natürlich berücksichtigt das hier dargestellte einfache Ursache-Wirkungsmodell viele Aspekte nicht, die auch noch eine Rolle spielen. Dazu aber noch mehr weiter unten.

Es gibt verschiedene Modelle, die aus der Vergangenheit zyklische Entwicklungen ableiten bzw. beschreiben. Gemeinsam ist ihnen, dass sie eine große Umbruchphase für diese Dekade prognostizieren.[5] Die Anzeichen für größere Umbrüche sind bereits mehr als deutlich, wobei die tatsächliche Tragweite erst im Nachhinein beurteilt werden kann.

---

[4] Vom österreichischen Wirtschaftswissenschaftler Joseph Alois Schumpeter (*1883, †1950) geprägter Begriff für den durch den Wettbewerb ausgelösten Prozess der ständigen Erneuerung und Verbesserung der Produktionsverfahren und Erzeugnisse. Den Prozess der schöpferischen Zerstörung, bei dem alte Güter und Produktionsverfahren ständig durch neue ersetzt werden, sieht Schumpeter als Motor der wirtschaftlichen Entwicklung. Eine zentrale Rolle spielt dabei der schöpferische, einfallsreiche Unternehmer, der durch neue Ideen und den Einsatz neuer Produktionsmethoden, Techniken und Verarbeitungsmöglichkeiten den wirtschaftlichen und technischen Fortschritt immer wieder vorantreibt. Quelle: Duden Wirtschaft von A bis Z: Grundlagenwissen für Schule und Studium, Beruf und Alltag. Mannheim 2013.

[5] Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit, Hochschule für Management Budapest 2013.

Um das Thema hybride Bedrohungen im Lichte dieser Entwicklungen besser beleuchten zu können, ist es noch erforderlich, sich mit einigen Grundlagen auseinanderzusetzen. Eine zentrale Rolle spielen dabei Systeme.

1.3.2 Systeme

Ein System beschreibt die funktionale Zusammensetzung von verschiedenen Systemelementen zu einem Ganzen. Entscheidend dabei sind die Beziehungen zwischen den Systemelementen, das „Wirkungsgefüge". Denn ohne Beziehungen gibt es kein System, sondern nur eine Ansammlung oder einen Haufen.[6] Entscheidend ist, dass ein System mehr ist, als die Summe der Einzelelemente. Was nicht weiter spektakulär klingt, hat es dennoch in sich. Es gibt unzählige Beispiele, wo diese einfache Weisheit unzureichend berücksichtigt wurde und es daher zu weitreichenden negativen Konsequenzen kam. Ob das im Umweltbereich (Wildbachverbauungen, Umweltverschmutzung), bei der Entwicklungszusammenarbeit (Brunnenbau) oder beim Finanzcrash 2007/2008 mit zahlreichen Folgekrisen war, immer wurde diese einfach klingende Aussage unzureichend berücksichtigt.

Auch wenn man alle chemischen Elemente des menschlichen Körpers kennt und zur Verfügung hat, ergibt das noch keinen Menschen. Ein Orchester ist viel mehr als die Summe von perfekten Einzelmusikern. Immer spielen die „unsichtbaren Fäden" zwischen den Einzelelementen eine Rolle, die erst einen Mehrwert schaffen.

Was konkret ein System ist, hängt von der jeweiligen Betrachtung und Detaillierung ab. Ob man etwa ein Molekül, eine Zelle, ein Organ, den Menschen, oder sein Sozialsystem betrachtet. Ein System kann auch eine inhaltliche, eine zeitliche und/oder eine soziale Grenze zu seiner Umwelt aufweisen, die von den Systemauswirkungen betroffen sein mag, aber keinen

---

[6] Vgl. Ossimitz, Günther/Lapp, Christian: Systeme. Denken und Handeln. Das Metanoia-Prinzip. Eine Einführung in systemisches Denken und Handeln. Berlin 2006.

Einfluss auf das Wirkungsgefüge hat.[7] Daher darf ein System nicht als etwas Absolutes verstanden werden.

Grundsätzlich wird zwischen einfachen und komplexen Systemen unterschieden. Einfache Systeme (Maschinen) stellen kein großes Problem dar, was ihre Steuerung, Regulierung und Lenkung – kurz, ihre Kontrolle – betrifft. Hier haben wir eine Erfolgsgeschichte hinter uns. Komplexe technische Systeme sind jedoch ein relativ neues Phänomen, mit dem wir erst umzugehen lernen müssen.[8] Zeitgleich sind wir aber ständig von komplexen Systemen umgeben, da die Natur nur aus offenen, dynamischen und damit komplexen Systemen besteht. Daher könnten wir auch von der Systemgestaltung in der Natur sehr viel lernen.

1.3.3 Komplexe Systeme

Komplexität ist ein häufig verwendeter Begriff, ohne das er eindeutig definiert wäre. Wir verbinden damit meist intuitiv undurchsichtige, komplizierte, vielschichtige oder unerklärlich Situationen oder Phänomene. Unsere Welt ist komplexer geworden, alles „dreht" sich schneller. Das „Hamsterrad" dient häufig als Metapher, alles muss schneller gehen oder wachsen, ohne jedoch ein Ziel erreichen zu können. Selten sind uns aber die dahinterliegenden Zusammenhänge bewusst.

Komplexe Systeme bestehen aus einer großen Anzahl von Elementen, die miteinander verbunden sind, die aber auch mit ihrer Umwelt interagieren und wo es laufend zu Rückkopplungen kommt. Es gibt auch technische Systeme (Maschinen) mit einer großen Anzahl von Elementen. Diese funktionieren aber nur in einer determinierten Umgebung und sie können in ihre Einzelteile zerlegt und wieder zusammengebaut werden. Das sind dann komplizierte Systeme, wie etwa mechanische Uhrwerke oder Druckmaschinen. Sie werden auch als tote Systeme bezeichnet. Komplexe Systeme

---

7 Vgl. Krizanits, Joana: Einführung in die Methoden der systemischen Organisationsberatung. Heidelberg 2013.

8 Vgl. Malik, Fredmund: Komplexität – was ist das? Modewort oder mehr? Kybernetisches Führungswissen Control of High Variety-Systems. <http://www.kybernetik.ch/dwn/Komplexitaet.pdf>, abgerufen am 24.10.2014.

hingegen können nicht einfach zerlegt und analysiert und dann wieder zusammengebaut werden. Sie werden daher auch als lebendige Systeme bezeichnet. Daher führt die Vernetzung in einer nicht determinierbaren Umgebung zu komplexen Systemen, die ein völlig anderes Systemverhalten aufweisen, als unsere bisherigen einfachen bzw. komplizierten Systeme (Maschinen).

In komplexen Systemen kommt es zu laufenden Rückkopplungen, es entstehen Eigendynamiken. Einfache Ursache-Wirkungszusammenhänge gehen verloren, die Steuerbarkeit (Management) sinkt bzw. wird unmöglich. Es kommt zu langen Ursache-Wirkungsketten. Eingriffe wirken sich zeitverzögert aus und sind irreversibel. Es entsteht die Gefahr einer Übersteuerung. Kleine Ursachen können zu großen Wirkungen führen und umgekehrt. Viel Aufwand mit wenig Ergebnis. Es kommt zu indirekten Wirkungen, die kaum abschätzbar sind und daher durch unsere etablierten Risikobewertungsmethoden nicht erfasst werden. Eine fehlende Reichweitenbegrenzung ermöglicht Domino- und Kaskadeneffekte, die umso verheerender ausfallen können, je größer das vernetzte System ist. Die Lösung eines Problems schafft neue Probleme (Aktionismus). Es kommt zu exponentiellen Entwicklungen und zur Erhöhung der Dynamik, mit denen wir nur sehr schlecht umgehen können, etwa mit dem Zinseszins[9].

Klingt vielleicht theoretisch. Bei näherer Betrachtung finden wir jedoch wieder unzählige Beispiele aus dem täglichen Leben. Ob das die Ohnmacht bei einer Vielzahl von anstehenden Problemen ist (Bildungs-, Gesundheits-, Pensionssystem), die zeitverzögerten negativen Auswirkungen des Internets mit den steigenden Herausforderungen aus dem Cyberspace (Cyber-Angriffe, Sicherheitsschwachstellen), ein Terroranschlag der zwei Kriege nach sich zieht (9/11), die immer wieder praktizierte Anlassgesetzgebung oder die unlösbaren Entwicklungen im Finanzsystem; immer spielt die unterschätzte Komplexität und Nicht-Steuerbarkeit eine Rolle. Ganz abgesehen davon, dass alle Kriege in ihrer Dynamik und Tragweite unterschätzt wurden.

---

[9] Bei einer angenommen Verzinsung von 5% (einschließlich Zinseszins) verdoppelt sich die angelegte Summe/die Schulden nach rund 14 Jahren. Nach 28 Jahren tritt eine Vervierfachung und nach 42 Jahren eine Verachtfachung ein. Dieser Vorgang wird exponentielles Wachstum genannt und betrifft zum Beispiel besonders Kreditnehmer.

1.3.4 Emergenz

Hinzu kommt, dass mit dem Grad der Vernetzung auch die Emergenz in einem System steigt. Unter Emergenz wird die spontane Herausbildung von neuen Eigenschaften oder Strukturen infolge des Zusammenspiels der Elemente in einem System verstanden. Die Eigenschaften der Elemente lassen dabei keine Rückschlüsse auf die emergenten Eigenschaften des Systems zu, was wiederum dazu führt, dass es zu einer spontanen Selbstorganisation und zu einer Nichtvorhersagbarkeit der Entwicklungen kommt.

Berücksichtigt man diesen Aspekt in aktuellen Entwicklungen, erscheinen diese wohl in einem neuen Licht. So wird etwa begreifbarer, wie faktisch aus dem Nichts eine Organisation wie der „Islamische Staat" (IS) unrühmliche Weltbekanntheit erlangen konnte. Durch die heutigen Möglichkeiten der technischen Vernetzung kann eine spontane und weitreichende Selbstorganisation erfolgen. In diesem negativen Fall führte das innerhalb sehr kurzer Zeit zu einer Schreckensherrschaft in einer sehr großen Region. Es ist jedoch nicht davon auszugehen, dass diese nachhaltig sein wird, da das Wachstum zu explosiv erfolgte. Dennoch wurden damit erhebliche Schäden und menschliches Leid verursacht. Verstärkt wurde das Ganze durch die heutigen Propagandamöglichkeiten, die wir durch das Internet bereitstellen. Daran ist aber weniger das Transportmedium schuld, als viel mehr, wie wir uns dadurch manipulieren lassen.

Die Nichtvorhersagbarkeit könnte aber auch dazu führen, dass nun die Gegenreaktionen auf den Islamischen Staat heftiger werden, was sich bereits abzeichnet, was wohl seitens dieser Gruppierungen nicht intendiert ist. Aber auch hier sind die Folgewirkungen nicht abschätzbar. Die steigende Sorge vor möglichen Anschlägen in anderen Ländern ist daher mehr als begründet.[10] Ein wesentliches Problem dabei ist, dass viele Reaktionen auf Aktionismus und Symptombehandlung zurückzuführen sind.

---

[10] Vgl. Sadowski, David/Becker, Jeff: Beyond the „Hybrid" Threat. Asserting the Essential Unity of Warfare. In: Small Wars Journal, 2010. <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-etal.pdf>, abgerufen am 24.10.2014.

1.3.5 Symptombehandlung

Eine wesentliche Änderung in der Bedrohungsbetrachtung wurde durch die Terroranschläge vom 11. September 2001 ausgelöst (9/11). Keine Sicherheitsdebatte kommt seither ohne das Thema „internationaler Terrorismus" aus.

Ein besonders hoher Aufwand wurde in die Erhöhung der Flugsicherheit investiert, was de facto einer Vorbereitung auf den „letzten Krieg" – auf das letzte Ereignis, dass in dieser Form aber wahrscheinlich nicht mehr eintreten wird - gleichkommt, ohne pauschal alle getroffenen Maßnahmen infrage stellen zu wollen. Bei einer systemischen Betrachtung stößt man jedoch rasch auf viel Aktionismus. Ob das beim „Krieg gegen den Terror" generell oder beim Irak- bzw. Afghanistankrieg im Speziellen, aber auch bei den inzwischen vielfach installierten technischen Sicherheitslösungen in der Flugsicherheit ist, der Erfolg ist bescheiden, bzw. wurden fast immer nur Symptome behandelt. Die meisten Maßnahmen haben zu keiner wesentlichen Verbesserung der Sicherheitslage insgesamt geführt, sondern zur weiteren Destabilisierungen bzw. zur Erhöhung der Scheinsicherheit, aber auch zu nicht intendierten Nebenwirkungen, wie etwa durch die Einschränkung der Privatsphäre oder indem durch die voranschreitende Überwachung unzählige unschuldige Menschen unter Generalverdacht geraten. Ganz abgesehen davon, dass diese Systeme ein hohes Missbrauchspotential aufweisen.

1.3.6 Terrorismus

Um Terrorismus verstehen und begegnen zu können, muss man zuerst wissen, wie er funktioniert. Kurz und knapp dargestellt wirkt Terrorismus zweimal. Einmal durch die unmittelbaren Auswirkungen bei einem Anschlag. Das zweite Mal durch die beim Opfer hervorgerufenen Reaktionen.[11] Aus verschiedenen Untersuchungen ist bekannt, dass die Sekundär-

---

[11] Vgl. Vester, Frederic. Die Kunst vernetzt zu denken. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ein Bericht an den Club of Rome. München 2011.

schäden wesentlich höher sind, als die Schäden durch das unmittelbare Ereignis. So geht man heute davon aus, dass die Folgekosten von 9/11 in die Billionen U.S.-Dollar gehen.[12] Damit führt eigentlich nicht das unmittelbare Ereignis, sondern unsere Reaktionen darauf zu den wesentlich größeren Schäden. Und dies nicht nur auf finanzieller Basis. Eine große Anzahl von unschuldigen Menschen verlor in Folge des „Kampfes gegen den Terror" ihr Leben. Neben den unzähligen Soldaten[13] eine viel größere Anzahl an Zivilisten – direkt, aber auch indirekt. Ist deshalb unsere Welt sicherer geworden?

In den vergangenen Jahren gab es ein positives Beispiel, bei dem nicht gleich überreagiert wurde. Und zwar nach den Anschlägen auf das öffentliche Verkehrssystem in London im Jahr 2005, da man mit dieser Möglichkeit gerechnet und sich darauf vorbereitet hatte.[14]

Ein zunehmendes Problem stellen die geänderten Ziele von Terrorgruppen dar. Im 20. Jahrhundert wurden mit Terrorismus noch vorwiegend politische Ziele zu erreichen versucht, weshalb man auch Rücksicht auf die gegnerische Bevölkerung nehmen musste. Das hat sich mit 9/11 geändert. Fundamentalistische, vorwiegend islamische Gruppierungen verfolgen nicht mehr dieses weltliche Ziel, womit auch gewisse Hemmschwellen wegfallen. Wir müssen daher in Zukunft mit höheren Schäden durch Terrorismus rechnen. Gleichzeitig ist das ein wichtiger Indikator, uns nicht zu sehr auf mögliche Akteure zu konzentrieren, sondern vielmehr auf unsere Verwundbarkeiten.

---

12 Vgl. Anti-Terror-Kampf kostet USA eine Billion Dollar. In: Die Welt, 14.05.2011. <http://www.welt.de/politik/ausland/article13371713/Anti-Terror-Kampf-kostet-USA-eine-Billion-Dollar.html>, abgerufen am 23.10.2014.

13 Gem. <http://de.statista.com/statistik/daten/studie/2006/umfrage/gefallene-oder-verungluecke-soldaten-der-westlichen-koalition-in-afghanistan/> sollen in Afghanistan rund 3.250 und gem. <http://icasualties.org/Iraq/Fatalities.aspx> im Irak rund 4.800 Soldaten westlicher Armeen ums Leben gekommen sein.

14 Saurugg, Herbert: Blackout. Eine nationale Herausforderung bereits vor der Krise. Seminararbeit, Universität Wien 2012.

1.3.7 Ursachen für Terrorismus

Die gegenwärtige „Terrorismusbekämpfung" ist weitgehend nur eine Symptombekämpfung. Selten wird versucht, den möglichen Ursachen auf den Grund zu gehen und dort anzusetzen. Der deutsche Risikoforscher Ortwin Renn sieht gerade in der zunehmenden Unzufriedenheit mit ungerechten Vermögens- und Machtverhältnissen eine Ursache, die zu sozialer Unzufriedenheit bis hin zu aggressiven Handlungen, wie sozialem Aufruhr, Fanatismus und Terrorismus führt.[15] Um wirklich einen Beitrag für eine sichere Zukunft zu leisten, müsste hier angesetzt werden. Leider stehen dazu nicht einfache technische Lösungen mit großen Versprechungen zur Verfügung.

1.3.8 Cyber-Bedrohungen

Ähnlich wie bei Terrorismus erfolgt die Auseinandersetzung auch mit Cyber-Bedrohungen. Während sie lange vernachlässigt wurden, ist auch hier sehr viel Aktionismus und Scheinsicherheit zu beobachten, was sich etwa bei Aussagen wie

> „Als Kernelemente werden der Verlust der Vertraulichkeit von Informationen, die digitale Spionage und das Einschleusen von Computerviren genannt. Die Cyberkriminalität hat ebenfalls einen steigenden Stellenwert, jedoch mit dem Hintergrund eines Betruges von professionellen Kriminellen und ist weniger als Machtprojektion zu bewerten."

widerspiegelt.[16] Auch hier orientieren wir uns an der Vergangenheit und am bisher Erlebten.

Die wirkliche Bedrohung für unsere Sicherheit und Gesellschaft ist nicht der Datenverlust, sondern die Gefahr, dass unsere zunehmend mit dem Internet verbundene Kritische Infrastruktur – durch welches Ereignis auch immer – physisch ausfallen könnte, was wiederum zahlreiche Dominoeffekte nach sich ziehen würde. Unsere derzeitige Systemgestaltung und Abhängigkeit lässt ein Versagen nicht zu. Wir haben viele überlebenswichtige Infrastruk-

---

15 Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten. Frankfurt am Main 2014.

16 Siehe Kapitel 3.3.

turen als „too big to fail“ gestaltet, ohne dass wir uns dessen bewusst wären, noch dass wir einen Plan B hätten, sollte es zu größeren Störungen kommen. Dabei geht die Gefahr nicht nur von Angreifern aus, sondern ist auch systemimmanent. Am 1. Jänner 2010 versagten etwa in Deutschland unzählige EC- und Kreditkarten, da die Mikrochips fehlerhaft programmiert worden waren. Die betroffenen Kunden konnten weder an Geldautomaten Bargeld abheben noch damit bargeldlos bezahlen.[17] Ein solcher Fehler in wichtigen Komponenten in einer hoch vernetzen Infrastruktur hätte wahrscheinlich verheerende Folgen, wie etwa auf der Hackerkonferenz Black Hat 2014 wieder einmal aufgezeigt wurde. Forschern ist es gelungen, einen in Spanien bereits millionenfach ausgerollten intelligenten Stromzähler („Smart Meter“) zu kompromittieren und eine Fernabschaltung über das Netzwerk zu initiieren.[18] Ein neues Geschäftsmodell für die Organisierte Kriminalität – die Gesellschaft ist massiv erpressbar geworden.

Ein anderes Beispiel für unsere „blinden Flecken“ zeigt der Bericht „Power Supply Dependencies in the Electronic Communications Sector“[19] von der European Union Agency for Network and Information Security (ENISA) auf. Als Nebenprodukt der Erfassung von Cyber-Vorfällen in der EU stellte sich heraus, „power cuts are a dominant cause of severe network and service outages in the EU's electronic communications sector“. Die höchsten Schäden werden demnach durch Überlastung, Stromausfälle und durch Softwarefehler verursacht. Wobei natürlich zu berücksichtigen gilt, dass in einem komplexen System eine kleine Ursache verheerende Auswirkungen nach sich ziehen kann. Aber wenn schon nicht einmal einfache Hausaufgaben gemacht wurden, bedeutet das wohl, dass die Verwundbarkeit dieser Systeme weit höher ist, als gemeinhin angenommen wird; auch wenn über-

---

17 Vgl. Geldautomatenproblem: 2010-Bug lässt Bankkunden verzweifeln. In: Spiegel Online, 04.01.2010. <http://www.spiegel.de/netzwelt/netzpolitik/geldautomatenproblem-2010-bug-laesst-bankkunden-verzweifeln-a-670062.html>, abgerufen am 16.06.2015.

18 Vgl. Thoma, Jörg: Intelligenter Stromzähler. Gehackte Smart Meter machen Lichter aus. <http://www.golem.de/news/intelligente-stromzaehler-gehackte-smart-meter-machen-lichter-aus-1410-109923.html>, abgerufen am 24.10.2014.

19 European Union Agency for Network and Information Security (ENISA): Power Supply Dependencies in the Electronic Communications Sector. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies>, abgerufen am 24.10.2014.

raschender Weise noch keine größeren Zwischenfälle passiert sind. Wir befinden uns hier wahrscheinlich in einer gefährlichen „Truthahn-Illusion“[20].

Aktuelle Cyber-Sicherheitskonzepte berücksichtigen diese Faktoren kaum. Ganz abgesehen davon, dass Cyber-Defence in einem vernetzten System keine zweite Verteidigungslinie darstellt, wie das gerne gesehen wird.

1.3.9 „Blinde Flecken“

Unser genereller Fokus auf die Bekämpfung von möglichen Akteuren führt dazu, dass wir viele Dinge übersehen, die eigentlich weit gravierender sind. Terrorismus kann nur wirken, wenn wir es zulassen. Einerseits durch unsere Reaktionen und andererseits, indem wir ihm entsprechende Verwundbarkeiten anbieten. Während in den letzten Jahren für die Erhöhung der Flugsicherheit viele Milliarden Euro aufgewendet wurden, haben wir gleichzeitig zugelassen, dass unsere Infrastrukturen immer verwundbarer geworden sind.

Durch die technische Vernetzung haben wir meist unbewusst hochkomplexe und wechselseitig abhängige Systeme mit möglicherweise verheerenden systemischen Risiken geschaffen. Dementsprechend sind wir auch in keiner Weise auf daraus resultierende strategische Schockereignisse („Schwarzer Schwan“)[21] vorbereitet. Egal, ob das die europäische Stromversorgungsinfrastruktur, die Telekommunikations- und Internetinfrastrukturen oder die Lebensmittelversorgung betrifft, wir bewegen uns in vielen Bereichen auf sehr dünnem Eis. Ein größeres Ereignis in einem Sektor würde weitreichende Dominoeffekte, selbst über Systemgrenzen hinaus,

---

[20] Ein Truthahn, der Tag für Tag von seinem Besitzer gefüttert wird, nimmt aufgrund seiner täglich positiven Erfahrung an, dass die Wahrscheinlichkeit, dass etwas Gravierendes passiert, von Tag zu Tag kleiner wird. Gleichzeitig steigt sein Vertrauen mit jeder positiven Erfahrung (Fütterung). Am Tag vor Thanksgiving (bei dem traditionell die Truthähne geschlachtet werden) erlebt der Truthahn allerdings eine fatale Überraschung.

[21] Ein Ereignis mit den drei Attributen Seltenheit, massive Auswirkungen und Vorhersagbarkeit im Rückblick (allerdings nicht in der Vorausschau). Siehe Taleb, Nassim Nicholas: Der Schwarze Schwan. Die Macht höchst unwahrscheinlicher Ereignisse. München 2013.

auslösen. Eine europäische Großstörung im Stromversorgungssystem („Blackout“) hätte verheerende Folgen, nicht nur für die Elektrizitätswirtschaft, sondern für die gesamte Gesellschaft, sind wir doch völlig von der einwandfrei funktionierenden Stromversorgung abhängig.[22] Ein solches Ereignis würde gleichzeitig unser Finanz- und Wirtschaftssystem auf eine gewaltige Belastungsprobe stellen, wenn nicht sogar weitere weitreichende Dominoeffekte auslösen. Dabei ist irrelevant, wodurch und durch wen ein solches Ereignis ausgelöst wird. Ob durch technische Pannen, Naturereignisse oder durch Terrorismus. Daher sollte unser Fokus und unsere Energie weniger auf mögliche Akteure gelegt werden als vielmehr auf die Angriffsflächen, die wir meist unbewusst geschaffen haben. Dabei geht es nicht nur um die Verwundbarkeit unserer Infrastrukturen, sondern ebenso um die Fähigkeit, als Gesellschaft mit solchen Störungen sinnvoll umzugehen.

1.3.10 Systemische Risiken

Die chaotische und nicht-systemische technische Vernetzung der vergangenen Jahre hat dazu geführt, dass in unserer Gesellschaft und in den Kritischen Infrastrukturen die Anzahl der systemischen Risiken massiv angestiegen ist.[23] Diese sind gekennzeichnet durch:

- einen hohen Vernetzungsgrad (Dynamik, Komplexität, Wechselwirkungen)
- der Gefahr von Dominoeffekten
- einer Nicht-Linearität in den Auswirkungen (keine einfachen Ursache-Wirkungsketten, die durch das standardisierte Risikomanagement erfasst werden) und
- durch eine systematische Unterschätzung durch Verantwortungsträger.

---

[22] Vgl. European Union Agency for Network and Information Security (ENISA): Power Supply Dependencies in the Electronic Communications Sector. Survey, analysis and recommendations for resilience against power supply failures. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/power-supply-dependencies>, abgerufen am 22.10.2014.

[23] Vgl. Zurich Insurance Company Ltd and Atlantic Council of the United States (Hrsg.): Beyond data breaches. Global interconnections of cyber risk. <http://www.atlanticcouncil.org/publications/reports/beyond-data-breaches-global-interconnections-of-cyber-risk>, abgerufen am 23.10.2014.

Das hat dazu geführt, dass die Wahrscheinlichkeit von strategischen Schockereignissen, also Ereignissen, die in der Lage sind, unser Zusammenleben nachhaltig – langfristig und erheblich – zu verändern („Game-Changer"), massiv angestiegen ist. Dabei wird hier noch gar nicht direkt auf die richtig großen Themen unserer Zeit eingegangen:[24]

1. Bedrohungen durch menschliche Interventionen in das Ökosystem Erde (z.B. Klimawandel, Ressourcenknappheit, Süßwasserkrise, Gefährdung der Artenvielfalt)
2. Bedrohungen durch Steuerungsdefizite in der Wirtschaft und Gesellschaft (Umgang mit öffentlichen Gütern, Finanzkrisen, Pandemien).
3. Bedrohungen durch soziale Fehlentwicklungen (ungleiche Lebensbedingungen).

Hinzu kommt, dass sich ohnmächtig fühlende Menschen oder Gruppierungen heute mithilfe moderner Technologien große Wirkungen bis hin zu Katastrophen auslösen können (kleine Ursache, große Wirkung). Die Terroranschläge von 9/11 wurden in letzter Konsequenz mit einem einfachen Teppichmesser ausgelöst:

> „Mit dieser Waffe können zwar Menschen ermordet werden, aber zu einem systemischen Risiko wird sie erst dann, wenn sie mit der Verwundbarkeit moderner vernetzter Technologien verbunden wird. Denn mit Hilfe eines Teppichmessers gelangten die Terroristen in den Besitz von wesentlich wirksameren Waffen wie Flugzeuge, die sie wiederum nutzten, um die Verwundbarkeit komplexer Hochhausstrukturen auszunutzen. Die Kaskade von einfachen Mitteln hin zu globalen Auswirkungen wird durch die beschriebenen Zusammenhänge der technischen Entwicklung, der Virtualisierung und der Zunahme der Verwundbarkeit ermöglicht. [...] Dazu kommt der Potenzierungseffekt [Dominoeffekt] durch Globalisierung und Vernetzung, durch den auch Machtmissbrauch, kriminelle Handlungen und Terrorismus eine wesentlich höhere Wirkmächtigkeit besitzen als früher."[25]

---

[24] Vgl. Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten. Frankfurt am Main 2014.

[25] Ebd., S. 494.

1.3.11 Risikowahrnehmung

Ein wesentlicher Grund für die vielen „blinden Flecken" ist darauf zurückzuführen, dass unsere Risikowahrnehmung vorwiegend auf vergangenen Erfahrungen und auf stark gefilterten Informationen aus den Medien passiert. Ersteres ist evolutionär bedingt und hat bisher ausgereicht. Aber auch institutionell aufbereitete Informationen unterliegen meist einer vorgefertigten Deutungshoheit bzw. geben meist nur einem Teilausschnitt der Wirklichkeit wieder.[26] Zudem wird die Öffentlichkeit einem Wechselbad von Dramatisierungen (Medien) und Verharmlosungen (Politik) ausgesetzt. Die Vielzahl an Themen und der ständige Zeitdruck lassen tiefer gehende Betrachtungen meist nicht zu. Zusätzlich wird häufig eine starke Vereinfachung eingefordert („Managementbriefing"). Ganz abgesehen davon, dass unsere Steuerungsmechanismen (Management) nach wie vor auf das industriegesellschaftliche Denken und Handeln bei einfachen und komplizierten Systemen (Maschinen) ausgerichtet sind.

Es gibt eine Vielzahl an falsch (und zum Teil irrational) wahrgenommenen Risiken. Während wir bei einzelnen vermeintlichen Risiken schon fast hysterisch reagieren, wie etwa zuletzt bei Ebola[27], nehmen wir andere weit bedrohlichere Risiken so gut wie überhaupt nicht war, wobei gerade Ebola ein Beispiel für Ambivalenz ist. Während die Gefahr in den betroffenen Gebieten zu lange unterschätzt wurde, wird sie bei uns völlig überschätzt. In Österreich sterben im Vergleich dazu jährlich rund 8.000 Menschen direkt oder indirekt an den Folgen von Alkoholkonsum, oder anders ausgedrückt, etwa 16-Mal so viel wie im Straßenverkehr.[28] In der EU sterben derzeit geschätzte 25.000 Menschen jährlich an Infektionen mit multiresistenten Keimen. Die damit verbundenen

---

[26] Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit, Hochschule für Management Budapest 2013.

[27] Wo bis Ende Mai 2015 rund 11.000 Menschen gestorben sind. WHO: Ebola Situation Report - 27 May 2015. <http://apps.who.int/ebola/current-situation/ebola-situation-report-27-may-2015>, abgerufen am 16.06.2015.

[28] Universität Salzburg: Alkohol. Fakten und Mythen. <http://www.uni-salzburg.at/index.php?id=50709>, abgerufen am 24.10.2014.

Sekundärkosten werden mit jährlich rund 1,5 Milliarden Euro beziffert.[29]

Im Zusammenhang mit Terrorismus wird auch gerne der globale Finanzmarkt mit der Möglichkeit der einfachen Finanzierung und Kapitalverschiebungen diskutiert.[30] Aufgrund der Finanzkrise 2007/2008 könnte man aber auch zum Schluss kommen, dass ein viel höheres Risiko von den Finanzmärkten selbst ausgeht und die Anzahl der Opfer – indirekt auch Todesopfer – durch den überbordenden Finanzkapitalismus weit höher sind. Doch das sieht man nicht so offensichtlich, bzw. widerspricht es unseren derzeitigen Denkmodellen. Wir haben hier kognitive Grenzen.

Ein anderes Beispiel stellt der Risikobericht 2012 der Schweiz dar.[31] Daraus geht hervor, dass eine Pandemie und ein Ausfall der Stromversorgung als größtes Risiko für die Schweiz in Bezug auf Schadensausmaß und Eintrittswahrscheinlichkeit darstellen. Gleichzeitig sprechen wir von einem europäischen Verbundsystem, in welchem alle Länder im gleichen Umfang betroffen wären, ähnlich einer Pandemie. Doch kaum ein anderes Land in Europa setzt sich derart intensiv damit auseinander. Ganz abgesehen davon, dass eine Bewältigung nur auf Behördenebene (Krisenmanagement) nicht möglich ist und es einer umfassenden gesellschaftlichen Auseinandersetzung erfordern würde, um mit derartigen strategischen Schockereignissen sinnvoll umgehen zu können.

1.3.12 Hybride Bedrohungspotenziale

Aber was hat das nun alles mit hybriden Bedrohungen zu tun? Sehr viel, obwohl es auf den ersten Blick viele Widersprüchlichkeiten zu geben scheint. Mit der Definition hybrider Bedrohungen wurde versucht, den realen Entwicklungen Rechnung zu tragen.[32] Dabei erfolgte jedoch ein Klassifizierungsversuch in

---

29 Hell, Markus: Clostridium-difficile-Infektion, antibiotikaassoziierte Diarrhö/Colitis. Nosokomiale Last. <http://www.medmedia.at/univ-innere-medizin/infektiologie-nosokomiale-last/>, abgerufen am 24.10.2014.

30 Siehe Kapitel 2.2 – Zudem erleichtern „globale Finanzmärkte" Kapitalverschiebungen von Terroristen.

31 Bundesamt für Bevölkerungsschutz (BABS): Katastrophen und Notlagen. Schweiz. Risikobericht 2012. <http://www.alexandria.admin.ch/bv001490434.pdf>, abgerufen am 24.10.2014.

32 Siehe Kapitel 1.3.

der bisher erfolgreichen Denklogik, etwa indem von „Akteuren", „Interessendurchsetzung" oder von einer „strategischen Schwelle" ausgegangen wird. Diese „Silos" stehen jedoch im Widerspruch zur Netzwerkgesellschaft und zu den realen Entwicklungen. Dies wird etwa auch bei der „Akteurs-Übersicht Hybride Bedrohung"[33] ersichtlich. Hier wurden bisher klar identifizierbare und übliche „Silos" gegenübergestellt, das Ganze ist auch übersichtlich darstellbar, entspricht jedoch kaum den Realitäten. Denn zwischen den unterschiedlichen Domänen gibt es vielschichtige Vernetzungen und Querverbindungen („unsichtbare Fäden") mit zeitlich verzögerten Wirkungen oder Abhängigkeiten. Daher entsprechen die daraus ableitbaren Konsequenzen der bisherigen Logik, die aber für VUCA Entwicklungen nur bedingt bis gar nicht tauglich sind.

Wenn man jedoch versucht, die Ausgangsfrage „Welche Faktoren sind für die Souveränität eines Staates (Staatengemeinschaft) ausschlaggebend" in einem Modell darzustellen, wird es sehr rasch unübersichtlich (Abbildung 11).

Daran ist aber nicht das Modell schuld, sondern unser Wunsch, komplexe Sachverhalte möglichst einfach darzustellen, was zu starken, leicht darstellbaren Vereinfachungen führt, aber mit den tatsächlichen Realitäten nur wenig zu tun hat. Eine Vielzahl an gescheiterten Großprojekten sind stumme Zeugen davon.

Aus der Forschung ist bekannt, dass unser Hirn die möglichen Wechselwirkungen zwischen max. 3-4 Faktoren erfassen kann. Alles, was darüber hinaus geht, erfordert Hilfsmittel und Visualisierungen. Eine Möglichkeit ist, wie im Modell „Souveränität eines Staates (Staatengemeinschaft)" (Abbildung 11) begonnen wurde, die möglichen Wechselwirkungen und Zusammenhänge zu erfassen und darzustellen. Durch weiterführende Analysen können dann zeitverzögerte bzw. sonst nicht erfassbare Wechselwirkungen aufgespürt werden.

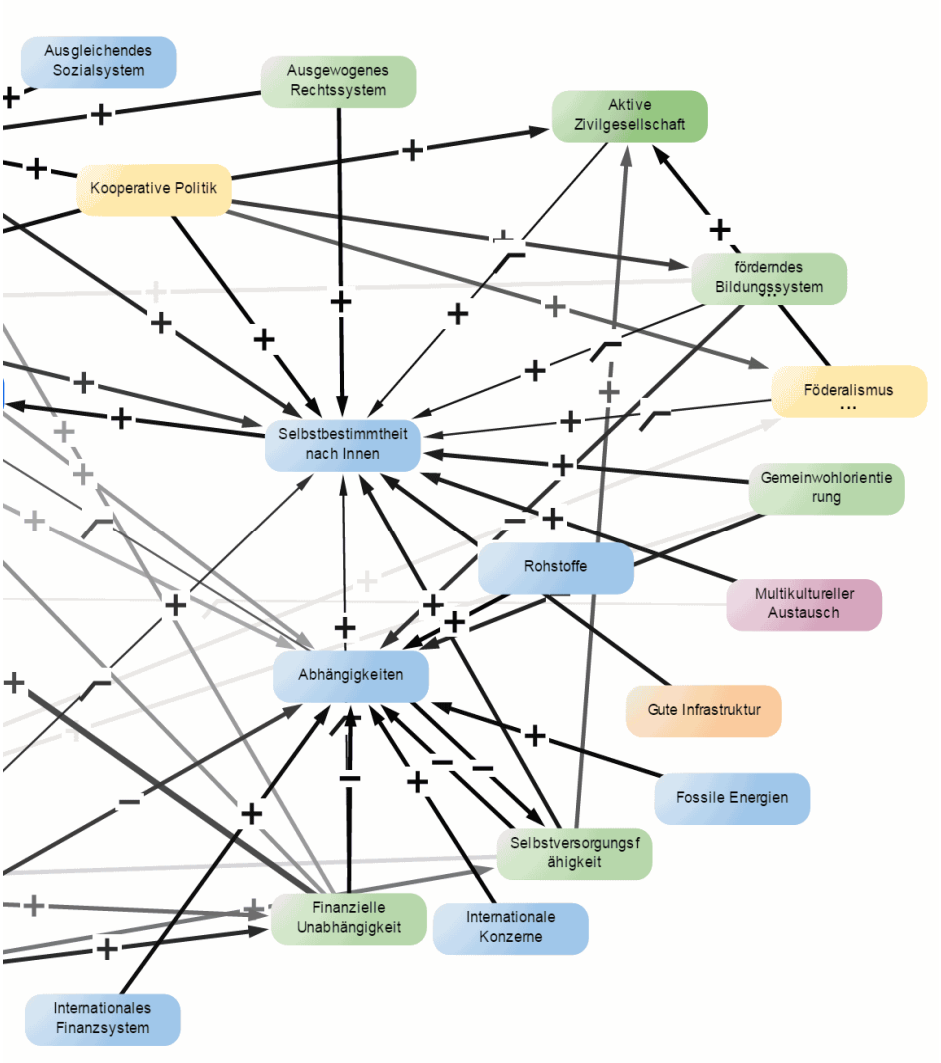
Andererseits bietet Modellieren die Möglichkeit, einzelne Aspekte isoliert zu betrachten und hervorzuheben, ohne jedoch dabei mögliche Wechselwirkungen außer Acht zu lassen (Abbildung 12). Ein Modell erlaubt es auch, mögliche widersprüchliche Ansichten zu erfassen, die es so gut wie immer geben wird.[34]

---

[33] Siehe Abbildung 3.

[34] Vgl. VUCA - volatil, unsicher, komplex und ambivalent.

Abbildung 11: Welche Faktoren sind für die Souveränität eines Staates (Staatengemeinschaft) ausschlaggebend
Herbert Saurugg


Ausgleichendes Sozialsystem
Ausgewogenes Rechtssystem
Aktive Zivilgesellschaft
Kooperative Politik
förderndes Bildungssystem
Föderalismus
Selbstbestimmtheit nach Innen
Gemeinwohlorientierung
Rohstoffe
Multikultureller Austausch
Abhängigkeiten
Gute Infrastruktur
Fossile Energien
Selbstversorgungsfähigkeit
Finanzielle Unabhängigkeit
Internationale Konzerne
Internationales Finanzsystem

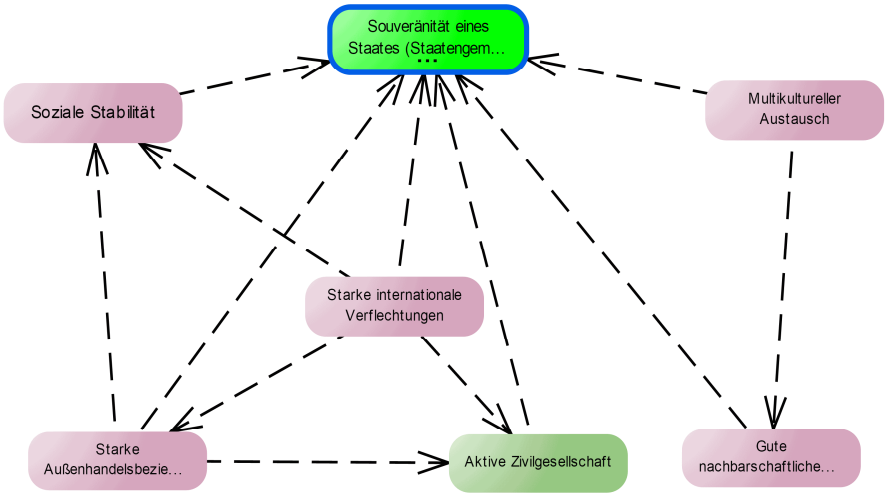


Abbildung 12: Welche Faktoren sind für die Souveränität eines Staates (Staatengemeinschaft) ausschlaggebend, reduzierte Darstellung
Herbert Saurugg

Aber auch ein Modell ist keine Abbildung der Wirklichkeit, sondern nur ein Versuch, dieser näher zu kommen. Hier bietet sich der Vergleich zwischen Gelände und Karte an. Nicht die Detaildichte führt zu einem besseren Ergebnis, sondern indem die wesentlichen Merkmale des Geländes abgebildet sind. Diese sind natürlich je nach Bedarf unterschiedlich, etwa ob man zu Fuß oder mit dem Flugzeug unterwegs ist. Und so ist es auch mit Modellen, die einen Wirklichkeitsausschnitt wiedergeben sollen. Sie dienen als Kommunikationsinstrument, um eine gemeinsame Sicht zu schaffen. Um die tatsächlichen Abhängigkeiten und Realitäten bei der Souveränität eines Staates (Staatengemeinschaft) erfassen zu können, müssten daher auch Akteure aus den unterschiedlichen „Silos“ mitwirken, um zu einem bestmöglichen Abbild der Realität zum Zeitpunkt der Erstellung zu kommen. Und das wir aufgrund der heutigen Dynamiken und Geschwindigkeiten zunehmend schwieriger. Genau genommen bedürfte es eines fortlaufenden Prozesses. Daher wäre, wie bei den Länderanalysen festgestellt

wurde, durchaus zu hinterfragen, ob nicht formalisierte (Schweden)[35] bzw. veraltete Strategien (Slowakei)[36] wirklich einen Mehrwert liefern.

1.3.13 Aber wie kann man dann mit hybriden Bedrohungen umgehen?

Indem man die Ausgangsdefinition[37] kritisch hinterfragt und prüft, ob diese aufgrund der bisherigen Ausführungen wirklich zweckmäßig oder ob es nicht vielmehr notwendig ist, eine neue Fragestellung zu definieren. Wenn wir davon ausgehen, dass die Zukunft volatiler, unsicherer, komplexer und ambivalenter (VUCA) wird, dann brauchen wir wohl auch neue Denkmodelle.

Die einzelnen Länderstrategien weisen durchaus erfolgversprechende Ansätze auf. Etwa in Schweden, wo man nicht auf formalisierte Strategien und auf niedergeschriebene Konzepte Wert legt, sondern vielmehr auf eine flexible und der Realität angepassten Kooperationskultur, auch wenn aus der Analyse hervorgeht, dass bei der praktischen Umsetzung noch Verbesserungsbedarf besteht.[38] Bei vielen Strategien stellt sich bei einer näheren Betrachtung heraus, dass es zwischen den formalisierten „Wunschvorstellungen" und der tatsächlichen Umsetzung erhebliche Differenzen gibt. Gerade in Österreich finden sich einige Beispiele dafür.

Auch die Aussage von Michael Miklaucic, Director of Research and Editor of PRISM at the Center for Complex Operations at National Defense University, „*A hybrid threat is more than just the sum total of its constituent parts. Com-*

---

35 Siehe Kapitel 2.2.

36 Siehe Kapitel 2.1.

37 Siehe Kapitel 1.3.

38 Siehe Kapitel 2.2.1: „Es gibt nicht einmal Weiß- oder Grünbücher, die mit der nationalen Sicherheit befasst sind. Bedrohungen werden in der Regel nicht mit veröffentlichten Konzepten, sondern pragmatisch begegnet, abhängig von der jeweiligen Situation."; siehe auch Kapitel 2.2.2 „Schwedens sicherheitspolitische Ausrichtung ist von einer sehr starken Kooperationskultur geprägt."

bating such threats does not require new capabilities as much as new partners, new processes and, above all, new thinking" ist völlig treffend.[39]

Ein anderer Aspekt, der in der schwedischen Analyse hervorsticht, ist das Amt für Bevölkerungsschutz und Bereitschaft.[40] Während man etwa auch in Deutschland über ein Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder in der Schweiz über ein Bundesamt für Bevölkerungsschutz (BABS) verfügt, gibt es in Österreich keine derartige Einrichtung. Der Katastrophenschutz ist in Österreich Ländersache und dementsprechend heterogen ist dieser auch abgebildet. Nationale oder sogar internationale Krisenlagen oder strategische Schockereignisse können damit nur unzureichend abgebildet werden. Die Erfassung von systemischen Risiken ist dadurch ebenfalls nur unzureichend gegeben. Bei einer derartigen Organisationsstruktur ist aber darauf zu achten, dass nicht wieder ein neuer Silo geschaffen wird, sondern ein Vernetzungsinstrument. Denn viele erforderliche Systemelemente sind bereits heute auf irgendeine Art und Weise abgebildet. Was fehlt, ist die bedarfs- und zielorientierte Vernetzung unter Hintanhaltung des bisherigen „Silodenkens und -verhaltens".[41]

Indirekt wird das auch in der slowakischen Analyse von Rastislav Báchora angesprochen, in welcher ein Schulterschluss zwischen institutionellen, nichtstaatlichen als auch zivilgesellschaftlichen und kommerziellen Akteuren eingefordert wird.[42] Grundsätzlich wurde dieser Gedanke in Österreich bereits in der Umfassenden Landesverteidigung (ULV) und heute in der Umfassenden Sicherheitsvorsorge (USV) formalisiert. Die Realität blieb aber immer deutlich hinter den vorgefassten Zielvorstellungen.

---

39 NATO: Countering the Hybrid Threat. <http://www.act.nato.int/nato-countering-the-hybrid-threat>, abgerufen am 23.10.2014.

40 Siehe Kapitel 2.2.1: „Ein wichtiger Akteur ist das Amt für Bevölkerungsschutz und Bereitschaft (MSB; Swedish Civil Contingencies Agency). Die Aufgabe des MSB besteht darin, die gesellschaftlichen Kapazitäten zu verbessern und die Vorbereitung auf und die Prävention von Notfällen und Krisen zu unterstützen."

41 Vgl. Saurugg, Herbert: Die Netzwerkgesellschaft und Krisenmanagement 2.0. Masterarbeit, Hochschule für Management Budapest 2013.

42 Die institutionelle Zusammenarbeit bei der Bekämpfung von Bedrohungen schließt sowohl nichtstaatliche als auch zivilgesellschaftliche, aber auch kommerzielle Gruppen ein.

Durch standardisierte und vereinfachte Prozesse wurden in den vergangenen Jahren große Fortschritte bei Standardeinsätzen gemacht, die auch zu einer sehr hohen Versorgungsqualität geführt haben. Eine organisationsübergreifende Zusammenarbeit von Einsatzorganisationen ist zwar mittlerweile State-of-the-Art, aber häufig nur bei konkreten Anlassfällen. Eine gemeinsame Ausbildung bzw. zumindest übergreifende Ausbildungsmodule stecken noch in den Kinderschuhen bzw. sind auf Einzelbereiche beschränkt. Die Interoperabilität zwischen den zivilen und militärischen Einsatzorganisationen wurde zwar verbessert (etwa bei der Führungsorganisation), jedoch gibt es noch ein großes Verbesserungspotential, um auch mit den Auswirkungen von möglichen strategischen Schockereignissen fertig zu werden. Ganz zu schweigen von der Herausforderung bei der Zusammenarbeit mit „ungebundenen Helfern“[43], wie etwa mit den Mitgliedern des Team Österreichs bei Katastrophenlagen.

Ein anderes Beispiel ist die zivilgesellschaftliche Initiative „Plötzlich Blackout!“ - Vorbereitung auf einen europaweiten Stromausfall.[44] Während es bisher in Österreich von institutioneller Seite kein nationales Szenario für einen möglichen plötzlichen, überregionalen und länger andauernden Stromausfall („Blackout“) gibt, thematisiert die Initiative dieses Szenario seit Herbst 2013 und hat bei verschiedenen Veranstaltungen mehrere hundert Organisationen aus allen gesellschaftswichtigen Bereichen (Behörden, Einsatzorganisationen, Unternehmen, Forschung und Zivilgesellschaft) eingebunden und sogar eine internationale Vernetzung geschaffen. Gerade bei neuen Themen ist die Zivilgesellschaft häufig flexibler und schneller. Dieses Potential sollte bei sicherheitspolitischen Themen stärker berücksichtigt werden.

Möglicherweise wird der zunehmende finanzielle Druck dazu führen, dass die Gesellschaft in Zukunft mehr auf Synergiemöglichkeiten achten werden. Gerade die österreichische Kultur ist durch den „kleinen Dienstweg“

---

43 Vgl. Kircher, Friedrich: Ungebundene Helfer im Katastrophenschutz. Die Sicht der Behörden und Organisationen mit Sicherheitsaufgaben. <http://www.katleuchtturm.de/assets/content/images/pdfs/593_597_Kircher.pdf>, abgerufen am 22.10.2014.

44 Siehe Resilienz Netzwerk Österreich, Plötzlich Blackout! Vorbereitung auf einen Europaweiten Stromausfall. <www.ploetzlichblackout.at>, abgerufen am 22.11.2014.

geprägt. Dort wo formalisierte Strukturen unzureichend sind, bilden sich informelle Wege („unsichtbare Fäden"), die zum Gelingen beitragen. Das Gegenbeispiel ist die Androhung „Dienst nach Vorschrift" zu versehen. Die Österreicher handeln häufig intuitiv nach den Grundsätzen der Netzwerkgesellschaft, sich flexibel und ad-hoc zu vernetzen, um einen Mehrwert zu schaffen. Um diese Eigenschaft werden wir anderorts häufig beneidet. Wir sollten sie daher bewusst als Stärke wahrnehmen, fördern und im Sinne des Ganzen nutzen.

1.3.14 Verwundbarkeiten

Wie sich aus den vorangegangenen Ausführungen ableiten lässt, sollten wir stärker auf Verwundbarkeiten als auf mögliche Akteure achten. Auch für die möglichen Akteure im Sinne der Definition von hybriden Bedrohungen ist es zunehmend schwieriger bis unmöglich, die eigenen Interessen gegenüber Dritte durchzusetzen. Für sie gelten die Gesetzmäßigkeiten von komplexen Systemen ebenfalls. Wobei das nicht ausschließt, dass eine temporäre Beeinflussung möglich ist. Hiezu ist es notwendig, nicht nur in den heute in der Betriebswirtschaftslehre üblichen sehr kurzen Zeithorizonten zu denken, sondern längerfristig. Denn viele *Quick and Dirty*-Lösungen konzentrieren sich nur auf die Symptome und lassen sich sofort umsetzen, während fundamentale Lösungen die Ursache des Problems zu beseitigen versuchen. *Quick and Dirty*-Lösungen sind meist schnell angewandt, verschlimmern aber langfristig das eigentliche Problem, während fundamentale Lösungen kurzfristig oft deutliche Nachteile bringen und sich erst langfristig als vorteilhaft herausstellen.[45]

Ein aktuelles Beispiel ist der Konflikt zwischen der EU/Ukraine und Russland. Keine der beiden Seiten kann wirklich abschätzen, welche Folgewirkungen mit den bisherigen Drohgebärden und Sanktionen noch verbunden sein werden. Gleichzeitig sind die Mechanismen dem alten Denken zuzuordnen. Nicht einmal haben historisch Banalitäten in die Katastrophe geführt. Auch hier haben wir zahlreiche „blinde Flecken".

---

[45] Vgl. Ossimitz, Günther/Lapp, Christian. Systeme: Denken und Handeln. Das Metanoia-Prinzip. Eine Einführung in systemisches Denken und Handeln. Berlin 2006.

Seit Monaten gibt es Hinweise auf gezielte Cyber-Angriffe auf westliche Energieversorgungsunternehmen, die vermeintlich aus Russland kommen sollen, was bei Cyber-Angriffen nie eindeutig feststellbar ist.[46] Dennoch sollten die Alarmglocken läuten. 2007 hat die Versetzung eines russischen Denkmals zu einem massiven Cyber-Angriff auf Estland geführt. Damals waren „nur" virtuelle Systeme betroffen. Heute könnte dabei unsere Kritischste Infrastruktur angegriffen und möglicherweise zum Ausfall gebracht werden. Dabei sollte davon Abstand genommen werden, eine solche Möglichkeit nur einem Akteur zuzuordnen. Gerade Cyber-Angriffe können äußerst rasch außer Kontrolle geraten und eine unvorhergesehene Eigendynamik entwickeln, wie das eben in komplexen Systemen möglich ist.

In der Schweiz wurde dieses Szenario als Ausgangsszenario für die Sicherheitsverbundsübung 2014 herangezogen,[47] infolgedessen es zu Instabilitäten im Stromversorgungssystem mit einem dadurch ausgelösten Blackout kommt. Als noch schlimmer wird dabei die darauf folgende mehrwöchige Strommangellage beurteilt, da weder die Gesellschaft noch die Infrastruktur auf ein solches strategisches Schockereignis vorbereitet ist.[48]

Die belgische Regierung hat im Sommer 2014 einen nationalen Notfallplan erlassen, indem für den kommenden Winter nationale Notabschaltungen in der Stromversorgung vorbereitet wurden. Auslöser sind zwei Atomkraftwerke, die aus massiven Sicherheitsbedenken vom Netz genommen werden mussten und die Sorge, dass die Stromversorgung über den Winter nicht

---

46 Thomson, Amy/Rahn Cornelius: Russian Hackers Threaten Power Companies, Researchers Say. <http://www.bloomberg.com/news/2014-06-30/symantec-warns-energetic-bear-hackers-threaten-energy-firms.html>, abgerufen am 24.10.2014.

47 Vgl. Saurugg, Herbert: SVU'14 – Überwinden der Krise. http://www.saurugg.net/2014/blog/stromversorgungssystem/svu14-ueberwinden-der-krise, abgerufen am 24.10.2014.

48 Vgl. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport, Newsletter SVU 14 –Juni, <http://www.vbs.admin.ch/internet/vbs/de/home/themen/security/svu14/dokumente.parsys.9373.downloadList.82421.DownloadFile.tmp/infosvu14junid.pdf>, abgerufen am 26.10.2014.

aufrecht erhalten werden kann. Gleichzeitig bleiben in Europa 22 baugleiche Reaktoren mit denselben kritischen Sicherheitsmängeln im Betrieb.[49]

Die (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) OECD hält in ihrer Studie „Future Global Shocks - Geomagnetic Storms" fest:

> „The lack of valid risk assessments has limited risk mitigation efforts in many critical infrastructure sectors, as it is difficult to demonstrate the utility of investing in either hardening or operational mitigation efforts, especially if these investments reduce time and money spent in preparing for more common risks. [...] Geomagnetic storms can be categorized as a global shock for several reasons: the effects of an extreme storm will be felt on multiple continents; the resulting damage to electric power transmission will require international cooperation to address; and the economic costs of a lengthy power outage will affect economies around the world."[50]

Es gibt eine beachtliche Bedrohung für unsere Infrastruktursysteme, die von geomagnetischen Sonnenstürmen ausgehen. Auch hier ist wiederum unsere Strominfrastruktur aufgrund des derzeitigen Systemdesigns massiv gefährdet.[51]

Im Zusammenhang mit dem schwelenden Konflikt mit Russland wurde ein europäischer Stresstest bei der Gasversorgung durchgeführt. Die Regulierungsbehörden versuchen zu beruhigen, indem festgehalten wird, dass bei einer Unterbrechung der Gaslieferung aus Russland für mehrere Monate keine Gefahr droht. Gleichzeitig hätte 2012 der damalige Engpass in der

---

[49] Vgl. Resilienz Netzwerk Österreich: Belgiens Angst vor dem nächsten Winter. <http://www.ploetzlichblackout.at/2014/08/21/belgiens-angst-vor-dem-nächsten-winter/>, abgerufen am 24.10.14.

[50] OECD/IFP: Futures Project on "Future Global Shocks - Geomagnetic Storms". <http://www.oecd.org/dataoecd/57/25/46891645.pdf>, abgerufen am 24.10.2014.

[51] Vgl. Resilienz Netzwerk Österreich: Ein heftiger Sonnensturm hat die Erde im Juli 2012 knapp verfehlt. <http://www.ploetzlichblackout.at/2014/07/26/ein-heftiger-sonnensturm-hat-die-erde-im-juli-2012-knapp-verfehlt/>, abgerufen am 24.10.2014.

Gasversorgung beinahe zum Blackout geführt. Auch hier wissen wir nicht, welche sonstigen Abhängigkeiten und Wechselwirkungen es noch gibt.[52]

Allein diese wenigen Beispiele weisen auf eine massive Verwundbarkeit unserer Kritischen Infrastruktur und damit auch unsere Gesellschaft hin. All diese Aspekte werden aber bisher beim Thema „Schutz Kritischer Infrastrukturen" kaum berücksichtigt. Dies wurde 2013 auch durch die EU-Kommission eingestanden:

> „The review process of the current EPCIP [European Program for Critical Infrastructure Protection], conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries. [...] The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an interconnected network. Most work has been sectoral, but these methodologies show their limits when cross-sectoral issues need to be addressed, so a systems approach will be by the Commission from now on."[53]

Der Schutz Kritischer Infrastrukturen (SKI) reicht bei weitem nicht mehr aus, sondern wir benötigen ebenso einen „Schutz VOR Kritischer Infrastruktur", einen Plan B, sollte es zu einem größeren Ausfall kommen.

Mittel- bis langfristig kann mit der derzeitigen Systemgestaltung und den hochgradig vernetzten und wechselseitigen Abhängigkeiten Sicherheit und der Schutz der Bevölkerung nicht gewährleistet werden. Daher hat sich in der Natur „small is beautiful" durchgesetzt, da zu große Strukturen anfälliger gegenüber Störungen sind. Die Natur begrenzt nicht die Interaktionen zwischen den Wesen, sondern nur ihre Größe.[54] Es erscheint daher mehr

---

[52] Vgl. Saurugg, Herbert: Druckmittel Gas. Reale Gefahr oder Hysterie? <http://www.saurugg.net/2014/blog/gesellschaft/druckmittel-gas-reale-gefahr-oder-hysterie>, abgerufen am 24.10.2014.

[53] European Commission: Commision Staff Working Document. On a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure. <http://ec.europa.eu/energy/infrastructure/doc/critical/20130828_epcip_commission_staff_working_document.pdf>, abgerufen am 24.10.2014.

[54] Vgl. Vester, Frederic. Die Kunst vernetzt zu denken. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität. Ein Bericht an den Club of Rome. München 2011.

als notwendig, auch bei unseren komplexen technischen Systemen und Lösungen von der Natur zu lernen, um eine langfristige Lebensfähigkeit sicherzustellen.

1.3.15 Systemgestaltung

Die Systemsicherheit jegliches Systems kann mit einfachen Grundregeln – gegenüber jeglichen Störungen – erhöht werden, egal ob eine Störung durch einen Fehler, ein Naturereignis, durch Zufall oder durch einen Aggressor ausgelöst wurde.

1.3.16 Energiebedarfssenkung

Jede evolutionäre Weiterentwicklung erfolgt in der Natur über eine Energiebedarfssenkung. Damit können die externen Abhängigkeiten reduziert und die Lebensfähigkeit eines Systems erhöht werden. Wobei dies nicht nur die klassischen Energieformen betrifft. Auch unser hochgradig synchronisiertes Logistik- und Versorgungssystem für unsere Lebensmittelgrundversorgung weist massive Verwundbarkeiten auf.[55] Ganz zu schweigen vom hohen Energieaufwand, der durch die Transport- und Verarbeitungsprozesse notwendig ist. Zudem ist eine Energieversorgung wie bisher mit einer volatilen Erzeugung nicht möglich. Die Energiewende kann nur gelingen, wenn wir unseren Bedarf durch intelligente Maßnahmen deutlich senken können. Das erfordert einen Kulturwandel und nicht nur technische Lösungen. Damit können aber auch Abhängigkeiten, wie sie im Industriezeitalter notwendig waren, reduziert werden.

---

[55] Siehe Kapitel 2.1.1: "It is clear that any disruption in the supply of raw materials and goods to Europe would have devastating economic effects on countries including the Netherlands. Securing supply routes, protecting vital infrastructure and promoting stability in states and regions can reduce these risks."

1.3.17 Dezentralität

Der zweite Aspekt ist die Dezentralität. Komplexe Systeme lassen sich nicht zentral steuern und organisieren. Sie erfordern dezentrale selbstregulierende Rückkopplungsprozesse. Dezentrale Systeme sind zugleich robuster und resistenter gegenüber Störungen. Dabei spielt die Selbstorganisationsfähigkeit eine wesentliche Rolle, die grundsätzlich systemimmanent vorhanden ist. Dezentralität bedeutet jedoch nicht eine Isolierung oder Abkapselung, ganz im Gegenteil. Dezentralität bedeutet die Bildung von lebensfähigen Strukturen, die durchaus mit anderen Strukturen wieder ein gemeinsames Größeres bilden können (Zellenstruktur), jedoch nicht durch eine chaotische Vernetzung. Viele Strukturen waren bereits vor der technischen Vernetzung vorhanden. Sie müssen nicht neu erfunden werden. Mit den heutigen Möglichkeiten kann jedoch ein zusätzlicher Mehrwert geschaffen werden, ohne dabei das gesamte System aufs Spiel zu setzen.

1.3.18 Fehlerfreundlichkeit

Ein weiterer Aspekt ist die Fehlerfreundlichkeit bzw. Fehlertoleranz in einem System. Wir haben unsere technischen Systeme weitgehend optimiert und versuchen, so weit als möglich, Fehler auszuschließen, was vor allem beim Faktor „Mensch" regelmäßig scheitert. Aber anstatt dass die Technik an die Menschen angepasst wird, wird es weiterhin umgekehrt versucht, mit wenig Erfolgsaussicht. In der Natur werden Störungen nicht ausgeschaltet, sondern in den Verlauf eingebunden. Dazu sind Freiräume, Puffer, Redundanzen, Variationen, Vielfalt, Flexibilität und eine Wandlungs- und Anpassungsfähigkeit erforderlich. Besonders wichtig sind Barrieren, um eine Reichweitenbegrenzung bei Störungen sicherstellen zu können.

Das europäische Stromversorgungssystem verfügt heute nur über unzureichende Barrieren, die eine Ausbreitung einer Störung verhindern könnten. Dadurch kann sich innerhalb weniger Sekunden eine Großstörung über den gesamten Kontinent ausbreiten.

Das Internet verfügt zwar aber unzählige Subnetze, aber es fehlt an der Vielfalt bei den Systemelementen. Dadurch kann sich etwa Schadsoftware

sehr rasch ausbreiten. Zudem sind beide Systeme „too big to fail". Die Fehlerfreundlichkeit eines Systems ist Voraussetzung, damit auch Unsicherheiten und Turbulenzen bewältigt werden können. Und sie beschränkt sich nicht nur auf technische Systeme.

In den letzten Jahren wurde versucht, durch immer höhere Aufwände jegliche Unsicherheiten zu minimieren oder sogar auszuschalten. Die Gesellschaft hat sich zu einer Art „Vollkaskogesellschaft" entwickelt, die immer weniger in der Lage ist, auch mit Turbulenzen oder Ausfällen von wichtigen Infrastrukturen umzugehen. Auch hier sind daher neue Denkansätze erforderlich.

1.3.19 Resilienz

Um die Sicherheit für die Gesellschaft zu erhöhen, ist neben der Berücksichtigung der genannten Aspekte ebenso die Resilienz der Menschen entscheidend. Dieser Begriff ist im deutschsprachigen Raum noch nicht sehr geläufig, gewinnt aber zunehmend an Bedeutung. Er beschreibt die Fähigkeit eines Systems, mit Störungen sinnvoll umzugehen. Er wird auch häufig einfach mit Widerstandsfähigkeit übersetzt, was aber zu kurz greift. Es geht nicht nur um Robustheit, sondern auch um Anpassungs- und Erholungsfähigkeit sowie um Agilität. Dies inkludiert die Fähigkeit, gestärkt aus Störungen herauszugehen. Resiliente Systeme können nach einer Störung in den ursprünglichen Zustand zurückkehren oder auf eine verbesserte transformierte Ebene gelangen. Der Begriff „Resilienz" wird in der Psychologie verwendet, um Menschen zu beschreiben, die trotz widriger Umstände gestärkt aus Krisen hervorgehen, während andere daran zerbrechen.

Was heißt das nun konkret? Viele Menschen sind gewohnt, dass immer irgendjemand zuständig ist und zur Hilfe eilen kann („Vollkaskogesellschaft"). Bei strategischen Schockereignissen sind jedoch die Ressourcen begrenzt. Nur wenn eine gewissen Eigenvorsorge und Eigenverantwortung übernommen wird, lassen sich solche Ereignisse sinnvoll als Gesellschaft meistern. Darüber hinaus führt eine Risikomündigkeit und Selbstwirksamkeit automatisch zu mehr Resilienz. Auswirkungen etwa von hybriden Bedrohungen werden dadurch begrenzt. Das Gesamtsystem Gesellschaft wird resilienter.

1.3.20 Zusammenfassung

Die vorliegende systemische Betrachtung kommt zum Schluss, dass aktuelle sicherheitspolitische Einschätzungen, wie sie etwa auch in der europäischen Sicherheitsstrategie niedergeschrieben wurden, bei weitem nicht ausreichen, um die aktuelle Bedrohungslage zu beschreiben:

> „Bei einer Summierung dieser verschiedenen Elemente – extrem gewaltbereite Terroristen, Verfügbarkeit von Massenvernichtungswaffen, Organisierte Kriminalität, Schwächung staatlicher Systeme und Privatisierung der Gewalt – ist es durchaus vorstellbar, dass Europa einer sehr ernsten Bedrohung ausgesetzt sein könnte."[56]

Eine systemische Betrachtung und vernetztes Denken erscheinen daher unverzichtbar, um mit den aktuellen und zukünftigen Herausforderungen sinnvoll und erfolgreich umgehen zu können. Sicherheit ist immer relativ und subjektiv. Wir haben es aber selber in der Hand, wie wir Betrachtungen und Mittel einsetzen. Sicherheit bedeutet nicht die Ausschaltung von Unsicherheit, sondern einen vernünftigen Umgang damit. Denn Sicherheit und Weiterentwicklung ist ohne Unsicherheit nicht möglich. Beide Pole bedingen einander.[57]

Wie sich aus der Betrachtung auch ergeben hat, sollten wir von den bisher häufig isolierten „Silo"-Betrachtungen abrücken, da diese nicht den vernetzten Realitäten entsprechen und bestenfalls Scheinsicherheiten schaffen. Die veränderten Rahmenbedingungen führen nicht nur dazu, dass die Welt immer undurchsichtiger und unsteuerbarer wird, sondern auch dazu, dass eine Fremdsteuerung schwieriger bis unmöglich wird. Es geht daher weniger um die Erfassung von möglichen Akteuren und konkreten Bedrohungen, als vielmehr um eine aktive und robuste Systemgestaltung, die mit jeglichen Störungen, egal ob durch Angreifer, Fehler, Naturereignisse, oder was auch immer, ausgelöst, umgehen kann.

---

[56] Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>, abgerufen am 24.10.2014.

[57] Vgl. Völkl, Kurt/Wallner, Heinz Peter. Das innere Spiel. Wie Entscheidung und Veränderung spielerisch gelingen. Göttingen 2013.

Um mit den sich daraus ergebenden Ambivalenzen besser umgehen zu können, ist ein „Sowohl-als-auch-Denken" erforderlich. Unser abendländisches „Entweder-oder-Denken" begrenzt die Möglichkeiten und behindert Lösungen. Die alte Weisheit des chinesischen Militärstrategen Sunzi, wonach der Krieg und der Kampf möglichst vermieden werden sollte, hat auch heute noch seine volle Gültigkeit. Wir sollten daher so wenige Angriffsflächen wie nur möglich bieten.

Deshalb ist es notwendig, dass wir die bisherigen „Silos" aufbrechen und eine kooperative Vernetzung und Zusammenarbeit zwischen Politik, Wirtschaft, Zivilgesellschaft und Wissenschaft sicherzustellen. Nur so wird es uns gelingen, systemische Risiken effektiv und effizient zu begrenzen und gleichzeitig den ökologischen, wirtschaftlichen und sozialen Nebenwirkungen der möglichen risikobegrenzenden Maßnahmen genügend Aufmerksamkeit zu schenken.[58] Wesentliche Kennzeichen der Netzwerkgesellschaft sind Transparenz, Partizipation und Kollaboration und die Bildung von adhoc Netzwerken. Nicht der Wettkampf, sondern die Kooperation steht im Vordergrund. Dabei darf nicht erwartet werden, dass sich alle Menschen aktiv einbringen. Wenn es jedoch gelingt, die jeweils „klügsten Köpfe" für das jeweilige Thema zusammenzubringen, dann werden wir auch wieder Lösungen entwickeln, die eine solche Bezeichnung verdienen und auch von der Gemeinschaft getragen werden.

Daraus lassen sich einige Aspekte für die österreichische Sicherheitspolitik und für das Österreichische Bundesheer im Speziellen ableiten:

- Die Wehrpflicht sollte dazu genutzt werden, junge Menschen in der Selbstwirksamkeit und Selbsthilfefähigkeit auszubilden. Dies würde einen großen gesellschaftlichen Mehrwert schaffen und zur Erhöhung der gesamtgesellschaftlichen Resilienz beitragen.
- Das Selbstverständnis des Österreichischen Bundesheeres sollte sich stärker an den neuen Herausforderungen orientieren. Das Österreichische Bundesheer wird weder die Mittel noch das Verständnis für ein Massenheer der Industriegesellschaft erhalten. Die Armee der Netz-

---

[58] Vgl. Renn, Ortwin: Das Risikoparadox. Warum wir uns vor dem Falschen fürchten. Frankfurt am Main 2014.

werkgesellschaft ist kleinteilig, flexibel und anpassungsfähig. Das bedingt vor allem flexiblere Strukturen, die das ermöglichen. D.h. aber auch, dass nicht die Fokussierung auf die Kernaufgaben (militärische Landesverteidigung), sondern eine Flexibilisierung notwendig ist, um auf möglichst viele Szenarien zum Wohle der Bevölkerung reagieren zu können. Unabhängig davon, wodurch diese ausgelöst wurden und ob sie im klassischen Sinn eine militärische Aufgabe darstellen.[59]

- Es ist eine Durchlässigkeit zwischen den unterschiedlichen Sicherheitsdomänen und eine bessere Kooperation erforderlich. Das Österreichische Bundesheer stellt eine gesamtstaatliche strategische Reserve dar, die gesellschaftlich unverzichtbar ist. Dabei geht es nicht nur um militärische Fähigkeiten, sondern um Fähigkeiten und Ressourcen, die sonst nicht vorgehalten werden (können). Dies könnte etwa auch bedeuten, dass Soldaten bei einem strategischen Schockereignis auf lokaler Ebene die Führung und Selbstorganisation übernehmen bzw. unterstützen. Dies erfordert ein Umdenken und eine Anpassung der Organisationskultur.

- Der Schutz Kritischer Infrastruktur muss neu ausgerichtet werden. Stark vernetzte Objekte und Infrastrukturen können nicht mittels Objektschutz geschützt werden. Vielmehr ist zu erwarten, dass Soldaten nach einem möglichen Anschlag nicht zur Absicherung/zum Objektschutz, sondern zum Aufräumen erforderlich sein werden. Andere Maßnahmen, wie etwa die Erhöhung der IT-Sicherheit, stellen nur einen kleinen Teilbereich der heutigen Erfordernisse dar.

- Strategische Schocks können nicht verhindert werden. Wir können zwar die begünstigenden systemischen Risiken minimieren, was dennoch keinen vollständigen Schutz bietet. Wir müssen uns daher so ausrichten und aufstellen, dass wir derartige Ereignisse möglichst rasch überwinden und wieder zu einer neuen Realität zurückfinden können. Ein sinnvoller Umgang mit Unsicherheiten und Ungewissheiten ist

---

[59] Vgl. Gutmann, Günther: Eisregen in Slowenien mit nachfolgendem großflächigen Stromausfall Anfang 2014. In: Truppendienst - Folge 340, Ausgabe 4/2014. <http://www.bundesheer.at/truppendienst/ausgaben/ausgabe.php?folge=340>, abgerufen am 26.10.2014.

dabei essentiell. Dies erfordert jedoch auch einen gesellschaftlichen Diskurs.

- Eine gesamtstaatliche Sicht ist erforderlich. Ein nationales Kompetenzzentrum für den Bevölkerungsschutz erscheint dringend geboten. Einerseits, um die vielschichtigen Problemlagen und systemischen Risiken erfassen zu können und andererseits, um eine nationale oder sogar internationale Koordinierung und Sicht zu gewährleisten. Dabei darf aber kein neuer „Silo" entstehen. Vielmehr ist die Vernetzung der bereits vorhandenen Einzelelemente in den Vordergrund zu stellen. Die Krisenbewältigung selbst muss auch weiterhin auf lokaler/regionaler Ebene und bei Bedarf auch autonom und durch Selbstorganisation erfolgen können.
- Versprechungen von technischen Lösungen sollten nicht unreflektiert akzeptiert werden. Mit vielen vermeintlichen Lösungen werden nur noch größere Probleme geschaffen.

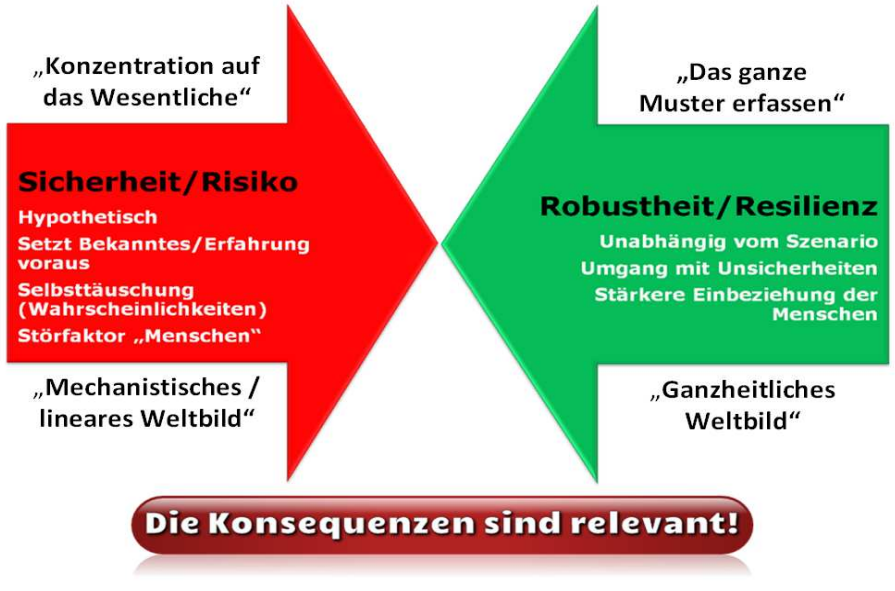


Abbildung 13: Konsequenzen
Herbert Saurugg

2 Darstellung der analysierten Sicherheitsstrategien der Referenzstaaten

Wie eingangs erwähnt fokussierte sich die Analyse auf zwei Staaten, die mit Österreich in einigen Aspekten vergleichbar sind, sich aber bei anderen, wie z.B. bei Kooperations-Perspektiven aufgrund der Zugehörigkeit zu weiteren Bündnispartnern, durchaus unterscheiden. Sicherheitsrelevante Strategiepapiere der Slowakei und Schwedens wurden von Experten aus den entsprechenden Ländern beziehungsweise von Experten mit einschlägigen Sprachkenntnissen auf die Sensibilisierung bezüglich hybrider Bedrohungen analysiert. Fanden sich keine Hinweise auf hybride Bedrohungen, sollten die Experten die in diesen Papieren erwähnten Gewaltakteure auf deren Relevanz zu hybriden Bedrohungen analysieren.

2.1 Slowakei

Rastislav Báchora

2.1.1 Einleitung

Der zeitgemäße Umgang mit hybriden Bedrohungen setzt ein entsprechendes Verständnis für Sicherheit sowie die notwendigen Kapazitäten staatlicher Institutionen voraus. Welche Bedeutung möglichen hybriden Bedrohungen in der slowakischen Sicherheitsstrategie sowie anderen Dokumenten beigemessen wird und welche Handlungsmaßnahmen von welchen Steuerungsinstrumenten bei deren Abwehr konzeptuell und institutionell erfasst werden, wird im Rahmen der vorliegenden Analyse zu klären sein. Vordergründig ist aber kritisch zu hinterfragen, ob ein Dokument wie die Sicherheitsstrategie der Slowakischen Republik (SR) aus dem Jahr 2005 die normativen Voraussetzungen überhaupt erfüllen kann, um den wissenschaftsanalytischen sowie realpolitischen Anforderungen von hybriden Bedrohungen gerecht werden zu können.

In der vorliegenden Untersuchung wird zunächst auf die wesentlichen sicherheitspolitischen Parameter eingegangen. Danach wird schwerpunktmäßig das in der slowakischen Sicherheitsstrategie, der Verteidigungsstrategie, der Strategie des slowakischen Außenministeriums sowie der Konzepte zum Schutz kritischer Infrastruktur erfasste Bedrohungsbild thematisiert. Zudem werden auch Interaktionen unterschiedlicher Institutionen bei der Bekämpfung von Bedrohungen sowie das Internationale Krisen- und Konfliktmanagement (IKKM) in der Sicherheits- und Verteidigungsstrategie untersucht.

2.1.2 Eckdaten der Slowakei

Die SR ist ein Völkerrechtssubjekt, das aus der Auflösung der übergeordneten tschechoslowakischen Staatsstruktur, der sogenannten „Dismembratio“[1], hervorging, und weist hinsichtlich der Fläche, Bevölkerung, Wirtschaft, Mitgliedschaft in internationalen Organisationen sowie ihrer Streitkräfte einige Spezifika auf.

Fläche, Bevölkerung

Die Gesamtfläche der Slowakei beträgt 48.845km^2 und hat eine 1.611km lange Staatsgrenze zu fünf Nachbarstaaten. In der Slowakei lebten mit Stichtag 31. Dezember 2013 insgesamt 5.415.949 Menschen, davon waren 2.639.060 Männer und 2.776.889 Frauen.[2] Im Vergleich zu den Nachbarstaaten hat die SR die jüngste Bevölkerung. Das Durchschnittsalter in der Slowakei beträgt 39,2, in Tschechien 40,9, in Ungarn 41,1 und 44,3 in Österreich.[3] Eine zusätzliche Besonderheit der Slowakei ist der relative hohe Anteil an nationalen und ethnischen Minderheiten, wobei mit 458.467 Personen die Angehörigen der ungarischen Minderheit die zahlenmäßig stärkste Minderheitengruppe darstellen.[4]

---

1 Vgl. Seidl-Hohenveldern, Ignaz: Die Staaten (), In: Neuhold, Hanspeter/Hummer, Waldemar und Schreuer, Christoph (Hrsg.): Österreichisches Handbuch des österreichischen Völkerrechts I. Wien 1997, S. 134ff, hier S. 159.

2 Vgl. Statistikamt der SR. <http://portal.statistics.sk/showdoc.do?docid=65809>, abgerufen am 13.09.2014.

3 Vgl. CIA: CIA Factbook: Slovakia, <https://www.cia.gov/library/publications/the-world-factbook/geos/lo.html>; Poland, <https://www.cia.gov/library/publications/the-world-factbook/geos/pl.html>; Czech Republic, <https://www.cia.gov/library/publications/the-world-factbook/geos/ez.html>; Hungary, <https://www.cia.gov/library/publications/the-world-factbook/geos/hu.html>; Austria, <https://www.cia.gov/library/publications/the-world-factbook/geos/au.html>; abgerufen am 13.09.2014.

4 Vgl. Statistikamt der SR. <http://portal.statistics.sk/showdoc.do?docid=47949>, abgerufen am 13.09.2014.

Wirtschafts- und Arbeitsmarktdaten

Die wirtschaftliche Entwicklung der Slowakei der letzten Jahre war stark von der Finanz- und Wirtschaftkrise beeinflusst. Während die slowakische Wirtschaft bis 2008 starke Zuwächse hatte, verzeichnete das Land im Jahr 2009 einen Rückgang um 5,1% der Wirtschaftsleistung.[5] Aufgrund der Wirtschaftskrise stieg auch die Arbeitslosigkeit, so waren bei Jahresende 2013 ca. 386.000 Menschen oder 14% ohne Arbeit.[6] Die Prognosen für die Wirtschaftsentwicklung wurden nach Ausbruch des Konfliktes in der Ukraine und den EU-Russland-Sanktionen für 2015 mit 2,6% Wachstum nach unten revidiert.

Mitgliedschaft in internationalen/militärischen Organisationen

Internationale Organisationen haben einen zentralen Stellenwert in der Sicherheitsstrategie und dies spiegelt sich sowohl in der Verteidigungsstrategie als auch in der Strategie des slowakischen Außenministeriums wider.[7] Das Außenministerium in Bratislava listet über 30 internationale Organisationen auf, mit denen die Slowakei vertragliche Beziehungen eingegangen ist, wo sie aber nicht überall Mitglied ist.[8] Für die slowakischen außen- und sicherheitspolitischen Prozesse ist die Mitgliedschaft in der UNO, EU, NATO, OSZE, OECD im Europarat und in der Visegrad-Gruppe essentiell.[9]

---

5 Vgl. Statistikamt der SR. <http://www.statistics.sk/pls/eutab/html.h?ptabkod=tsdec100>, abgerufen am 20.09.2014.

6 Vgl. Statistikamt der SR. <http://portal.statistics.sk/showdoc.do?docid=67076>, abgerufen am 20.09.2014.

7 Vgl. Ministerium für Äußeres der SR: Úspešné Slovensko v Bezpečnom svete – Stratégia MZV SR [Erfolgreiche Slowakei in einer sicheren Welt – Strategie des Außenministeriums der SR], S. 5. <http://www.mzv.sk/App/wcm/media.nsf/vw_ByID/ID_E64D391723AD1CCFC1257648004601A5_SK/$File/Strategia%20MZV%20definit%20260208.pd>, abgerufen am 20.09.2014.

8 Vgl. Ministerium für Äußeres. <http://www.mzv.sk/sk/zahranicna__politika/medzinarodne_zmluvy-zoznam_podla_medzinarodnych_organizacii>, abgerufen am 20.09.2014.

9 Diese Organisationen werden als einzige detailiert auf der Homepage des slowakischen Außenministeriums aufgelistet. Vgl. Ministerium für Äußeres. <http://www.mzv.sk/sk/zahranicna__politika/slovensko_v_osn-sr_v_osn>, abgerufen am 20.09.2014.

Streitkräfte und Auslandseinsätze

Die „Streitkräfte der Slowakischen Republik/Ozbrojené sily Slovenskej republiky" (OSSR) wurden in den Jahren nach der Wirtschaftskrise gemäß der Verkleinerung des Wehrbudgets stark reduziert. Die schwache Wirtschaftsleistung hatte eine unmittelbare Folgewirkung für das Wehretat und somit auch auf sicherheitspolitische Maßnahmen. Das Wehrbudget wurde im Jahr 2012 gegenüber dem Jahr 2008 um 19,3% gekürzt.[10] Die Personalstärke der OSSR betrug 2013 insgesamt 15.850 Personen und bedeutete gegenüber 2008 eine Verringerung um 1.279 Personen.

In der zweiten Jahreshälfte 2014 waren Angehörige der slowakischen Streitkräfte sowohl in UN-Friedensmissionen als auch unter dem Kommando der NATO und EU im Einsatz und beteiligten sich an den Missionen UNFICYP (Cypern), UNTSO (Israel und Syrien), ISAF (Afghanistan) und im NATO-Stab in Bosnien und Herzegowina. Im Rahmen von EU-Missionen sind slowakische SoldatInnen an EUFOR ALTHEA (Bosnien und Herzegowina) und der EUMM in Georgien beteiligt.[11]

2.1.3 Sicherheitspolitische Konzeptlandschaft

Im Allgemeinen sind die für die slowakische Sicherheit erarbeiteten Konzepte durch unterschiedliche institutionelle aber auch thematische Schwergewichtssetzungen gekennzeichnet. Klar zu differenzieren ist zwischen gesamtstaatlichen Konzepten und jenen Dokumenten, die eine institutionsspezifische Verantwortlichkeit vorsehen. Festzuhalten ist, dass sich alle Maßnahmen direkt oder indirekt von der Sicherheitsstrategie ableiten.

---

[10] Eine noch höre Kürzung des Wehrbudgets erfolgte im mitteleuropäischen Kontext in Ungarn. Das ungarische Verteidigungsministerium hatte im Jahr 2012 im Vergleich zu 2008 um 27,1% weniger Budget zur Verfügung. Vgl. Báchora, Rastislav: Regionale Kooperationen als umfassende Security Provider? In: Frank, Johann/Matyas, Wolgang (Hrsg.) Strategie und Sicherheit 2014. Wien, Köln, Weimar 2014,S. 327ff, hier S. 329.

[11] Vgl. Ministerium für Verteidigung der SR. <http://www.mod.gov.sk/zahranicne-operacie/>, abgerufen am 17.09.2014.

Systematik der „Schutz-Strategien"

Grundsätzlich erweist sich die grobe Unterscheidung der Strategien nach gesamtstaatlichen Ansätzen und „teiladministrativen" Zuständigkeiten als nützlich, wie Tabelle 1 zeigt.

Gesamtstaatliche Strategien		
Sicherheitsstrategie der SR (2005)[12]		
Nationale Strategie für Informationssicherheit in der SR (2008)[13]		
Nationale Antidrogenstrategie für die Jahre 2013-2020 (2013)[14]		
Gesamtstaatliche Strategie zum Schutz und Förderung der Menschenrechte (Entwurf 2011, 2014)[15]		
Äußeres	**Verteidigung**	**Inneres**
Strategie des Außenministeriums (2008)	Verteidigungsstrategie (2005)[16]	Nationaler Aktionsplan zur Bekämpfung des Terrorismus (2005, 2006, 2007, 2011)[17]
Mittelfristige Strategie des Außenministeriums bis 2015	Doktrin der Streitkräfte (2009)[18]	Nationales Programm zum Schutz und Verteidigung kritischer Infrastruktur (2007)[19]

[12] Vgl. Ministerium für Verteidigung der SR. <http://www.mosr.sk/data/files/833.pdf>, abgerufen am 14.09.2014.

[13] Vgl. Ministerium für Finanzen der SR. <http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s>, abgerufen am 14.04.2014.

[14] Vgl. Drogeninformationsportal. <http://www.infodrogy.sk/indexAction.cfm?module=Library&action=GetFile&DocumentID=1043>, abgerufen am 14.04.2014.

[15] Vgl. Regierungsrat für Menschenrechte, nationale Minderheiten und Genderbalance. <http://www.radavladylp.gov.sk/celostatna-strategia-ochrany-a-podpory-ludskych-prav-v-sr/>, abgerufen am 20.09.2014.

[16] Vgl. Ministerium für Verteidigung der SR. <http://www.mod.gov.sk/data/files/832.pdf>, abgerufen am 14.09.2014.

[17] Vgl. Ministerium für Inneres der SR. <http://www.minv.sk/?akcny_plan>, abgerufen am 30.09.2014.

[18] Vgl. Ministerium für Verteidigung der SR. <http://www.mod.gov.sk/data/files/831.pdf>, abgerufen am 14.09.2014.

[19] Vgl. Ministerium für Inneres der SR. <http://www.minv.sk/?ochrana-kritickej-infrastruktury>, abgerufen am 14.09.2014.

	Planungsmodell des Verteidigungsministeriums bis 2015 (2010)[20]	Strategie für Kriminalitätsprävention und anderer gegen die Gesellschaft gerichteter Handlungen für die Jahre 2012-2015 (2011)[21]
	Weißbuch der Verteidigung (2013)[22]	Konzept der Bekämpfung von Extremismus 2011-2014 (2011)[23]
		Nationaler Aktionsplan gegen den Menschenhandel 2011-2014 (2011)[24]

Tabelle 1: Systematisierung strategischer Dokumente
Rastislav Báchora

Diese Sicherheitskonzepte können generell als „Schutz-Strategien" bezeichnet werden, weil sie staatliche Schutzfunktionen gegenüber den BürgerInnen und dem Staat beinhalten. Darunter befinden sich auch jene Strategien, die konkrete Bedrohungen thematisieren und als „traditionelle" Sicherheitskonzepte im engeren Sicherheitsverständnis gelten. Dies sind vor allem die Sicherheits- und die Verteidigungsstrategie.

Gemäß der Aufgabenstellung des IFK-Projektes erfolgt hinsichtlich der hybriden Bedrohungen eine Untersuchung der Sicherheitskonzepte. Bei der vorliegenden Analyse wurden deshalb die Sicherheitsstrategie, Verteidigungsstrategie und die Strategie des Außenministeriums sowie die Konzepte für den Schutz der kritischen Infrastruktur berücksichtigt. Die Sicherheitsdokumente werden gemäß dem von Anton Dengg und Michael Schurian erstellten Analyseraster hinsichtlich drei vorgegebener Untersuchungsdimensionen analysiert. Diese sind:

---

20 Vgl. Ministerium für Verteidigung der SR. <http://www.mod.gov.sk/data/files/834.pdf>, abgerufen am 14.09.2014.

21 Vgl. Regierung der SR. <http://www.vlada.gov.sk/rada-vlady-sr-pre-prevenciu-kriminality>, abgerufen am 14.09.2014.

22 Vgl. Forum für internationale Politik. <http://www.mepoforum.sk/media/kniznica/kniznica/SR/Biela-kniha-o-obrane-SR-2013.pdf>, abgerufen am 14.09.2014.

23 Vgl. Ministerium für Inneres der SR. <http://www.minv.sk/?dokumenty-na-stiahnutie>, abgerufen am 14.09.2014.

24 Vgl. Ministerium für Inneres der SR. <http://www.minv.sk/?dokumenty-na-stiahnutie>, abgerufen am 14.09.2014.

(A) Bedrohungsbild;
(B) Operationen und Interaktionen;
(C) Internationales Konflikt- und Krisenmanagement.

Die Beurteilung, ob die erwähnten Konzepte eine „hybride Bedrohung" enthalten, obliegt unterschiedlichen Interpretationszugängen. Dabei stellt die Definition von Anton Dengg, Walter Feichtinger und Michael Schurian vom Institut für Friedenssicherung und Konfliktmanagement (IFK) – in der vorliegenden Analyse als „IFK-Definition" bezeichnet – den wichtigsten Beurteilungsrahmen dar.

2.1.4 Bedrohungsbild

In der SR wurde am 23. September 2005 die Verteidigungsstrategie und erst am 27. September 2005 die Sicherheitsstrategie im Parlament verabschiedet. Trotz dieser Unstimmigkeit gibt es in diesen Dokumenten ein einheitliches „Bedrohungsbild". Während in der Verteidigungsstrategie[25] Bedrohungen aufgezählt, aber nicht weiter inhaltlich präzisiert werden, setzt sich die Sicherheitsstrategie näher mit diesen auseinander.

Sicherheitsstrategie

Die aus 83 Absätzen bestehende Sicherheitsstrategie der SR erfasst insgesamt 16 Bedrohungen, die zum Teil von unterschiedlichen Offensivakteuren aber auch von nicht geplanten Ereignissen ausgehen. Im vorliegenden Text wird die Reihung und Beschreibung der Bedrohungen gemäß der Auflistung im Originaldokument durchgeführt. Ziel ist es, die einzelnen Bedrohungen nach ihrer inhaltlichen Korrelation mit den Bestimmungen der IFK-Definition für „hybride Bedrohungen" zu untersuchen. Die vorgenommene Nummerierung der Bedrohungen richtet sich nach der Sicherheitsstrategie.

---

[25] Vgl. Obranná stratégia Slovenskej republiky [Verteidigungsstrategie der SR], am 23. September 2005 vom Nationalrat verabschiedet, Kapitel I.5: Slovenská republika v meniacom sa bezpečnostnom prostredí [SR im sich ändernden Sicherheitsumfeld].

Erlangung und Einsetzung von Massenvernichtungswaffen (MVW)

Die Erlangung und der Einsatz von MVW werden in der Strategie deswegen als die „größten Bedrohungen" bezeichnet, weil diese den „größten Schaden" in der SR sowie ihren Verbündeten anrichten können. Als mögliche Offensivakteure werden explizit terroristische Gruppen sowie „failed states" genannt.[26]

Terrorismus

Der Terrorismus wird als eine „strategische globale Bedrohung" deklariert und nach einer ideologischen, ethnischen, religiösen Ausprägungsform unterschieden. Terrorismus beabsichtigt die „Untergrabung demokratischer Werte" wie: „Offenheit", „Freiheit des Individuums" sowie „Wert des einzelnen Lebens und Toleranz".[27]

Verbreitung von Massenvernichtungswaffen

Als eine „globale Bedrohung" für die SR gilt die Verbreitung von MVW. Die Zugänglichkeit dieser Waffen für „Staaten sowie für nichtstaatliche Akteure" stellt aufgrund des „wissenschaftlichen und technischen Fortschrittes, der Mobilität von Wissenschaftlern, des illegalen Handels mit radioaktivem Material sowie dual-use Material [...]" eine Bedrohung dar. Im Zusammenhang mit der Verbreitung der MVW wird auch die unkontrollierte „Verbreitung von konventionellen Waffen" als ein „ernstes Problem" bezeichnet.[28]

„Failed States"

„Failed states" stellen eine Bedrohung auf unterschiedlichen Ebenen dar, da sie „nicht fähig oder nicht willig" sind, die Grundfunktionen des Staates zu garantieren. Dazu gehören die „eigene Sicherheit sowie Einhaltung der Menschenrech-

---

26 Vgl. Sicherheitsstrategie der SR, Kapitel II, Abs. 17.
27 Vgl. ebd., Kapitel II, Abs. 18.
28 Vgl. ebd., Abs. 19.

te“ und daher werden sie zur „Bedrohung für ihr Umfeld und tragen zu regionalen Konflikten bei.“[29] Dieser Zustand fördert:

- Machtmissbrauch;
- Feindseligkeiten zwischen Bevölkerungsgruppen;
- Unterdrückung der Demokratie und Zivilgesellschaft;
- Einschränkung von Menschenrechten und Freiheiten;
- Korruption und Handel mit Menschen, Drogen und Waffen.[30]

Andauernde regionale Konflikte

Regionale Konflikte bedrohen die Sicherheit im euroatlantischen Raum und werden hauptsächlich von bewaffneten innerstaatlichen Auseinandersetzungen hervorgerufen. Diese Konflikte sind verbunden mit:

- Extremismus;
- Terrorismus;
- Bemühungen, Waffen zu erlangen;
- Armut;
- Massenmigration;
- Organisierter Kriminalität;
- Schwacher wirtschaftlicher Entwicklung in der Region.[31]

Organisierte Kriminalität

Organisierte Kriminalität (OK) gilt als „direkte Bedrohung“ für die SR. Unter Einsatz von modernen technischen Geräten und Kommunikationsmitteln versucht die OK in „alle Einrichtungen des öffentlichen Lebens“ einzudringen. Eine Reihe spezifischer krimineller Aktivitäten der OK werden aufgelistet:

- Illegale Erzeugung und Vertrieb von Drogen;

---

29 Vgl. ebd., Abs. 20.
30 Vgl. ebd.
31 Vgl. ebd., Abs. 21.

- Illegale Migration;
- Menschenhandel;
- Prostitution;
- Computerpiraterie;
- Diebstahl des geistigen Eigentums;
- Finanzkriminalität.[32]

Die „internationale OK“[33] wird als Quelle für die „Personalfinanzierung von Terrorismus“ bezeichnet, beteiligt sich an der „Verbreitung von MVW“, nützt „regionale Konflikte“ und gescheiterte Staaten aus. Neben negativer Beeinflussung der Weltwirtschaftssystems ergibt sich eine Reihe von Bedrohungsbildern für den Staat.

Verwundbarkeit von Informations- und Kommunikationssystemen

Aufgrund der Informationstechnologie und moderner Kommunikationsmittel ergeben sich neue Formen von Bedrohungen.

Unkontrollierte Migration

In der Sicherheitsstrategie wird generell die Bedrohung durch unkontrollierte Migration aus sozioökonomisch schwachen Regionen in die EU beschrieben. Dies führt zu „Populismus und Intoleranz“. Die Slowakei selbst wurde als ein Transitland für Migration deklariert, jedoch geht die Sicherheitsstrategie davon aus, dass mit dem wirtschaftlichen Aufschwung in Zukunft auch für die Slowakei die Bedrohungslage zunehmen wird. Mit illegaler Migration würden unterschiedliche Formen der OK in Verbindung stehen.[34]

---

32 Vgl. ebd., Abs. 22.

33 Der in der Strategie verwendete Begriff „internationale organisierte Kriminalität“ wird in der Fachliteratur meistens als „transnationale organisierte Kriminalität“ bezeichnet.

34 Vgl. ebd., Abs. 24.

Aktivitäten fremder Nachrichtendienste

Aktivitäten fremder Nachrichtendienste, die mittels „traditioneller und nicht traditioneller Methoden" sowie neuer Technologie ihrer Tätigkeit nachgehen, stellen eine „ständige Bedrohung" für die SR dar. Vor allem durch den Beitritt der SR zur NATO und EU wird mit einer erhöhten Bedrohungslage gerechnet.[35]

Globalisierung

Globalisierung ist sowohl für positive als auch für negative Folgewirkungen verantwortlich. Eine mangelnde Vorbereitung auf die Folgewirkungen der Globalisierung stellt eine „ernste Herausforderung für die Sicherheit" dar. Durch die Globalisierung würden die „Grenzen zwischen innerer und äußerer Sicherheit" sowie zwischen „Innen- und Außenpolitik" verwischt. Ausdrücklich werden „global operierende Wirtschaftssubjekte" genannt, die einen „wachsenden Einfluss auf weltweite Entwicklung" haben, diese werden jedoch nicht als Bedrohung deklariert. „Informationstechnologie" und „allgemeiner Zugang" zum Internet erleichtern die „Beschaffung von Waffensystemen", „Anleitungen zu deren Anwendung" und „Pläne zur Ausübung von Angriffen". Zudem erleichtern „globale Finanzmärkte" Kapitalverschiebungen durch Terroristen.[36]

Nichtstaatliche Akteure

Unmittelbar mit der Globalisierung hängt die Zunahme von nichtstaatlichen Akteuren im System der internationalen Beziehungen zusammen, was den Verlust der Monopolstellung des Staates bei der Garantierung von Sicherheit sowie beim Einsatz von Gewalt anbelangt.[37]

---

35 Vgl. ebd., Abs. 25.
36 Vgl. ebd., Abs. 26.
37 Vgl. ebd., Abs. 27.

Wirtschaftliches Ungleichgewicht

Die sich weltweit vertiefenden „sozialen und wirtschaftlichen Unterschiede zwischen den einzelnen Regionen" führen zu „Destabilisierung und fördern die Entstehung von Sicherheitsbedrohungen." Die soziale Kluft in den armen Gebieten bildet auch die Ursache für Unzufriedenheit und Radikalisierung und schafft gemäß der Strategie Voraussetzungen für:

- Extremismus;
- Terrorismus;
- Missbrauch des Glaubens und der Traditionen;
- Anstieg des religiösen Fanatismus;
- Entstehung von autoritären Regimen;
- Illegale Migration. [38]

Das wirtschaftliche Ungleichgewicht wird nicht nur als Quelle einer Reihe weitreichender Bedrohungen erachtet, sondern kann auch direkte Auswirkungen auf unterschiedliche gesellschaftspolitische Bereiche haben.[39]

Gefühl des Identitätsverlustes

Aufgrund der Globalisierungsprozesse und der Arbeitsmigration treten „Gefühle der Bedrohung des eigenen Lebensniveaus, Kultur und Identität" in der Bevölkerung auf. Damit verbunden ist der Anstieg des „radikalen Nationalismus und von Feindseligkeiten", die oft durch „politischen Populismus" unterstützt werden.[40]

---

38 Vgl. ebd., Abs. 28.
39 Vgl. ebd.
40 Vgl. ebd., Abs. 29.

Wachsender Energie- und Rohstoffbedarf

Durch wachsenden Verbrauch von Rohstoffen, weiterer lebensnotwendiger Ressourcen und auch Lebensmitteln wird es laut Strategie „wahrscheinlich" zu „Rohstoff- und Energiekrisen" und somit auch zu Konflikten kommen. [41]

Naturkatastrophen

Natürliche Umweltkatastrophen, Pannen und andere Katastrophen stellen aufgrund der nicht vorhandenen Vorhersehbarkeit eine „permanente Bedrohung für Leben und Besitz im großen Ausmaß dar". Damit hängt unter anderem die Luftverschmutzung, Mangel an Trinkwasser und die Zerstörung von Ökosystemen zusammen.[42]

Unausgeglichene demographische Entwicklung

Eine unausgeglichene demographische Entwicklung hat negative Folgewirkungen auf das „Sozialsystem", was zur „Bedrohung der sozialen Stabilität im Staat" führen kann. Die Migration wird in diesem Zusammenhang auch als Faktor der demographischen Entwicklung betrachtet.[43]

Die in der Sicherheitsstrategie dargestellten Bedrohungen veranschaulichen ein breites Spektrum an unterschiedlichen Herausforderungen, wobei zwischen den einzelnen Bedrohungsbildern nach spezifischen Kriterien unterschieden werden muss.

Analyse

Fasst man die einzelnen Bedrohungen in der slowakischen Sicherheitsstrategie zusammen, dann lassen sich diese grob in drei Kategorien einteilen:

---

41 Vgl. ebd., Abs. 30.
42 Vgl. ebd., Abs. 31.
43 Vgl. ebd., Abs. 32.

a) Bedrohungen, die von einer willentlichen, zielgerichteten Handlung eines konkreten Akteurs ausgehen;
b) Bedrohungen, ausgelöst von äußeren Prozessen, die vordergründig keiner direkten Bedrohungsabsicht zugrunde liegen;
c) Innerstaatliche Zustände oder Entwicklungen.[44]

a) Willentliche Absicht	b) Prozesse außen	c) Prozesse innen
Erlangung und Einsatz von MVW (1)	failed states (4)	Verwundbarkeit von Informations- und Kommunikationssystemen (7)
Terrorismus (2)	Andauernde regionale Konflikte (5)	Gefühl des Identitätsverlustes (13)
Verbreitung von MVW (3)	Unkontrollierte Migration (8)	Unausgeglichene demographische Entwicklung (16)
Organisierte Kriminalität (6)	Globalisierung (10)	
	Wirtschaftliches Ungleichgewicht (12)	
Aktivitäten fremder Nachrichtendienste (9)	Wachsender Energie- und Rohstoffbedarf (4)	
Nichtstaatliche Akteure (11)	Naturkatastrophen (15)	

Tabelle 2: Einteilung der Bedrohungen in der Sicherheitsstrategie der SR
Rastislav Báchora

Es liegt im Wesen und der Charakteristik der Bedrohungen, dass keine eindeutige Abgrenzung gemäß der aufgestellten Kategorisierung (Tabelle 2) möglich ist, jedoch lassen sich einzelne Akteure identifizieren, die laut der Sicherheitsstrategie entsprechende Bedrohungshandlungen setzen könnten. Diese Akteure stellen auch die „Verbindung" zu den hybriden Bedrohungen dar.

Gemäß der IFK-Definition liegt eine hybride Bedrohung dann vor, wenn diese von der Absicht eines Akteures ausgeht. Zudem muss der Akteur in der Lage sein, sein Gefährdungspotential in mehreren sicherheitsrelevanten Dimensionen einzusetzen. In der IFK-Begriffsklärung können seitens des Offensivakteurs „politische", „wirtschaftliche", „militärische", „gesellschaftliche" und „mediale"

[44] Die Einteilung der Bedrohungen in der slowakischen Sicherheitsstrategie nach willentlicher Absicht, äußeren und innerstaatlichen Prozessen basieren auf den Überlegungen des Autors.

Handlungsmaßnahmen zur Beeinträchtigung der Sicherheit gesetzt werden. Das Benennen von Akteuren, von welchen zielgerichtete Sicherheitsbedrohungen ausgehen, stellt demnach die Grundlage für das Erkennen von hybriden Bedrohungen dar. In der slowakischen Sicherheitsstrategie werden Akteure genannt, von denen unterschiedlichste Bedrohungen ausgehen oder laut IFK-Definition das „Vermögen" hätten, ihr „Potential" „mehrdimensional" gegen die Sicherheit der SR zu richten. Diese in der Sicherheitsstrategie genannten Akteure können als Offensivakteure bezeichnet werden und sind:

- Terroristische Gruppen (Bedrohung 1, 2, 4);
- Staaten und nichtstaatliche Akteure (Bedrohung 3);
- Terroristische und extremistische Gruppen und Netzwerke (Bedrohung 4);
- OK-Gruppen (Bedrohung 6);
- Fremde Nachrichtendienste (Bedrohung 9);
- Global operierende Wirtschaftssubjekte (Bedrohung 10);
- Nichtstaatliche Gruppen, Organisationen und Netzwerke (Bedrohung 11);
- Populismus und Nationalismus von politischen Gruppen (Bedrohung 13).

Grundsätzlich lassen sich aus der Darstellung der Bedrohungs- und Akteurslage zwei Schlussfolgerungen ziehen: Erstens könnten theoretisch alle in der Sicherheitsstrategie erwähnten Akteure das Potential aufbringen, Aktivitäten entsprechend den IFK-Bestimmungen von hybriden Bedrohungen zu setzen. In der Sicherheitsstrategie selbst werden diese aber nicht in der entsprechenden Weite und Tiefe erfasst. Zweitens lassen sich jene Bedrohungen, welchen eine zielgerichtete Willensabsicht zugrunde liegt, als „hybride Bedrohungen" interpretieren. Somit können vier Bedrohungen als „hybrid" bezeichnet werden:

- Erlangung und Einsatz von MVW;
- Terrorismus, Verbreitung von MVW;
- Organisierte Kriminalität;
- Aktivitäten fremder Nachrichtendienste.

Zwar gelten in der Sicherheitsstrategie nichtstaatliche Akteure als eigene Bedrohung, diese stellen aber im Rahmen der anderen Bedrohungsformen einen fixen

Bestandteil dar und werden daher auch nicht extra angeführt. Mittels strengerer Textauslegung der IFK-Definition und ihrer operationellen Anwendung auf die slowakische Sicherheitsstrategie wäre zu konstatieren, dass am ehesten die Bedrohungen durch den Terrorismus und die OK den inhaltlichen Bestimmungen der vorgegebenen „Hybridität" entsprechen. Inwieweit die in der Strategie enthaltenen Bedrohungen als „hybrid" bezeichnet werden können, hängt aber auch vom Sicherheitsverständnis sowie den methodischen und analytischen Zugänge des/der BetrachtersIn selbst ab. Womit objektivierbare Kriterien mittels weiterer wissenschaftlicher Vorgehensweise aufzustellen wären.

Strategie des Außenministeriums

Grundsätzlich hat das Außenministerium in Bratislava bei strategischen Fragestellungen im Bereich der Sicherheitspolitik starke Einflussmöglichkeiten. Daher ist auch die Strategie des Außenministeriums aus dem Jahr 2008 mit dem Titel „Erfolgreiche Slowakei in einer sicheren Welt" hinsichtlich der darin enthaltenen sicherheitspolitischen Herausforderungen zu berücksichtigen.

Insgesamt werden in der Strategie vier „strategische Prioritäten" definiert. Diese sind die Bereiche Sicherheit, Wirtschaft und Regionales, EU-Agenden sowie Bürgerservice. Zwar werden in der außenpolitischen Strategie keine konkreten Bedrohungen (wie in der Sicherheitsstrategie) eingehender beschrieben, jedoch sehr wohl im Kontext der sicherheitspolitischen Prioritätensetzung aufgezählt. Konkret werden die EU und NATO für die Gestaltung der eigenen internationalen Beziehungen als die wesentlichen Rahmen präsentiert. Unter dem Punkt „Stärkung der Sicherheit im euroatlantischen Raum" wird „das Entgegenwirken von Krisen und Konflikten, sowie sich den Herausforderungen und potentiellen Bedrohungen im euroatlantischen Raum zu stellen", als eine Priorität präsentiert.[45] Unter dem Punkt „Kämpfen gegen globale Herausforderungen und Bedrohungen" werden Bekämpfung des Terrorismus, den MVW und der OK als Prioritäten vorgestellt.[46] Zwar werden in der Strategie des Außenministeriums

---

[45] Vgl. Ministeriums für Äußeres: Strategie des Ministeriums für Äußeres, Kapitel 5: Strategické ciele [Strategische Ziele].

[46] Stratégia MZV SR - Úspesné Slovensko v bezpecnom svete [Strategie des Außenministeriums der SR – Eine erfolgreiche Slowakei in einer sicheren Welt], Kapitel 5.1.3: Bo-

keine Bedrohungen konkretisiert, jedoch wird das Bedrohungsbild der Sicherheitsstrategie bestätigt.

Schutz kritischer Infrastruktur

Dem Schutz der kritischen Infrastruktur wird in der slowakischen Sicherheitsstrategie keine besondere Priorität beigemessen. Insgesamt wird die kritische Infrastruktur dreimal kurz erwähnt und zwar zweimal im Zusammenhang mit der Terrorismusbekämpfung und einmal konkret bei den Maßnahmen zur Erhöhung der Informationssicherheit.[47] In der Sicherheitsstrategie werden aber konzeptuelle, administrative und legislative Folgeprozesse angekündigt. So wurde im Jahr 2006 das „Konzept der kritischen Infrastruktur in der SR und die Maßnahmen zu ihrem Schutz und ihrer Verteidigung" erstellt. Bereits im Jahr 2007 wurde das „Nationale Programm zum Schutz und zur Verteidigung der kritischen Infrastruktur" von der Regierung angenommen und stellt somit ein zentrales Konzept dar.[48] Zusätzlich wurden auch in der Informationsstrategie aus dem Jahr 2010 relevante inhaltliche Aspekte aufgenommen. Schließlich sind wichtige Rahmenbedingungen im „Gesetz über den Schutz der kritischen Infrastruktur", das im Wesentlichen auf dem Arbeitsprogramm von 2007 beruht, gesetzlich verankert worden. Laut diesem „Nationalprogramm" ist kritische Infrastruktur:

> „[...] jener Teil der nationalen Infrastruktur (ausgewählte Organisationen und Institutionen, Objekte, Anlagen, Einrichtungen, Dienste und Systeme), dessen Zerstörung oder Funktionsbeeinträchtigung als Folgewirkung eines Risikofaktors eine Bedrohung oder Schädigung des politischen oder wirtschaftlichen Ganges des Staates oder Bedrohung an Leben und Gesundheit der Bevölkerung verursacht."[49]

---

jovat' proti globálnym výzvam a hrozbám [Kämpfen gegen globale Herausforderungen und Bedrohungen].

47 Vgl. Sicherheitsstrategie der SR, Kapitel II.18, Kapitel III.44 und Kapitel III 49.

48 Vgl. Ministerium für Inneres der SR. <http://www.minv.sk/?ochrana-kritickej-infrastruktury>, abgerufen am 30.09.2014.

49 Ministerium für Inneres: Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [Nationales Programm zu Schutz und zur Verteidigung kritischer Infrastruktur der SR], Einleitung 2007. <http://www.minv.sk/?ochrana-kritickej-infrastruktury>, abgerufen am 30.09.2014.

Der Schutz der kritischen Infrastruktur obliegt dem Verantwortungsbereich mehrerer „Subjekte“:

- Internationale Partner und internationale Organisationen;
- Regierung und öffentliche Verwaltung;
- Gebietskörperschaften und Einrichtungen der Selbstverwaltung;
- Staatliche Wirtschaftssubjekte;
- Private Wirtschaftssubjekte.[50]

Im Programm wurden Einrichtungen der kritischen Infrastruktur auf neun verschiedene Sektoren aufgeteilt:

- Wasser;
- Nahrungsmittel;
- Gesundheit;
- Energiewirtschaft;
- Informations- und Kommunikationstechnologie;
- Verkehr;
- Öffentliche Ordnung und innere Sicherheit;
- Industrie;
- Finanzsektor.[51]

Die zentralen Koordinationsaufgaben zum Schutz der kritischen Infrastruktur obliegen dem Ministerium für Inneres, jedoch werden im „Nationalprogramm“ insgesamt neun Ministerien genannt, die konzeptuell und institutionell in die Erfüllung der Schutzmaßnahmen eingebunden sind. Darunter befinden sich auch die für die primären sicherheitspolitischen Angelegenheiten zuständigen Ministerien für Äußeres und Verteidigung. Extra angeführt wird auch der Inlandsnachrichtendienst.[52] Als Bedrohungen werden explizit der Terrorismus, aber auch Katastrophen hervorgehoben, gegen die man die kritischen Einrich-

---

50 Vgl. ebd., Kapitel 2.1: Aktuálny stav ochrany kritickej infraštruktúry v Slovenskej republike [Aktuelle Lage des Schutzes der kritischen Infrastruktur in der SR].

51 Vgl. ebd., Kapitel 3.1 – 3.9.

52 Vgl. ebd., Kapitel 4: Úlohy zainteresovaných subjektov [Aufgben der interessierten Subjekte].

tungen schützen muss.[53] Der Terrorismus kann auch hinsichtlich der Konzepte zum Schutz der kritischen Infrastruktur als eine hybride Bedrohung bezeichnet werden.

2.1.5 Operationen und Interaktionen

Für die Bekämpfung nahezu aller Bedrohungsformen sind sowohl nationale als auch internationale Mechanismen notwendig und erfordern einen der Bedrohungsart angepassten spezifischen Kooperationsgrad unterschiedlicher Institutionen der öffentlichen Verwaltung. Die institutionelle Zusammenarbeit bei der Bekämpfung von Bedrohungen schließt sowohl nichtstaatliche als auch zivilgesellschaftliche, aber auch kommerzielle Gruppen ein. In welchem Ausmaß diese Interaktionen in der Sicherheitsstrategie der SR konzipiert werden, wird unter drei wesentlichen Vorzeichen untersucht:

a) Kooperationsbereitschaft zwischen Regierungsstellen;
b) Sicherheitscluster-Ansätze;
c) Gemeinsame Lagebeurteilung und gemeinsames Lagebild.

Kooperationsbereitschaft zwischen Regierungsstellen

Die Aufrechterhaltung oder Herstellung der Sicherheit ist die Aufgabe der Sicherheitspolitik und diese beruht laut slowakischer Sicherheitsstrategie auf dem „Sicherheitssystem". Das „Sicherheitssystem" ist ein „vielseitiger Komplex" und beinhaltet die Instrumente der Außenpolitik, Wirtschaft, Verteidigung, Innenpolitik, des Sozialsystems, des Rettungswesens sowie Umweltschutzeinrichtungen.[54] Die staatlichen Instrumente für die Bedrohungsbekämpfung werden als „traditionelle Mittel" bezeichnet und diese sind:

- Auslandsnachrichtendienst;
- Streitkräfte;

---

53 Vgl. ebd., Kapitel 2.1.

54 Vgl. Sicherheitsstrategie der SR, Kapitel III.37: Bezepečnostná politika Slovenskej republiky [Sicherheitspolitik der SR].

- Nachrichtendienst (Inland);
- Polizei;
- Justizwache;
- Zollverwaltung;
- Feuerwehr;
- Rettungseinrichtungen;
- Bergwerksrettung;
- Hochgebirgsrettung;
- Subjekte der Wirtschaft;
- Subjekte des Finanzmarktes;
- Institute, verantwortlich für Datenschutz.[55]

Zum koordinierten Einsatz von staatlichen Instrumentarien bei der Bedrohungsbekämpfung kommt die Zusammenarbeit mit anderen staatlichen und nichtstaatlichen Akteuren auf nationaler sowie auf internationaler Ebene hinzu. Konkret heißt es in der Sicherheitsstrategie, dass die Sicherheitspolitik im Rahmen vorgegebener Strukturen und Mittel erfolgt. Dieser Rahmen stellt sich wie folgt dar:

- UNO;
- EU;
- NATO;
- OSZE;
- Europarat;
- Visegrad-Gruppe;
- Mitteleuropäische Initiative;
- NGOs;
- Internationale Abmachungen und Verträge;
- Normen und Standards;
- Medien.[56]

---

55 Vgl. ebd., Kapitel III.39.
56 Vgl. ebd., Kapitel III.40.

Insbesondere die Bekämpfung der hybriden Bedrohungen, also jener Bedrohungen, die auf einer Willensabsicht beruhen, macht eine konzeptuell festgelegte Kooperation zwischen unterschiedlichen Regierungsstellen notwendig. In Tabelle 3 wird genauer auf die Bekämpfungsmaßnahmen gegen diese willentlich erzeugten und zielgerichteten Bedrohungen in der Sicherheitsstrategie eingegangen.

Hybride Bedrohung (mit Willensabsicht)	**Kooperation bei Abwehr**
• Erlangung, Verbreitung und Einsatz von MVW	• Internationale Normen • Sanktionen • Rüstungsexportkontrolle • Kooperation mit NATO und EU (Abs. 45)
• Terrorismus	• Nachrichtendienste • Spezialabteilungen der Strafverfolgungsbehörden • Koordinierung mit Partnerdiensten im Ausland • Entwaffnung von Terroristen unter Einsatz des Militärs (Abs. 44)
• Organisierte Kriminalität	• Rechtliche, wirtschaftliche, mediale Rahmenbedingungen stärken • Präventive und repressive Maßnahmen: Nachrichtendienste, Polizei, Staatsanwaltschaft, Gerichte (Abs. 48)
• Aktivitäten fremder Nachrichtendienste	• Erhöhter Informationsschutz durch Nachrichtendienste und verstärkte Kooperation mit Partnerdiensten aus NATO- und EU-Staaten (Abs. 51)

Tabelle 3: Kooperationen bei der Bekämpfung hybrider Bedrohungen
Rastislav Báchora

Einen wichtigen Stellenwert bei der Bedrohungsbekämpfung nehmen internationale Organisationen ein. Betrachtet man die (potentiell) hybriden Bedrohungen gesondert, dann stellen EU und NATO einen essentiellen Aktionsradius für die slowakische Sicherheitspolitik dar.

Sicherheitscluster-Ansätze

Aus der Interpretation und Beurteilung der in der Sicherheitsstrategie beinhalteten konzeptuellen Ansätze geht hervor, dass diese einerseits eine weitreichende Bandbreite an Kooperationen zwischen Institutionen vorsehen, andererseits werden im eigentlichen Sinne keine Zusammenführungen von staatlich-administrativen Instrumentarien bei der Bekämpfung konkreter Bedrohung zu Clustern vorgenommen.

Die Maßnahmen der Strategie geben zum Ausdruck, dass sich das Sicherheitssystem aus allen Teilelementen der öffentlichen Verwaltung zusammensetzt und von der Regierung koordiniert wird. Für die Koordinierung der Sicherheitsaufgaben auf der höchsten Entscheidungsebene ist der Sicherheitstrat der Regierung zuständig, dessen Funktion und Aufgabenstellung wird in der Sicherheitsstrategie allerdings überhaupt nicht erwähnt. Somit wird ein wesentliches Koordinationsorgan, das institutionelle Cluster-Ansätze bei der Gestaltung des slowakischen Sicherheitssystems operativ und konzeptuell vereint, in der Sicherheitsstrategie nicht beachtet. Ungewöhnlich ist dies vor allem deshalb, weil gemäß dem Gesetz über die „Leitung des Staates in Krisensituationen außerhalb des Krieges und Kriegszustandes" dem Sicherheitsrat eine wesentliche Aufgabe in Friedenszeiten zukommt.[57] Aber auch im Ausnahme- und Kriegszustand erfüllt der Sicherheitsrat zentrale Führungsaufgaben.[58]

Gemeinsame Lagebeurteilung und Lagebild

Eine gemeinsame Lagebeurteilung sowie ein gemeinsames Lagebild im Sinne einer gesamtstaatlichen institutionenübergreifenden systematischen Darstellung der Bedrohungen und Abschätzung von deren Auswirkungen auf die Sicherheit der SR existieren im Konzept der Sicherheitsstrategie nicht. Zur Lagebeurteilung

---

57 Vgl. Regierung der SR, Gesetz 387/2002: O riadení štátu v krízových situáciách mimo času vojny a vojnového stavu [Leitung des Staates in Krisensituationen außerhalb des Krieges und Kriegszustandes], §3. http://www.vlada.gov.sk/data/files/4373_387.pdf, abgerufen am 30.09.2014.

58 Vgl. Regierung der SR: Štatút Bezpečnostnej rady Slovenskej republiky [Statut des Sicherheitsrates der SR], Nr.2. <http://www.vlada.gov.sk/bezpecnostna-rada-sr/>, abgerufen am 30.09.2014.

des Außenumfeldes, aber auch zum Lagebild im Inneren tragen unter anderem die Nachrichtendienste bei, auf die in mehreren Textstellen hingewiesen wurde. Insbesondere die Beurteilung der Entwicklungen im Ausland und möglicher Auswirkungen auf die eigene Sicherheit erfolgt vordergründig im Rahmen der NATO und EU. Im Dokument selbst wird vor allem auf die Beeinflussung des Außenfeldes, aber nicht auf die Beurteilung der Lage hingewiesen.[59] Gemäß der Sicherheitsstrategie hat die Mitgliedschaft in der NATO und EU einen wesentlichen Einfluss auf die Beurteilung der sicherheitspolitischen Entwicklungen und prägt auch das IKKM.

2.1.6 Internationales Konflikt- und Krisenmanagement

Der Fokus bei der Darstellung des IKKM wird auf die Auslandseinsätze gerichtet und dabei sowohl die Sicherheitsstrategie als auch die Verteidigungsstrategie berücksichtigt.

IKKM in der Sicherheitsstrategie

Beim IKKM steht die Beteiligung der slowakischen Streitkräfte an Auslandseinsätzen im Mittelpunkt und wird als ein Beitrag zur Wahrung der eigenen Sicherheit und als eine Bündnisverpflichtung gegenüber der NATO und EU interpretiert. Zudem spielen konzeptuell die Einsätze im Rahmen der UNO ebenfalls eine wichtige Rolle. Generell betrifft das militärische IKKM-Engagement sowohl das Entsenden von Truppen in akute Krisenregionen als auch in Post-Konfliktgebiete. Bei der Maßnahmensetzung gegen die Bedrohungen, ausgehend von schwachen Staaten, ist in der Sicherheitsstrategie die Zusammenarbeit zwischen militärischen und zivilen Kräften im Rahmen der Entwicklungshilfe vorgesehen.[60] Dass das IKKM im Rahmen der NATO und EU zu erfolgen hat, wird an mehreren Stellen

---

59 Vgl. Sicherheitsstrategie der SR, Kapitel III.60.
60 Vgl. Sicherheitsstrategie der SR, Kapitel III, Abs. 47.

betont. Somit besteht unter anderem das Ziel darin, dass „operative Kapazitäten" der EU gestärkt werden.[61]

Hinsichtlich konkreter Bedrohungen im Auslandseinsatz mit Wechselwirkungen auf die Heimat werden im Dokument weder konzeptuelle noch operative Zusammenhänge mit Relevanz für administrativ-institutionelle Folgeprozesse hergestellt. Somit ist das IKKM in der Sicherheitsstrategie der SR eher durch allgemeine außen- und sicherheitspolitische Positionierung charakterisiert. Dabei wird die Bedeutung der Streitkräfte für das IKKM betont und in der Verteidigungsstrategie weiterführend behandelt.

IKKM in der Verteidigungsstrategie

So wie in der Sicherheitsstrategie wird auch in der Verteidigungsstrategie eine stärkere Beteiligung an Auslandsmissionen im Rahmen der NATO und EU an mehreren Stellen hervorgehoben. Genauere Angaben über das militärische IKKM sind im Kapitel „Anforderungen an die Verteidigung der SR" zu finden. Darin wird der Schutz der BürgerInnen und des Staates hervorgehoben, der den Einsatz militärischer Mittel gegen den internationalen Terrorismus auch im Ausland konzeptuell vorsieht.[62] Zudem können laut der Verteidigungsstrategie Streitkräfte gegen die Verbreitung von MVW sowie bei der Regelung von Konflikten in Krisenregionen eingesetzt werden.[63]

Im Bereich des IKKM wird der Einsatz der Streitkräfte gegen Terrorismus als „am wahrscheinlichsten" angesehen, was die besondere Hybridität dieser Bedrohung sowie die diesbezügliche Wahrnehmung in der Slowakei ausdrückt.[64] Bei Auslandseinsätzen wird ausdrücklich die Übernahme von NATO-Standards eingefordert, wobei die Ausbildung und die Vorbereitung auf die Auslandsein-

---

61 Vgl. ebd., Kapitel III, Abs. 69.

62 Vgl. Obranná stratégia Slovenskej republiky [Verteidigungsstrategie der SR], am 23. September 2005 vom Nationalrat verabschiedet, Kapitel III: Požiadavky na obranu Slovenskej republiky [Anforderungen an die Verteidigung der SR], Abs. 18.

63 Vgl. ebd., Abs. 20.

64 Obranná stratégia Slovenskej republiky [Verteidigungsstrategie der SR], am 23. September 2005 vom Nationalrat verabschiedet, Kapitel III, Abs. 26.

sätze in enger Kooperation mit den Partnern zu erfolgen hat.[65] In diesem Zusammenhang wird ersichtlich, dass die konzeptuelle und operative Planung des IKKM den Prioritäten der NATO und an zweiter Stelle der EU angepasst wurde.

Etwaige konzeptuelle und/oder operative Ansätze besonderer Vorkehrungsmaßnahmen hinsichtlich von Wechselwirkungen zwischen Einsatzort und Heimat wurden in die Verteidigungsstrategie – so wie in die Sicherheitsstrategie – nicht einbezogen. Somit bleibt die Bedrohung durch den Terrorismus und Verbreitung von MVW die wesentliche Bedrohungsart, gegen die im Rahmen des IKKM militärisch vorgegangen werden sollte. Aufgrund der konzeptuellen Einsatzplanungen im IKKM-Bereich, die sowohl den Terrorismus als auch die Verbreitung von MVW hervorheben, kann daher von hybriden Bedrohungen gesprochen werden.

2.1.7 Schlussfolgerungen

Die wesentliche Schlussfolgerung der Untersuchung lautet, dass das Erfassen und vor allem die konzeptuelle und in weiterer Folge auch administrativ-institutionelle operative Handhabung von Sicherheitsherausforderungen im Allgemeinen und den hybriden Bedrohungen im Besonderen vom Sicherheitsverständnis abhängig sind. Im Fallbeispiel der Slowakei steht die Sicherheit des Bürgers/der Bürgerin sowie des Staates gleichermaßen in den konzeptuellen Bedrohungsdarstellungen der Sicherheitsstrategie im Vordergrund. Dadurch werden gesellschaftspolitische Themenbereiche wie „wirtschaftliches Ungleichgewicht", „Angst vor dem Verlust der Identität" oder „demographisches Ungleichgewicht" sicherheitspolitisch konjugiert und als Bedrohungen für die Sicherheit konzipiert. Was konkret hybride Bedrohungen gemäß der IFK-Arbeitsdefinition nach Anton Dengg, Walter Feichtinger und Michael Schurian in den Sicherheitskonzepten der SR anbelangt, so lässt sich schlussfolgern, dass die Dokumente generell an ein modernes Bedrohungsverständnis angepasst werden müssten. Zwar werden Bedrohungen, die von einer zielgerichteten Schadensabsicht eines oder mehrerer Akteure ausgehen, beschrieben, jedoch werden diese nicht systematisch als solche konzipiert und weiterführend bearbei-

---

[65] Vgl. ebd., Kapitel IV: Rozvoj ozbrojených síl [Entwicklung der Streitkräfte], Abs. 41.

tet. Es wird weder ein konzeptueller noch operativer Unterschied zwischen beabsichtigten hybriden Bedrohungen wie Terrorismus, Verbreitung von MVW oder der OK einerseits und den eher „prozessresultierenden" unbestimmten Bedrohungen wie Globalisierung, schwache Staaten, Migration etc. andererseits gemacht. Zwar werden durchaus Akteure aufgelistet, von denen das Potential hybrider Bedrohungen ausgeh, jedoch werden diese konsequenterweise nicht explizit also solche kategorisiert. Eine präzise Charakterisierung von Bedrohungen würde zwangsläufig auch die administrativ-institutionellen Bekämpfungsmaßnahmen konkretisieren und zu einem höheren Maß an Klarheit bei den Verwaltungszuständigkeiten führen.

Eine wesentliche Schwachstelle weist die Sicherheitsstrategie eindeutig in den Bereichen der Darstellung konzeptueller und operativer Kooperationen von Institutionen bei der Bedrohungsbekämpfung sowie beim IKKM auf. So lässt z.B. die Verteidigungsstrategie – ebenso wie die Sicherheitsstrategie – Wechselwirkungen von Bedrohungen im Einsatzraum und der Heimat komplett unberücksichtigt, obwohl die Bekämpfung von Terrorismus und die Verbreitung von MVW mit militärischen Mitteln im Rahmen von Auslandsmissionen konzeptuell vorgesehen sind. Grundsätzlich positiv zu werten ist, dass auf der Grundlage der Sicherheitsstrategie spezifische Teilstrategien für unterschiedliche Verwaltungsbereiche erstellt wurden, allerdings orientieren sich diese dann konsequenterweise nicht an dem Bedrohungsbild.

Zusammenfassend lassen sich drei wesentliche Ableitungen ziehen:

(1) Eine umfassende Konzipierung hybrider Bedrohungen ist vordergründig das Resultat einer zeitgemäßen Perzeption sicherheitspolitischer Herausforderungen.
(2) Die Analyse von Bedrohungen in Sicherheitskonzepten und die Beurteilung dieser, ob eine Hybridität im Sinne der IFK-Bestimmungen gegeben ist, unterliegt einer gewissen Schwankungsbreite. Variable Interpretationen sind primär das Resultat eines unzureichenden Forschungsstandes.
(3) Allgemeine und generalisierbare Aussagen über hybride Bedrohungen und deren Verankerung in sicherheitspolitischen Konzepten erfordern einen weiterführenden Diskussionsprozess unter Einschluss politischer, wissenschaftlicher und zivilgesellschaftlicher Fachkreise.

2.2 Schweden

Michael Fredholm

Anmerkung: Die geäußerten Meinungen sind ausschließlich vom Autor und entsprechen nicht notwendigerweise der Meinung der schwedischen Regierung

Bevölkerung:	9.684.858 (31.05.2014)[1]
Fläche:	528.447 km² [2]
BIP pro Einwohner:	SEK 379.300 (2013)[3]
Prognose Wirtschaftswachstum:	N/V.
Mitgliedschaft in Internationalen Organisationen (mil. Organisation):	EU (seit 1995)
Größe der Streitkräfte:	19.995, zusätzlich zu 20.596 Heimwehr (31.12.2013)[4]

Tabelle 4: Eckdaten von Schweden
Michael Fredholm

2.2.1 Bedrohungsbild

Konzeptlandschaft

Schweden veröffentlicht keine sicherheitsrelevanten Konzepte. Es fehlen sowohl ein nationales Sicherheitskonzept sowie ein außenpolitisches Konzept. Es

---

1 Statistics Sweden, <www.scb.se>.
2 Ebd.
3 Ebd.
4 Webseite der Streitkräfte, <www.forsvarsmakten.se>.

gibt auch keine autorisierte Sicherheitsstrategie oder Verteidigungsstrategie. Es gibt nicht einmal Weiß- oder Grünbücher, die mit der nationalen Sicherheit befasst sind. Bedrohungen werden in der Regel nicht mit veröffentlichten Konzepten, sondern pragmatisch begegnet, abhängig von der jeweiligen Situation. Was am ehesten einem Sicherheitskonzept ähnelt, ist die Militärstrategische Doktrin (MSD 12), Ausgabe 2012, die als einziges Dokument die hybride Kriegführung und hybride Bedrohung als ein Konzept erwähnt. Die Schwerpunkte der Militärstrategischen Doktrin sind jedoch primär relevant für internationale Einsätze und IKKM. In der Realität ist die Militärstrategische Doktrin möglicherweise nicht auf Territorialverteidigung ausgerichtet.

Das Konzept der hybriden Machtprojektion oder der hybriden Bedrohung wird in Schweden nicht sehr stark thematisiert. Ein Grund dafür ist die militärische Planungsarbeit. Da hybride Kriegführung von der konventionellen Kriegführung über Terrorismus bis hin zu organisierter Kriminalität und Cyberbedrohungen praktisch alles erfasst, ist es für die Streitkräfte schwierig, ihre zukünftige Stärke und Größe für solche Bedrohungen zu planen. Darüber hinaus fehlt den schwedischen Streitkräften die Fähigkeit, auf die vielen Formen hybrider Bedrohungen angemessen zu reagieren. Viele Binnenbedrohungen müssen durch andere schwedische Behörden, wie die Polizei behandelt werden, während sie in einem internationalen Kontext gemeinsam mit anderen Staaten oder Organisationen bewältigt werden müssen.

Die Militärstrategische Doktrin (MSD 12) erwähnt hybride Kriegführung und hybride Bedrohung als ein Konzept moderner Kriegführung nur flüchtig und ohne Details:[5]

Aufgrund der Schwierigkeit, klar zwischen irregulärer und regulärer Kriegführung zu unterscheiden und der Erkenntnis, dass die gleichzeitige Anwendung beider Formen der Gewaltausübung in der Zukunft eine immer größere Herausforderung wird, wird der Begriff der „Hybriden Kriegführung" oder auch ausgedrückt als „Hybride Bedrohung", immer häufiger verwendet. Im Grunde handelt es sich um ein Konzept, in dem Akteure, ungeachtet ihres Status, Zugang zu regulären militärischen Fähigkeiten sowie zur gesamten Bandbreite der Gewaltausübung haben, die in der Regel mit irregulärer Kriegführung verbun-

---

[5] Der Hauptvertreter des Konzepts innerhalb der Streitkräfte ist Dr. Håkan Gunneriusson. an der Verteidigungsakademie in Stockholm.

den ist (Ein Beispiel für hybride Kriegführung ist der Krieg der Hisbollah gegen Israel im Jahr 2006).[6]

Unter hybrider Kriegführung wird jene Kriegführung verstanden, die verschiedene Strategien, Taktiken und Kampftechniken im gleichen Konflikt (Gebiet) verbindet. Sie trägt Auswirkungen der Globalisierung Rechnung: Kommunikation ist bedeutender geworden und qualifizierte Waffensysteme sind einfacher verfügbar. Hybride Kriegführung kann als eine Weiterentwicklung des Konzepts der „irregulären Kriegführung" mit verstärktem Einsatz moderner Technologien betrachtet werden. Es erfordert die Fähigkeit der regulären und irregulären, aber auch unkonventionellen Kriegführung.[7]

Spezialoperationen halten Schritt mit der gestiegenen Relevanz der Aufstandsbekämpfung (*Counterinsurgency*), wobei irreguläre und hybride Kriegführung einen immer höheren Stellenwert gewinnen.[8]

Die Streitkräfte brauchen jedoch für internationale Einsätze die Fähigkeit, im Verbund den irregulären Gegnern und hybriden Bedrohungen entgegen zu treten, und zusätzlich die Fähigkeit zur regulären Kriegführung. Diese reguläre Kriegführung ist in einem breiten Spektrum notwendig, unabhängig von der Art des Gegners.[9]

Außerdem ist Schweden hinsichtlich operativer Gesamtstaatlichkeit im institutionellen Kontext – soweit aus offenen Informationen bekannt ist – nicht besonders stark aufgestellt. In Schweden sind mehrere unterschiedliche Ministerien, Ämter und Behörden für den Schutz vor hybriden Bedrohungen und deren Abwehr verantwortlich. Jedoch sind diese verschiedenen Behörden unabhängig voneinander und nicht umfassend koordiniert.

---

6 Militärstrategische Doktrin mit doktrinären Gründen. In: Streitkräfte. Ausgabe 2012, M7739 -354023, S. 29. Aus dem Schwedischen übersetzt.

7 Ebd., S. 29. Aus dem Schwedischen übersetzt.

8 Ebd., S. 30. Aus dem Schwedischen übersetzt.

9 Ebd., S. 134. Aus dem Schwedischen übersetzt.

Identifizierung möglicher Akteure einer hybriden Bedrohung

Schweden hat in der öffentlichen Diskussion keine tatsächlichen Gegner mit der Fähigkeit zur hybriden Machtprojektion identifiziert.

Allerdings gibt es ausländische staatliche Akteure wie fremde Nachrichtendienste (z.B. in Russland; siehe Anhang Nord-Stream-Projekt, Kapitel 5.1) und nichtstaatlicher Konfliktakteure in Schweden (im Terrorismus und in der organisierten Kriminalität) mit potenziellen Kapazitäten.

Schweden wird auch mit Aufständischen und Terrorgruppen in internationalen Einsätzen in fragilen Staaten (*failing states*) oder regionalen Konflikten konfrontiert, die hybride Bedrohungen nützen (z.B. im Fall von Afghanistan; siehe Anhang).

Einsatz von Massenvernichtungswaffen (MVW) durch Terroristen und IT-Bedrohungen sind auch als potenzielle hybride Bedrohungen identifiziert worden, obwohl das nicht in allen offiziellen Dokumenten erwähnt ist. Vielleicht könnten auch extremistische Akteure und der internationale Terrorismus wie Al-Kaida in diese Gruppe aufgenommen werden.

Schutz der kritischen Infrastruktur

Die Gefahreneinschätzung hinsichtlich der kritischen Infrastruktur ist in Schweden mehrdimensional ausgeprägt. Es gibt mehrere nationale Kooperationsprojekte für den Schutz der kritischen Infrastruktur. Jedoch gibt es keine Sicherheitskonzepte, die hybride Bedrohungen erwähnen.

Ein wichtiger Akteur ist das Amt für Bevölkerungsschutz und Bereitschaft (MSB; Swedish Civil Contingencies Agency).[10] Die Aufgabe des MSB besteht darin, die gesellschaftlichen Kapazitäten zu verbessern und die Vorbereitung und präventive Vermeidung von Notfällen und Krisen zu unterstützen.

Weitere wichtige Akteure sind:

---

[10] Myndigheten för samhällsskydd och beredskap, <www.msb.se.>.

- Der Kooperative Rat für Terrorismusbekämpfung
- Das Nationale Zentrum für die Bewertung der Bedrohungslage im Terrorismus (NCT)
- Das Kooperationsprojekt „Nationale Zusammenarbeit gegen schwere IT-Sicherheitsbedrohungen“ (NSIT)
- Die Kooperationsgruppe für Informationssicherheit (SAMFI)
- Das Kooperationsprojekt gegen gefährliche Stoffe (SOFÄ)

Der Kooperative Rat für Terrorismusbekämpfung ist eine Partnerschaft von vierzehn schwedischen Behörden mit dem Ziel, Schwedens Fähigkeit zur Terrorismusbekämpfung zu stärken. Der Rat hielt seine erste Sitzung im Februar 2005. Der Rat wird vom Generaldirektor des Sicherheitsdienstes geleitet. Im Rat vertreten sind auch die höchsten Beamten der nationalen Polizei, Streitkräfte, Nachrichtendienst, Amt für Bevölkerungsschutz und Bereitschaft (MSB), die Küstenwache, Zollamt, Strahlenschutz und so weiter.[11]

Unter dem Kooperativen Rat für Terrorismusbekämpfung ist das Nationale Zentrum für die Bewertung der Bedrohungslage im Terrorismus (NCT) angesiedelt. Dem NCT gehören Vertreter des Nachrichtendienstes und des Sicherheitsdienstes an. Die Aufgaben des NCT umfassen die Erstellung von strategischen Analysen über Ereignisse, Trends und externe Entwicklungen im Zusammenhang mit Terrorismus, welche Schweden und schwedische Interessen beeinflussen oder beeinflussen können.[12]

Das Kooperationsprojekt „Nationale Zusammenarbeit gegen schwere IT-Sicherheitsbedrohungen“ (NSIT) ist eine Kooperation zwischen dem Sicherheitsdienst, den Streitkräften und der Nachrichtendienste. Das Kooperationsprojekt hielt seine erste Sitzung im Dezember 2012. NSIT analysiert und bewertet die Bedrohungen und Schwachstellen und ergreift Schutzmaßnahmen im Falle einer schweren oder qualifizierten IT-Bedrohung gegen die wichtigsten nationalen Interessen. Expertengruppen arbeiten an

---

[11] Samverkansrådet mot terrorism, Counter-Terrorism Co-operative Council: Webseite des Sicherheitsdienstes, www.sakerhetspolisen.se; Säkerhetspolisen, Årsrapport 2013, S. 15.

[12] Nationellt centrum för terrorhotbedömning, National Centre for Terrorist Threat Assessment: Webseite der Sicherheitsdienstes, <www.sakerhetspolisen.se>.

konkreten Projekten. Die Arbeit wird im Auftrag der einzelnen Agenturen durchgeführt und beinhaltet keine zusätzlichen Befugnisse. NSIT arbeitet nicht gegen Cyber-Kriminalität wie Finanzbetrug oder *distributed denial-of-service* (DDoS)-Angriffe gegen Webseiten.[13]

Unter dem MSB ist die Kooperationsgruppe für Informationssicherheit (SAMFI), eine Partnerschaft der nationalen Polizei, des Sicherheitsdienstes, der Streitkräfte, des Nachrichtendienstes und so weiter.[14]

Auch unter dem MSB ist das Kooperationsprojekt gegen gefährliche Stoffe (SOFÄ). Dieses Kooperationsprojekt ist nur ein nationales Forum und eine Referenzgruppe ohne zusätzliche Befugnisse, aber es ist doch eine wichtige Expertengruppe und spielt eine Rolle für die Bereitschaft.[15]

Jedoch sind diese verschiedenen Behörden voneinander unabhängig und nicht koordiniert. Außerdem sind ihre Verantwortungsbereiche sehr begrenzt und sie üben keine Kontrolle über Aktivitäten in ihrem Bereich aus. Im institutionellen Kontext gibt es keine ständige interministerielle Arbeitsgruppe, nur Kooperationsprojekte; in Zeiten der Krise werden temporäre Arbeitsgruppen auf einer ad hoc-Basis einberufen (siehe Anhang zum Nord-Stream-Projekt, Kapitel 5.1).

Ein weiterer Aspekt des Schutzes kritischer Infrastrukturen ist Energiesicherheit. Schweden ist abhängig von Einfuhren von Öl und Ölprodukten. Ölkonzerne, Großindustrie und Kraftwerke sind erforderlich, um eine Notversorgung mit Rohöl und Ölprodukten in Mengen die 90 Tage des normalen Verbrauches entsprechen zu gewährleisten. Der Einsatz dieser Notfall-Versorgung wird von der EU und der Internationalen Energieagentur (IEA) auf der Basis internationaler Abkommen beschlossen. Im Krisenfall werden diese Organisationen das Öl unter den Mitgliedstaaten aufteilen. Schweden übt keine unabhängige Kontrolle über diese zentrale Rohölspeicherung aus. Da Schweden kaum Erdgas

---

13 Samarbetsprojektet Nationell samverkan till skydd mot allvarliga IT-hot: Webseite der MSB,< www.msb.se>; Säkerhetspolisen, Årsrapport 2013, S.12.

14 Samverkansgruppen för informationssäkerhet: Webseite der MSB, <www.msb.se>.

15 Samverkansområdet Farliga Ämnen: Webseite der MSB, <www.msb.se>.

nutzt, gibt es keine ähnlichen Vorkehrungen für eine Notfall-Erdgasspeicherung.[16]

2.2.2 Operationen und Interaktionen

Kooperationsbereitschaft zwischen Regierungsstellen

Schwedens sicherheitspolitische Ausrichtung ist von einer sehr starken Kooperationskultur geprägt. Die innerstaatlichen Akteure müssen kooperieren und einen Konsens finden. Allerdings ist die Gesamtstaatlichkeit im institutionellen Kontext nicht besonders ausgeprägt und die formal-strukturelle Kooperation zwischen Ministerien ist – soweit es bewertet werden kann – nicht stark. Jedoch verfügt Schweden über einen tatsächlichen gesamtstaatlichen Ansatz in nationalen Kooperationsprojekten. Dieser Ansatz gestaltet sich pragmatisch und zweckmäßig, ist aber jedoch nicht operationalisiert. In einer tatsächlichen Krise würde die Zusammenarbeit von Praxis- und ad hoc-Ansätzen abhängen.

Allerdings gibt es doch Zusammenarbeit. Ministerien sind nach dem Verwaltungsrecht verpflichtet miteinander zu kooperieren.[17] Doch gibt es nur wenige formalisierte Schnittstellen für eine gemeinsame Lagebeurteilung, falls Schutzmaßnahmen notwendig sind.

Die tatsächliche Kooperationsbereitschaft ist nicht leicht zu beurteilen. Da es nur wenige Dokumente zu diesem Thema gibt, sind pragmatische Ansätze notwendig. Die praktischen Erfahrungen bei historischen Krisen zeigen, dass eine Zusammenarbeit stattfinden wird, allerdings gibt es nur wenige formale Vorkehrungen zwischen den relevanten Akteuren.

---

16 Statens energimyndighet: Hur trygg är vår energiförsörjning? En översiktlig analys av hot, risker och sårbarheter inom energisektorn 2006 (Eskilstuna: Statens energimyndighet, Referenz ER 2007:06, veröffentlicht 2007), S. 23 und 25.

17 (Schwedisches) Verwaltungsgesetz von 1986, § 6.

Sicherheits-Cluster-Ansätze

In Schweden sind mehrere unterschiedliche Ministerien, Ämter und Behörden für den Schutz vor hybriden Bedrohungen, und im Falle des Eintretens, für deren Abwehr verantwortlich. Allerdings sind diese Behörden unabhängig und nicht vollständig koordiniert, obwohl sie zur Kooperation verpflichtet sind. Außerdem sind ihre Verantwortungsbereiche sehr begrenzt und sie üben keine tatsächliche Kontrolle über Aktivitäten in ihrem Bereich aus.

Ein üblicher Ansatz ist, wie immer, auf pragmatischen ad hoc-Lösungen basiert. Dies würde auch ermöglichen, die Streitkräfte zu unterstützen und im Gegenzug aus anderen Ersthelfer-Organisationen wie der Polizei und Küstenwache Unterstützung zu erhalten. Leider bedeutet das Anstreben von ad hoc-Lösungen natürlich, dass die Sicherheits-Cluster-Ansätze nicht sehr etabliert sind.

Schnittstellen zwischen staatlichen und nicht-staatlichen Akteuren

Schnittstellen zwischen staatlichen und nicht-staatlichen Akteuren sind heute – soweit bewertet werden kann – nicht stark definiert bzw. ausgeprägt. Übungen, wie sie noch während des Kalten Krieges gewohnt waren, finden selten oder nicht mehr statt.

Gemeinsame Lagebeurteilung

Eine gesamtstaatliche, auf einem *Whole of Nation*-Ansatz basierende Bedrohungsanalyse mit einem gemeinsamen Lagebild und gemeinsamen Lageverständnis staatlicher und nicht-staatlicher Akteure fehlt – soweit es bewertet werden kann – in vielen Verantwortungsbereichen. Doch verfügt Schweden über einen tatsächlichen gesamtstaatlichen nicht-operativen Ansatz bei nationalen Kooperationsprojekten, z.B. die Projekte hinsichtlich des Schutzes der kritischen Infrastruktur. Man kann folglich in Schweden relevante gesamtstaatliche Elemente identifizieren, die sich jedoch nicht institutionell niederschlagen. Institutionelle Strukturen zur gemeinsamen Lagebeurteilung fehlen.

Gemeinsame Schutzmaßnahmen

Da eine gesamtstaatliche Bedrohungsanalyse in den meisten Fällen fehlt, können gemeinsame Schutzmaßnahmen – soweit dies bewertet werden kann – nicht sehr stark sein.

2.2.3 IKKM

Wechselwirkungen im Hinblick auf eine Beteiligung im IKKM im Einsatzraum

Im Einsatzraum kennen nur die Streitkräfte ein Konzept der hybriden Machtprojektion, das allerdings auf die Kriegsführung begrenzt ist. Die Möglichkeit einer hybriden Bedrohung in anderen Verantwortungsbereichen im Einsatzraum ist kaum identifiziert worden, aber es gibt sie doch (z.B. im Fall von Afghanistan; siehe Anhang).

Die Militärstrategische Doktrin (MSD 12), de facto hauptsächlich relevant für internationale Einsätze (und möglicherweise nur de jure von Belang für die Territorialverteidigung), erwähnt hybride Kriegführung und hybride Bedrohung im Einsatzraum als relevant:

Die Streitkräfte brauchen jedoch für internationale Einsätze die Fähigkeit, zusammen mit anderen Partnern irregulären Gegnern und hybriden Bedrohungen entgegen zu treten, parallel mit der Fähigkeit zur regulären Kriegführung. Diese reguläre Kriegführung ist in unterschiedlichem Ausmaß notwendig, unabhängig von der Art des Gegners.[18]

[18] Militärstrategische Doktrin mit doktrinären Gründen. In: Streitkräfte. Ausgabe 2012, M7739 -354023, S. 134. Aus dem Schwedischen übersetzt.

Die Worte „zusammen mit anderen“ in diesem Kontext haben eine pragmatische Bedeutung. Damit ist z.B. die Bereitschaft Schwedens für IKKM-Einsätze in enger Anbindung an die NATO möglich.[19]

Wechselwirkungen im Hinblick auf eine Beteiligung im IKKM im Entsendestaat

Die Möglichkeit einer hybriden Bedrohung im Entsendestaat als Reaktion auf eine Beteiligung im IKKM wird – soweit bewertet werden kann – als nicht akut eingestuft. Doch es gibt solche Möglichkeiten, wie im Anhang zu Afghanistan erklärt wird.

Einbettung in Sicherheitsorganisationen

In Anbetracht der wenigen existierenden Dokumente über hybride Bedrohungen ist es schwer zu bewerten, ob Schweden den Schutz vor hybriden Bedrohungen primär als eine nationale oder internationale Aufgabe bewertet. Schwedens traditionelle Allianzfreiheit und Neutralitätspolitik erschweren die Bewertung zusätzlich. Wie angemerkt, berücksichtigt die Militärstrategische Doktrin (MSD 12) die Bereitschaft für IKKM z.B. in enger Anbindung an die NATO oder an andere Sicherheitsorganisationen. Es kann jedoch bewertet werden, dass in Schweden die Identifizierung und die Bewältigung hybrider Bedrohungen wahrscheinlich primär als eine nationale Aufgabe angesehen wird.

2.2.4 Folgerungen

Das Konzept der hybriden Machtprojektion oder hybriden Bedrohung wird in Schweden – soweit bewertet werden kann – nicht stark thematisiert. Dies kann zu einem großen Teil durch Schwedens fehlende Bereitschaft zur Formulierung formaler Strategiedokumente für den nicht-militärischen Bereich erklärt werden. Das Konzept erhöht auch die Schwierigkeiten für die Streitkräfte. Da hybride

---

[19] Für eine Diskussion siehe dazu Gauster, Markus: Whole of Nation-Ansätze auf dem Prüfstand. Ein neues Paradigma im internationalen Krisenmanagement? Wien 2013, S. 67ff.

Kriegführung alles umfasst, von der konventionellen Kriegführung über Terrorismus bis hin zu organisierter Kriminalität und Cyberbedrohungen, ist es schwierig, die zukünftige Stärke und Größe der Streitkräfte für diese Bedrohungen zu planen. Darüber hinaus fehlt den schwedischen Streitkräften die Fähigkeit, auf all die vielen Formen hybrider Bedrohungen ohne Unterstützung von anderen Ersthelfer-Organisationen angemessen zu reagieren.

In Schweden sind doch mehrere unterschiedliche Ministerien, Ämter und Behörden für den Schutz gegen hybride Bedrohungen und, im Falle des Eintretens, für deren Abwehr verantwortlich. Die formal-strukturelle Kooperation zwischen Ministerien ist – soweit bewertet werden kann – nicht stark, doch verfügt Schweden über einen tatsächlichen gesamtstaatlichen Ansatz bei nationalen Kooperationsprojekten und verfügt über eine traditionelle Kooperationskultur. Dieser Ansatz ergibt sich aus der typisch schwedischen Konsensorientierung; er ist jedoch nicht operativ. Außerdem sind diese Behörden unabhängig und nicht vollständig koordiniert. Allerdings sind ihre Verantwortungsbereiche sehr begrenzt und sie üben keine tatsächliche Kontrolle über Aktivitäten in ihrem Bereich aus.

Bisher hat Schweden keine Gegner mit der Fähigkeit hybrider Machtprojektion öffentlich identifiziert. Allerdings gibt es doch ausländische staatliche Akteure (z.B. Russland) und nicht-staatliche Konfliktakteure in Schweden (Terrorismus und organisierte Kriminalität) mit der potenziellen Kapazität. Im IKKM wurde die Möglichkeit einer hybriden Bedrohung auch selten identifiziert, aber es gibt sie doch (wie z.B. im Fall von Afghanistan).

3 Ergänzende Analyse im Kontext von hybriden Bedrohungen

3.1 Hybride Bedrohungen: eine Reflexion über Ableitungen aus strategischen Dokumenten der EU

Gerald Brettner-Messler

„Hybrid" bedeutet „aus Verschiedenartigem zusammengesetzt, gemischt". Die hybride Bedrohung ist also eine, die sich aus verschiedenen Elementen zusammensetzt, die abgestimmt zur gleichen Zeit angewendet werden (können). Mit dieser Bezeichnung soll ein wesentlicher Aspekt der heutigen Bedrohungssituation beschrieben werden. Die vielfältigen Möglichkeiten und deren Nutzung durch bestimmte Gegner der Rechtsordnung und des Gesellschaftssystems der Europäischen Union sollen mittels dieses neuen Begriffs deutlich aufgezeigt werden, um sie entsprechend bekämpfen zu können. Doch finden sich hybride Bedrohungen überhaupt in den strategischen Dokumenten der Union?

Das zentrale Papier ist die Europäische Sicherheitsstrategie (ESS), die auf der Sitzung des Europäischen Rates am 12. Dezember 2003 angenommen wurde. Wesentliche Herausforderung nach den Anschlägen vom 11. September 2001 in New York und Washington war die Bekämpfung des Terrorismus. 2004 wurde eine „Strategie gegen die Terrorismusfinanzierung" präsentiert. Im Jahr darauf – nach den Anschlägen in Madrid 2004 und London 2005 – folgten die „Strategie der EU zur Terrorismusbekämpfung" und die „Strategie zur Bekämpfung der Radikalisierung und Anwerbung für den Terrorismus".[1] Ebenfalls 2005 wurde die „Strategie für die Außendimension des Raums der Sicherheit, der Freiheit und des Rechts" vorgestellt. Der technischen Entwicklung wurde mit der „Strategie für eine sichere Informationsgesellschaft" 2006 Rechnung getragen. 2008 wurde der „Bericht über die Umsetzung der ESS" vorgestellt, der die Punkte der

[1] Zur Terrorismus und EU siehe: Hauser, Gunther: Europa und der Kampf gegen den Terrorismus. In: Hauser, Gunther/Brettner-Messler, Gerald (Hrsg.): Sicherheit und Recht zu Beginn des 21. Jahrhunderts. Schriftenreihe der Landesverteidigungsakademie 8/2007. Wien 2007, S. 11ff.

ESS in aktualisierter Form behandelt. 2010 folgte die „Strategie für die innere Sicherheit der EU“.[2]

3.1.1 Theoretische Überlegungen zum Begriff „hybride Bedrohung/Kriegsführung“

Der Begriff der „hybriden Bedrohung/Kriegsführung“ tauchte spätestens 2002 in der militärischen Fachliteratur in den USA auf.[3] Es dauerte eine Zeit, bis die Diskussion darüber Europa erreichte; richtig in Gang gekommen ist sie bis heute nicht. In einem Artikel von 2012 ist zu lesen, dass sie in Deutschland erst begonnen habe.[4] Demgemäß ist diese Bedrohungsform auch in aktuellen Dokumenten nicht ausdrücklich genannt. Das gilt nicht nur für die EU. Das Strategische Konzept der NATO von 2010 geht auf hybride Bedrohungen gleichfalls nicht ein. Bedrohungen (Terrorismus, Cyber-Angriffe, Verbreitung von Massenvernichtungswaffen usw.) werden genannt, es findet aber keine Zusammenschau statt, somit wird nicht gesagt, was es bedeutet, wenn mehrere Bedrohungen gezielt gleichzeitig erfolgen und was die Ableitungen aus dieser Gleichzeitigkeit sind. Dieser Faktor ist aber für die Charakteristik einer Bedrohung als „hybrid“ sehr wichtig. Michael Miklaucic meint, dass hybride Bedrohungen mehr als die Summe einzelner Bedrohungen sind. Er unterstreicht auch, dass es nicht um die bloße, zufällige Gleichzeitigkeit von Bedrohungen geht, sondern um systematische Anwendungen zur Erreichung von Zielen. Darin liegt die Besonderheit: die Bedrohungen für sich genommen sind allesamt nicht neu, die Neuheit liegt in ihrer Kombination. Ein wichtiger Punkt ist, dass es nicht bloß um nichtstaatliche Gegner geht: Die Bedrohung kann auch, muss aber nicht von

---

2 Es gibt noch eine Reihe anderer Dokumente, die die Ausrichtung der EU im Bereich Sicherheit zum Inhalt haben. Die oben aufgelisteten sind die zentralen Papiere zu dem Thema; es handelt sich um keine vollständige Aufzählung.

3 Siehe: Hoffman, Frank G.: Hybrid Threats: Neither Omnipotent nor Unbeatable. In: Orbis (2010), doi:10.1016/j.orbis.2010.04.009. <http://www.lifelong.ed.ac.uk/OAC2010/archive/Hoffman%202010%20Hybrid%20Threats.pdf>. Laut Hofmann war eine der ersten Arbeiten zu dem Thema: Nemeth, William. J.: Future War and Chechnya: A Case for Hybrid Warfare. Monterey, CA, Naval Postgraduate School, June 2002.

4 Oprach, Marc: Hybrid Warfare – neue Dimension der terroristischen Bedrohung. Herausforderung an die Sicherheitspolitik. In: Die Politische Meinung, Nr. 508, März 2012, S. 59ff, hier S. 59. <http://www.kas.de/wf/doc/kas_30476-544-1-30.pdf?120402104509>.

einem Staat kommen. Staaten werden sich vor allem hybrider Kriegführung bedienen, wenn es darum geht, Mittel zum Einsatz zu bringen, die ihnen nicht zugeordnet werden können (z.B. indem Soldaten im Ausland ohne Hoheits- und Dienstabzeichen eingesetzt werden und der Einsatz bestritten wird – Russland soll so in der Ukraine verfahren haben[5]). Dieser Umstand muss bei Gegenmaßnahmen bedacht werden. Bei der Bekämpfung von hybriden Bedrohungen geht es nicht so sehr um neue Fähigkeiten als um neue Prozesse und ein neues Denken.[6]

Mit dem Begriff der „hybriden Bedrohung" soll der geänderte Charakter militärischer Herausforderungen umfassend beschrieben und herkömmliche Charakterisierungen hinfällig werden, um die gegenwärtigen Realitäten besser erfassen zu können. Nach 9/11 standen die USA einem Gegner gegenüber, der zu vergleichsweise geringen Kosten einen Schaden angerichtet hatte, den zu verursachen bis dato nur regulären Streitkräften zugetraut worden war. Terrorismus und Kriminalität als wichtige Finanzierungsmöglichkeit für Terrorgruppen sollten nach 9/11 entsprechend in die theoretischen Überlegungen über Bedrohungen einbezogen werden. Frank Hoffman, der die Debatte um den Begriff „hybride Bedrohung" wesentlich mitgestaltete, zitierte einen britischen General, der gemeint hatte, dass Vergangenheit und Tradition in Streitkräften machtvolle Prismen seien, durch die gegenwärtige und künftige Trends gesehen werden. Dieses Verzerrungseffekts müssten sich Streitkräfte bewusst sein.[7]

Hoffman meint, dass die Debatte über die Natur von Kriegen sich oft zwischen den beiden Polen „counterinsurgency" bzw. „nation building" und konventionellen Kriegen bewegt habe, eine „bipolare Diskussion", die inadäquat sei.[8] Er stellte sich die Frage, was denn „konventionell" überhaupt bedeute, und bemerkte zutreffend, dass (in den USA) niemand annehme, eine Auseinandersetzung mit China, Nordkorea, dem Iran oder Russland würde „konventionell",

---

5 Kleine grüne Männchen, ein "Hybrid-Krieg" und die Probleme der NATO. In: Vorarlberg Online, 25.06.2014. <http://www.vol.at/kleine-gruene-maennchen-ein-hybrid-krieg-und-die-probleme-der-nato/4006225>.

6 Miklaucic, Michael: NATO Countering the Hybrid Threat. 23.09.2011. <http://www.act.nato.int/nato-countering-the-hybrid-threat>.

7 Hoffman, Frank G.: Hybrid Threats: Neither Omnipotent nor Unbeatable. In: Orbis (2010), doi:10.1016/j.orbis.2010.04.009, S. 5.

8 Ebd., S. 5.

also mit Panzern, Raketen, Kampfflugzeugen usw., geführt werden – so verstand Hoffman den Begriff „konventionell“.[9] Sind also Russland, China usw. keine konventionellen Gegner? Als Beispiel für eine moderne „hybride Kriegsführung“ führte er die Auseinandersetzungen 2006 mit der Hisbollah im Libanon an. Dieser nichtstaatlichen Gruppe war es gelungen, mit einer Anti-Schiffs-Rakete ein israelisches Boot zu treffen, wodurch gewohnten Einschätzungen über die Fähigkeit solcher Gruppen zur maritimen Kampfführung Abbruch getan wurde.[10]

Die Hisbollah war sich der Art und Weise ihrer Kriegsführung voll bewusst und Hassan Nasrallah, ihr Chef, reflektierte auch darüber. Er beschrieb die Kampfweise seiner Organisation als „irgendwas zwischen klassischem Krieg und Guerillakampf“.[11] Zentraler Faktor für eine solche Form der Kriegsführung ist die Einschätzung, dass in westlichen Gesellschaften die Menschen am Leben hängen, während für ihre islamischen Widersacher der Tod keinen Schrecken hat – damit ist in letzter Konsequenz durch das physische Ausschalten des Gegners kein (psychologischer) Sieg zu erreichen, weil schon ihre bloße Weiterexistenz aus Sicht der Hisbollah ein Erfolg für sich selbst und eine Niederlage für den Gegner ist.[12] Ein Kritiker von Hoffmans Auffassung, Dan G. Cox, wandte ein, dass dessen Konzept zu ungenau sei, um damit in der Praxis etwas anfangen zu können. Letztlich müssen die Erkenntnisse über neue Bedrohungen bzw. Kriegsführung in konkrete Handlungsoptionen münden. Davor steht aber die Diskussion, wie denn diese neue Bedrohung bzw. die Art, Kriege zu führen, genau beschaffen ist.[13]

---

9 Ebd., S. 6.

10 Ebd., S. 6f.

11 Sahm, Ulrich W.: Raketenbedrohung Israels. Der neue islamistische 'hybride Krieg' zur Judenvernichtung und Weltherrschaft. 16.12.2011. <http://derwille.wordpress.com/2011/12/16/raketenbedrohung-israels-der-neue-islamistische-hybride-krieg-zur-judenvernichtung-und-weltherrschaft/>.

12 Sahm, Ulrich W.: Raketenbedrohung Israels. Der neue islamistische 'hybride Krieg' zur Judenvernichtung und Weltherrschaft. 16.12.2011. <http://derwille.wordpress.com/2011/12/16/raketenbedrohung-israels-der-neue-islamistische-hybride-krieg-zur-judenvernichtung-und-weltherrschaft/>.

13 Cox, Dan G.: What if the Hybrid Warfare/Threat Concept Was Simply Meant to Make Us Think? 13.02.2013. <http://www.e-ir.info/2013/02/13/what-if-the-hybrid-warfarethreat-concept-was-simply-meant-to-make-us-think/>.

„Hybride Kriegsführung" bezeichnet eine Kombination von regulären und irregulären Methoden der Kriegsführung. Hybridität kann als Reflexion über die Einheit materieller und kognitiver Elemente in der Kriegsführung verstanden werden. Das entscheidende Mittel, auf das es im Krieg ankommt, ist nicht das Militär. Gemäß dieser Sichtweise kann jeder Kriege führen, unabhängig davon, welche „militärischen" (Anführungsstriche aus dem Originaltext übernommen) Mittel er besitzt.[14] Sadowski und Becker wollen in ihrem Beitrag die wahre Natur des Kriegs diskutieren und entwickeln durch diese allgemeinen Beobachtungen einen gesamthaften Ansatz. Bei den kognitiven Elementen geht es um den Einfluss auf den menschlichen Verstand. Durch Täuschen, Ablenken, Abschrecken, Abraten wird der gegnerische Wille beeinflusst. Gefühle, Verhaltensweisen, Wahrnehmungen sind das Ziel, auf das die Mittel ausgerichtet werden.[15] Materielle Einrichtungen (z.B. Waffensysteme) werden so umgangen und trotzdem kann auf den Gegner eingewirkt werden. Eine solche Form der Kriegsführung ist besonders für eine Kriegspartei interessant, die ihrem Gegner materiell unterlegen ist[16] – siehe dazu das weiter oben angeführte Beispiel der Hisbollah. Letztlich sind beide Elemente für den Gesamterfolg essentiell: es müssen die Köpfe der Gegner erreicht werden, aber materielle Erfolge (physische Schäden) sind trotzdem unerlässlich. Es geht darum, beide Elemente zu integrieren und im richtigen Verhältnis anzuwenden. Materiell unterlegene Gegner werden kostengünstige Mittel anwenden, die enorme Schäden anrichten (Bsp. 9/11).[17]

Sadowski und Becker listen als Bedrohung für die USA folgende Arten von „kleinen Kriegen" auf: Aufstände (Irak, Afghanistan), Piraterie (Horn von Afrika, Straße von Malakka), Terrorismus (Al-Kaida), Organisierte Kriminalität (Taliban, Mafia, Drogenkartelle), Abschnüren „allgemeiner Güter" (Angriffe im Cyberspace, Sperre der Straße von Hormuz), Proto-Staaten (Organisationen mit quasi-staatlichem Charakter, die von den offiziellen staatlichen Einrichtungen geduldet werden, z.B. die Farc – Fuerzas Armadas Revolucionarias de Colombia, Revolutionäre Streitkräfte Kolumbiens – oder die Hisbollah). Als Beispiel für einen „großen Krieg" nennen sie eine Konfrontation mit China um Taiwan.

---

14 Sadowski, David/Becker, Jeff: Beyond the „Hybrid" Threat. Asserting the Essential Unity of Warfare. In: Small Wars Journal, 2010, S. 4. <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-etal.pdf>.

15 Ebd., S. 4f.

16 Ebd.

17 Ebd., S. 5f.

„Große Kriege" werden wohl mit konventionellen Streitkräften, unter Umständen mit Einsatz von Nuklearwaffen, geführt werden. Die Opferzahlen sind höher, die örtliche Ausdehnung weiter, sie werden verhältnismäßig rasch beendet sein. Materielle Elemente werden eine wichtige Rolle spielen und die Bandbreite der eingesetzten Mittel (Militär, Wirtschaft, Diplomatie) wird groß sein. In „kleinen Kriegen" liegt der Erfolg mehr an kognitiven Elementen, die Dauer wird länger sein, es wird also Geduld und Durchhaltevermögen bedürfen.[18] Die große Herausforderung bei so verschiedenen Möglichkeiten von Konflikten besteht künftig in der Wahrung der Einheit der Kriegsführung, angesichts der Notwendigkeit sich verschiedener Elemente der Kriegsführung in der jeweils passenden Weise bedienen zu müssen – eine hohe Anpassungsfähigkeit ist somit erforderlich, um rasch auf Unerwartetes reagieren zu können.[19] Die Aussage der beiden Autoren über die Führung eines Krieges gilt letztlich für die Bewältigung hybrider Herausforderungen insgesamt, denn schon in Friedenszeiten müssen die Mittel abgestimmt werden, um es erst gar nicht zu einem Krieg kommen zu lassen.

3.1.2 Hybride Herausforderungen oder Bedrohungen?

Aus diesem Grund ist es wohl besser von „hybriden Herausforderungen" zu sprechen, weil Sicherheitspolitik so früh ansetzen sollte, dass Bedrohungen erst gar nicht entstehen können. Damit eine Bedrohung als solche bezeichnet werden kann, muss sie eine gewisse „strategische Schwelle" überschreiten. Die Entstehung der Bedrohung liegt aber schon vor dem Erreichen dieser Schwelle. Dort muss die Bekämpfung bereits ansetzen. Die Europäische Sicherheitsstrategie verlangt auch ein solches Vorgehen:

> „Die neuen Bedrohungen sind dynamischer Art. Die Proliferationsrisiken nehmen immer mehr zu; ohne Gegenmaßnahmen werden terroristische Netze immer gefährlicher. Staatlicher Zusammenbruch und Organisierte Kriminalität breiten sich aus, wenn ihnen nicht entgegengewirkt wird [...] *Daher müssen wir bereit sein, vor Aus-*

---

18 Ebd., S. 7f.
19 Ebd., S. 10.

bruch einer Krise zu handeln. Konflikten und Bedrohungen kann nicht früh genug vorgebeugt werden."[20]

Gehandelt muss also werden, noch ehe Bedrohungen manifest werden. „*Im Mittelpunkt unserer Bemühungen muss die frühzeitige Prävention stehen, damit Bedrohungen nicht zu Konfliktquellen werden*", heißt es dazu im Umsetzungsbericht.[21]

Heruntergebrochen auf die operative Ebene bedeutet das beispielsweise – wie es in der Strategie für Terrorismusbekämpfung festgelegt ist –, dass das Reisen in Konfliktgebiete überwacht werden soll. Reisen selbst ist keine Tätigkeit, die im Sinne der Terrorismusbekämpfung rechtlich relevant ist, darüber Kenntnis zu erlagen ist aber für die zuständigen Behörden notwendig.[22] Aktuell gab es in diesem Zusammenhang erst vor kurzem einen Fall in Österreich. Zwei junge Mädchen, 15 bzw. 16 Jahre alt, waren aus Wien abgängig, kurz darauf wurden Signale ihrer Mobiltelefone in der Türkei geortet, angeblich auch in Syrien. In Online-Postings behaupteten die Mädchen (oder Personen, die sich als diese ausgaben), dass sie sich islamistischen Kämpfern in Syrien angeschlossen hätten.[23] Entsprechende weltanschauliche Aussagen hatten eine der beiden bereits in Wien getätigt. Verhindert können solche Reisen nicht werden, es ist aber wichtig, darüber Bescheid zu wissen, um Stimmungslagen und Einstellungen in bestimmten Bevölkerungsgruppen zu kennen und in der Folge Gegenmaßnahmen zu ergreifen – in einem Fall wie dem vorliegenden z.B. verstärkte Aufklärung über terroristische Bewegungen unter (muslimischen) Jugendlichen. Und natürlich soll die Identität von islamistischen Kämpfern möglichst geklärt wer-

---

20 Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 7. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

21 Rat der Europäischen Union: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie – Sicherheit schaffen in einer Welt im Wandel. Brüssel 11.12.2008, S. 9, 407f. <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/DE/reports/104634.pdf>.

22 Rat der Europäischen Union: Strategie der Europäischen Union zur Terrorismusbekämpfung. 14469/4/05 REV 4. Brüssel 30.11.2005, S. 8. <http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2014469%202005%20REV%204>.

23 Henckel, Elisalex: Postergirls des Dschihad. Teenager mit einem Herz für al-Qaida. In: Die Welt Online, 15.5.2014. <http://www.welt.de/vermischtes/article128025803/Teenager-mit-einem-Herz-fuer-al-Qaida.html>.

den, um entsprechende sicherheitspolizeiliche Maßnahmen gegen sie ergreifen zu können.

Auch Staaten können Herausforderungen darstellen, noch ehe es zu einer Bedrohung kommt. Dazu ein Beispiel: China stellt sicherheitspolitisch für die europäischen Staaten zweifellos eine Herausforderung dar. Von einer Bedrohung zu sprechen, wäre wohl zu stark, weil es die Wirklichkeit nicht angemessen beschreibt. China ist als zweitstärkster Handelspartner der EU – wie das Wort sagt – ein bedeutender Partner der Europäer. Was nicht heißt, dass China ein Verbündeter ist und als solcher handelt. Es verfügt über verschiedene Mittel, die es zur Durchsetzung seiner Interessen einsetzen kann: militärische, wirtschaftliche, diplomatische, mediale, wissenschaftliche. Eine hybride Herausforderung stellt es deshalb dar, weil es seine Mittel gezielt und abgestimmt einsetzt und dies auch im Konfliktfall tun wird. Das zeigt sich gut am Beispiel chinesischer Cyber-Spionage. Die Einheit 61398 der chinesischen Volksbefreiungsarmee betreibt – laut U.S.-Justizministerium – Spionage via Internet. Sie soll für chinesische staatliche Unternehmen arbeiten, um diesen wirtschaftliche Vorteile zu verschaffen. Eine klare Trennung Militär – Wirtschaft ist nicht gegeben. Für die Volksrepublik hat Sicherheit eine wirtschaftliche Dimension und somit handelt es sich bei dieser Form der Spionage nicht einfach um „Wirtschaftsspionage".[24] Der chinesische Denkansatz ist überhaupt gesamthaft und weniger auf einzelne Kategorien wie Staat, Wirtschaft u.a. gerichtet. Die Volksbefreiungsarmee hat daher auch an der wirtschaftlichen Entwicklung des Landes mitzuarbeiten – so wird es im chinesischen Weißbuch für Verteidigung 2012 festgehalten.[25] China hat schon bewiesen, dass es im Konfliktfall das eigene wirtschaftliche Potential zu nutzen bereit ist. Als sich 2011 die Streitigkeiten mit Japan um Inseln im Ostchinesischen Meer verschärften, verhinderte China die Exporte von „Seltenen Erden" – wichtige Metalle für technische Produkte – nach Japan. China hat bei diesen Rohstoffen eine marktbeherrschende Stellung und demonstrierte Japan,

---

[24] Schmidt, Michael S./Sanger, David E.: 5 in China Army Face U.S. Charges of Cyberattacks. In: The New York Times Online, 19.05.2014. <http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0>.

[25] The Diversified Employment of China's Armed Forces. IV. Supporting National Economic and Social Development. 16.04.2013. <http://www.china.org.cn>, <http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm>.

dass es vor wirtschaftlichen Druckmitteln nicht zurückscheut.[26] Wenn chinesische Aktivitäten im Cyber Space bemerkt werden, so sind diese mit sehr hoher Wahrscheinlichkeit auch Vorbereitungsmaßnahmen für den Fall direkter Konfrontationen, um im richtigen Augenblick über die nötigen Informationen zu verfügen, Aktionen eines Gegners zu be- und verhindern und selbst mit maximaler Kraft zuschlagen zu können.

An dieser Stelle sei angemerkt, dass auch die USA über das Potential verfügen, eine hybride Herausforderung darzustellen. Dan G. Cox merkt an, dass das Konzept der hybriden Bedrohung so verstanden werden kann, dass die USA „die gefährlichste" hybride Bedrohung darstellen, weil sie verschiedene Mittel (militärische, politische, wirtschaftliche) konzertiert zum Einsatz bringen können.[27] Die durch den ehemaligen Mitarbeiter der National Security Agency Edward Snowden enthüllten Überwachungsmaßnahmen dieser Behörde sind eine Bestätigung einer solchen Bewertung: technisches Potential wird zu politischen, wirtschaftlichen und militärischen Zwecken ausgenutzt. Für die meisten EU-Staaten sind die USA aber Verbündeter im Rahmen der NATO, stellen also keine Herausforderung dar – zumindest in offiziellen Bewertungen.

Den Eindruck von Bedrohlichkeit will auch China nicht erwecken. Peking setzt gezielt „soft power" ein und zielt auf die Gefühle der Europäer. Panda-Bären sollen als „Botschafter" ein freundliches Bild von China vermitteln. Als 2014 zwei dieser Bären in ihrer neuen „Heimat" Belgien eintrafen, kurz vor einem Besuch von Staats- und Parteichef Xi Jinping, war sich der belgische Regierungschef Elio Di Rupo der Bedeutung der tierischen Gäste sehr wohl bewusst. „Für unsere Wirtschaft, den Handel, unsere wissenschaftlichen und kulturellen Beziehungen, ist das wirklich ein wichtiges Ereignis", bemerkte der Premierminister.[28] Ebenso ein Werbeträger ist der chinesische Nationalzirkus; diese Funktion wird auch gar nicht verschleiert: „Der Tradition verpflichtet und der Zu-

---

[26] Brettner-Messler, Gerald: Internationale Rundschau China. In: Österreichische Militärische Zeitschrift, 1/2011, S. 111ff, hier besonders S. 112.

[27] Cox, Dan G.: What if the Hybrid Warfare/Threat Concept Was Simply Meant to Make Us Think? 13.02.2013. <http://www.e-ir.info/2013/02/13/what-if-the-hybrid-warfarethreat-concept-was-simply-meant-to-make-us-think/>.

[28] Giant pandas get a celebrity welcome in Belgium. In: Reuters, 23.02.2014. <http://www.reuters.com/article/2014/02/23/us-belgium-pandas-idUSBREA1M0MV20140223>.

kunft mit innovativen Ideen zugewandt hat er es geschafft, auch neben den Akrobatik-Highlights insbesondere Chinas Geschichte, Kultur und Menschen einem interessierten Publikum näher zu bringen", heißt es auf der Homepage. Die auftretenden Künstler werden in über 1.000 (!) Zirkusschulen im ganzen Land ausgebildet.[29] Sportereignisse wie die Olympischen Spiele, die Darbietungen der Shaolin-Mönche und anderes sollen gleichfalls die Welt von Chinas kultureller Größe, aber auch von seinen friedlichen Ambitionen überzeugen.

Die Europäische Union, die (im Unterschied zur NATO) über zivile und militärische Mittel verfügt, sollte eigentlich besonders befähigt sein, hybriden Bedrohungen entgegenzutreten. In den strategischen Grundlagendokumenten kommt der Begriff der Hybridität bislang nicht vor. Die Europäische Sicherheitsstrategie wurde 2003 angenommen, als die Diskussion zu dem Thema erst am Beginn war. Auch im Bericht über die Umsetzung der ESS von 2008 bleibt der Begriff unerwähnt, weil er noch keine Verbreitung gefunden hatte.

Hybride Bedrohungen bedürfen eines Verursachers, der verschiedene Mittel zur Anwendung bringt. Konkrete Akteure werden in den europäischen Papieren kaum genannt. Staaten, wenn sie erwähnt werden, werden hauptsächlich als „Partner" bezeichnet, darunter Russland und China. Im Umsetzungsbericht aus 2008 wird der Iran mit seinem Nuklearprogramm als „Gefahr für die Stabilität der Region und für das gesamte Nichtverbreitungssystem"[30] bezeichnet. Auch Nordkorea wird im Zusammenhang mit der nuklearen Bedrohung explizit genannt. Eine hybride Bedrohung durch diesen Staat ist daraus nicht abzulesen. Namentlich kommt auch Afghanistan in dem Bericht vor, allerdings kann dieser Staat aufgrund seiner internen Probleme nicht als Akteur bezeichnet werden, er wird daher auch als Ziel von Stabilisierungsmaßnahmen beschrieben. Das gilt auch für die Demokratische Republik Kongo, Guinea-Bissau und Somalia, das zudem wegen der von dort ausgehenden Piraterie genannt wird.[31] Als Terrorgruppe wird Al-Qaida in der ESS beim Namen genannt; sie und die von ihr „inspirierten Gruppen" werden auch in der Terrorismusstrategie benannt, weil

---

29 Der chinesische Nationalcircus. <http://www.chinesischer.nationalcircus.eu>.

30 Rat der Europäischen Union: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie – Sicherheit schaffen in einer Welt im Wandel. Brüssel 11.12.2008, S. 1.

31 Ebd., S. 3, 7f.

sie die „größte Bedrohung der Union“[32] darstellten – autochthoner, europäischer Terrorismus wird als nachrangig erachtet. Erwähnt werden in den Strategie-Dokumenten Herausforderungen durch Phänomene wie Armut, Wettstreit um Naturressourcen oder Energieabhängigkeit.[33] Als Bedrohungen werden Prozesse wie Regionalkonflikte (z.B. der Balkankonflikt), das Scheitern von Staaten und die Piraterie genannt.[34]

3.1.3 Elemente hybrider Bedrohung

Terrorismus und Organisierte Kriminalität sind Handlungsweisen, die die Sicherheit gefährden. Terrorismus ist eine Form von Konfliktführung, die von einem Akteur angewendet wird und somit Teil einer hybriden Bedrohung sein kann. „Terroristen“ selbst können natürlich auch eine hybride Bedrohung bilden, indem sie verschiedene Mittel zum Einsatz bringen, von denen nicht jedes einzelne „terroristisch“ ist. Dass die Gefahr durch Terrorismus vielschichtig ist, wird im Umsetzungsbericht insofern erwähnt, als Terroristen als potentielle Verbreiter von Massenvernichtungswaffen bezeichnet werden.[35] Implizit ist auch in der ESS sehr wohl von hybriden Bedrohungen die Rede, denn am Ende des Kapitels über die Hauptbedrohungen wird, wie folgt, zusammengefasst:

> „Bei einer Summierung dieser verschiedenen Elemente – extrem gewaltbereite Terroristen, Verfügbarkeit von Massenvernichtungswaffen, Organisierte Kriminalität,

---

[32] Rat der Europäischen Union: Strategie der Europäischen Union zur Terrorismusbekämpfung. 14469/4/05 REV 4. Brüssel 30.11.2005, S. 7. <http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2014469%202005%20REV%204>.

[33] Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 2f. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

[34] Ebd., S. 4f; Rat der Europäischen Union: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie – Sicherheit schaffen in einer Welt im Wandel. Brüssel 11.12.2008, S. 1, 8.

[35] Rat der Europäischen Union: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie – Sicherheit schaffen in einer Welt im Wandel. Brüssel 11.12.2008, S. 3.

> Schwächung staatlicher Systeme und Privatisierung der Gewalt – ist es durchaus vorstellbar, dass Europa einer sehr ernsten Bedrohung ausgesetzt sein könnte."[36]

Diesen Satz kann man so verstehen, dass die Bedrohungen gleichzeitig und gezielt auf Europa einwirken könnten, und es ist anzunehmen, dass die Autoren es auch so gemeint haben.

Organisierte Kriminalität ist eine besondere Form wirtschaftlicher Aktivitäten, denen von zu diesem Zweck gebildeten Organisationen nachgegangen wird, die auch von Staaten ausgehen können. Cyberkriminalität ist eine weitere Form von Kriminalität, die in der ESS, im Umsetzungsbericht, aber auch in der Strategie für die innere Sicherheit genannt wird. Auch für sie gilt, dass sie von staatlichen und nichtstaatlichen Akteuren ausgeht und Element einer hybriden Bedrohung sein kann.

Die Spannweite von Cyber-Kriminalität ist groß. Es beginnt beim Ausspionieren staatlicher Geheimnisse oder Betriebsgeheimnisse von Unternehmen im Cyber-Raum, geht über Betrug mittels Internet (Herauslocken von Geld mittels Mails unter Vorspiegelung, dass eine finanzielle Vorleistung zum Antritt einer Erbschaft oder anderer vorgeblich verfügbarer Vermögenswerte nötig sei) bis zu Geschäften mit illegaler Ware im Internet (gefälschte Medikamente, Mode-, Elektroartikel usw., Raubkopien von Filmen und Musik, Kinderpornographie bis hin zu Waffen und Drogen). Kriminelle Handlungen im Cyber-Raum können aber auch als Beitrag zu anderen strafbaren Taten erfolgen. Niederländischen Hackern gelang es, in Computer der Hafenverwaltung im belgischen Antwerpen einzudringen und Zielorte bzw. Ankunftszeiten von Containern zu manipulieren. In die betroffenen Container wurden Drogen geladen, die dann von Drogenhändlern ohne Risiko von der Polizei ertappt zu werden in Empfang genommen wurden.[37]

---

[36] Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 5. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

[37] Interpol: Against Organized Crime. Interpol Trafficking and Counterfeiting Casebook 2014, S. 80. <http://www.interpol.int/Media/Files/Crime-areas/Trafficking-in-Illicit-Goods/Against-Organized-Crime-INTERPOL-Trafficking-and-Counterfeiting-Casebook-2014>.

Für Terrorgruppen ist der Cyber-Raum essentiell für ihre mediale Selbstdarstellung. Sie machen im Internet Werbung für den „heiligen Krieg", um Menschen für ihre Anliegen zu gewinnen, sei es als aktive Kämpfer, aber auch als Geldspender. Die mediale Aufbereitung ihrer Aktivitäten hat sich zu einem wichtigen Aspekt der Arbeit dieser Gruppen entwickelt. Auf YouTube, Twitter oder anderen Diensten wird Werbung in eigener Sache betrieben, indem die jeweiligen Ziele propagiert werden und die jeweilige Organisation als besonders effizient dargestellt wird. Es geht aber nicht nur um die Mobilisierung eines möglichen Zielpublikums, sondern auch um das kognitive Element in der Kampfführung. Bei ihren Operationen in Irak im Juni 2014 verbreitete der „Islamische Staat" (IS) auch im Cyber-Raum Angst und Schrecken, indem Bilder und Videos von Gräueltaten ins Netz gestellt wurden. Damit sollen die eigenen Kämpfer angestachelt, der Feind aber eingeschüchtert und demoralisiert werden. Die Nutzung des Internets geschieht auf eine sehr professionelle Weise. Dieses Potential wird auch auf der Gegenseite erkannt. So hat die irakische Regierung verschiedene Dienste gesperrt und die größten Internetprovider aufgefordert, in den vom IS kontrollierten Provinzen die Internetzugänge zu sperren.[38]

Terrororganisationen arbeiten oft mehrdimensional und bringen die Dimensionen ihres Handelns gezielt und abgestimmt zum Einsatz. Sie führen nicht bloß Operationen wie Bombenanschläge oder Entführungen durch, sondern betätigen sich auch auf sozialem Gebiet. Das trifft auf die Palästinenserorganisation Hamas zu, die von der EU und den USA als Terrororganisation eingestuft wurde.[39] Die „Internationale Humanitäre Hilfsorganisation" war ein deutscher Spendensammelverein für soziale Maßnahmen im Gaza-Streifen – entfaltete also selbst keine terroristische Aktivität. Aufgrund der Nähe zur Hamas wurde der Verein 2010 verboten (der gleichnamige österreichische Verein besteht nach wie vor). Zweck seiner Tätigkeit war es, der Hamas durch die sozialen Aktivitäten (die sie seit ihrer Gründung betreibt) eine entsprechende gesellschaftliche Verankerung in der palästinensischen Bevölkerung zu sichern und gleichzeitig einen größeren finanziellen Spielraum zu schaffen, der vermehrte terroristische Aktivitäten ermöglicht. Der hybride Charakter von Terrororganisationen war

---

[38] Kotrba, David: Terrorgruppe ISIS im Irak. Islamisten führen Dschihad im Internet. 18.06.2014. <http://futurezone.at/digital-life/terrorgruppe-isis-im-irak-islamisten-im-internet-dschihad/70.817.550>.

[39] Anmerkung: Der Europäische Gerichtshof wies die EU im Dezember 2014 an, die Hamas nicht mehr in der Liste der terroristischen Organisationen zu führen.

schon 2004 vom deutschen Bundesverwaltungsgericht implizit festgestellt worden, indem es die politischen, sozialen und terroristischen Aktivitäten der Hamas als untrennbar sah.[40]

Terrorismus ist umgekehrt ein Instrument, das auch von Staaten eingesetzt werden kann und so zum Bestandteil einer hybriden Bedrohung wird. Das zeigt ein Beispiel aus der deutschen Geschichte. Der Minister für Staatssicherheit der Deutschen Demokratischen Republik (DDR), Erich Mielke, erwog für den Fall eines deutsch-deutschen Konfliktes den Einsatz von Linksterroristen aus den Reihen der Roten Armee Fraktion im Rücken des Gegners. Es kam aber auch zur Unterstützung durch die DDR bei konkreten Aktionen. Ein Anschlag auf das französische Kulturzentrum in West-Berlin mit einem Toten wurde in Ost-Berlin durch einen Mann aus dem Umfeld des Terroristen Carlos vorbereitet.[41] Ein anderes Beispiel ist Libyens einstiger Staatschef Muammar al Gadaffi. Ihm werden zahlreiche Verwicklungen in terroristische Unternehmungen vorgeworfen. Der spektakulärste Fall war die Sprengung eines Passagierflugzeuges der U.S.-Gesellschaft PanAm über dem schottischen Lockerbie, bei dem 189 U.S.-Bürger und 43 Briten starben. Die genauen Hintergründe sind zwar bis heute ungeklärt, allerdings übernahm Libyen die Verantwortung für den Anschlag, der ehemalige libysche Justizminister bezichtigte Gaddafi, persönlich den Befehl für den Anschlag gegeben zu haben. Die ehemalige U.S.-Außenministerin Hillary Clinton wirft Gaddafi vor, hinter Attentatsplänen gegen den saudischen König gestanden zu sein. Unbestreitbar ist, dass 1984 aus der libyschen Botschaft in London auf Demonstranten gefeuert wurde, eine Polizistin starb.[42]

---

40 Bundesministerium des Innern: Pressemitteilung 12.07.2010, Bundesinnenminister Dr. de Maizière verbietet Hamas-Spendenverein. <http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/07/vereinsverbot.html>.

41 Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik: Ein „Faustpfand" des Mielke-Apparates. Die Staatssicherheit und die Rote Armee Fraktion (RAF). <http://www.bstu.bund.de/DE/Wissen/Aktenfunde/RAF/raf_node.html>.

42 Daniel Bates, Clinton: Gaddafi responsible for Lockerbie bombing. In: Scotsman Online, 11.06.2014. <http://www.scotsman.com/news/politics/top-stories/clinton-gaddafi-responsible-for-lockerbie-bombing-1-3439871>; Gaddafi ordered Lockerbie bombing. In: Aljazeera Online, 24.02.2011. <http://www.aljazeera.com/news/africa/2011/02/201122321354784554 6.html>.

Organisierte Kriminalität (OK) ist gleichfalls eine hybride Bedrohung. Es verschwimmen illegale mit legalen Geschäften, die Gesellschaft wird durch die kriminellen Aktivitäten beeinflusst, auch Medien können sich ihnen oftmals nicht entziehen. Die mögliche Dimension wird in der ESS knapp und prägnant genannt: „In Extremfällen kann das organisierte Verbrechen einen Staat beherrschen."[43] Es liegt in der Natur der OK, mehrdimensional in Erscheinung zu treten. Die Rechtswidrigkeit der verschiedenen Geschäftsfelder zwingt die Verbrecher, ein günstiges Umfeld für ihre „Geschäfte" schaffen zu müssen. Politiker und Beamten müssen durch Korruption oder Gewalt gefügig gemacht werden, um die Gesetzgebung und die Strafverfolgung entsprechend nachlässig zu betreiben, Medien dürfen möglichst wenig über die kriminellen Aktivitäten berichten. Die Strategie für die innere Sicherheit stellt hierzu fest: „Darüber hinaus untergräbt die Korruption das demokratische System und die Rechtsstaatlichkeit."[44] Zur Schaffung eines günstigen „Arbeitsumfeldes" treten die Bosse oft als Wohltäter in Erscheinung, erwerben sich ein Robin-Hood-Image und können so wieder selbst Gefälligkeiten verlangen.

Terrorismus und OK sind teilweise miteinander verbunden: „[...] bisweilen bestehen Verbindungen zu terroristischen Bewegungen."[45], heißt es in der ESS. Ein Beispiel ist die linksradikale Guerillaorganisation Farc (Fuerzas Armadas Revolucionarias de Colombia, Revolutionäre Streitkräfte Kolumbiens), die im Kokain-Geschäft tätig ist. Das Rauschgift war bislang ihre Haupteinnahmequelle mit ca. 4 Milliarden USD im Jahr. Ursprünglich kassierten die Guerilleros „Steuern", später wurden sie mit kriminellen Organisationen ohne politischen Hintergrund Teil des internationalen Drogenhandels.[46] Die Grenzen zwischen OK und Terrorismus sind fließend. Beide müssen im Verdeckten operieren und

---

43 Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 5. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

44 Generalsekretariat des Rates: Strategie für die innere Sicherheit der Europäischen Union: Auf dem Weg zu einem europäischen Sicherheitsmodell. Luxemburg 2010, S. 14. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313DEC.pdf>.

45 Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 4. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

46 Endres, Alexandra: Kolumbien. Die Farc geht auf Kokain-Entzug. Die Zeit Online, 17.05.2014. <http://www.zeit.de/politik/ausland/2014-05/farc-kolumbien-kokain>.

somit liegt es nahe, Synergien zu bilden. Die OK verfügt über Netzwerke im Waffenhandel oder für die Geldwäsche. Es werden aber auch Dienste wie Dokumentenfälschung von Terrorgruppen angenommen. Mit Methoden der OK können terroristische Aktivitäten finanziert werden. OK und terroristische Gruppen lernen voneinander und ergänzen einander zu wechselseitigem Nutzen. Ein Beispiel dafür ist die Finanzierung der Al-Shabaab-Milizen in Somalia durch illegalen Elfenbeinhandel. In Nordirland wiederum ist eine Geldquelle republikanisch gesinnter Paramilitärs der Schmuggel von Diesel aus der Republik Irland ins britische Nordirland.[47]

Dass OK eine hybride Bedrohung ist, spiegelt sich auch in der ESS:

> „Indem die EU auf dem Balkan auf die Wiederherstellung der verantwortungsvollen Staatsführung und die Förderung der Demokratie hinwirkt und die dortigen Behörden in die Lage versetzt, gegen die Organisierte Kriminalität vorzugehen, wird in wirksamster Weise zur Bekämpfung der Organisierten Kriminalität in der EU selbst beigetragen."[48]

Umgekehrt wird damit ausgesagt, dass schwache staatliche Strukturen im Interesse der OK liegen und diese zur Aufrechterhaltung eines solchen Zustandes nach Möglichkeit beitragen wird. Ihr hybrider Charakter findet sich auch in Definitionen von OK. Das deutsche Bundesinnenministerium schreibt auf seiner Homepage:

> „Voraussetzung (für das Vorliegen von OK; Anmerkung des Autors) ist, dass mehr als zwei Beteiligte unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen oder unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft auf längere oder unbestimmte Dauer arbeitsteilig zusammenwirken."[49]

---

47 Interpol: Against Organized Crime. Interpol Trafficking and Counterfeiting Casebook 2014, S.112ff. <http://www.interpol.int/Media/Files/Crime-areas/Trafficking-in-Illicit-Goods/Against-Organized-Crime-INTERPOL-Trafficking-and-Counterfeiting-Casebook-2014>.

48 Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 6. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

49 Bundesministerium des Innern: Sicherheit, Kriminalitätsbekämpfung, Organisierte Kriminalität. <http://www.bmi.bund.de/DE/Themen/Sicherheit/Kriminalitaets

Das Potential zur umfassenden Einflussnahme zeigen allein einige Zahlen. 2,1 Billionen USD sollen laut UNO die Geschäfte der OK weltweit ausmachen, alleine die italienische Mafia ist mit bis zu 180 Milliarden USD beteiligt. Das Landeskriminalamt Baden-Württemberg schätzt, dass die Kriminellen ungefähr die Hälfte ihrer Einnahmen in legale Geschäfte fließen lassen. Auf diese Weise gewinnen sie wirtschaftlichen und gesellschaftlichen Einfluss weit über die eigenen Kreise hinaus – eine Tatsache, die möglichst nicht auffallen soll.[50] In Deutschland ist das Ziel, unbemerkt aufzutreten, um nicht die Aufmerksamkeit der Strafverfolgungsbehörden auf sich zu ziehen. Morde werden nach Möglichkeit nicht hier begangen, sondern potentielle Opfer nach Italien gelockt. Auch Schutzgelderpressung kommt in Deutschland kaum vor. Die Deutschen sollen möglichst gar nicht merken, dass die italienische Mafia in ihrem Land äußerst aktiv ist. Das Geld fließt in Restaurants, Immobilien oder Baufirmen.[51]

Diese Vorgangsweise der OK muss erkannt werden, um die nötigen Gegenmaßnahmen, besonders in der Gesetzgebung, ergreifen zu können. Der Generalstaatsanwalt von Palermo wirft Deutschland vor, zu wenige gesetzliche Bestimmungen getroffen zu haben, um die OK effektiv bekämpfen zu können. Mafiosi investieren in Deutschland, weil sie im Unterschied zu Italien eine günstige Rechtslage vorfinden, so der Generalstaatsanwalt. So können in Italien bereits bei Verdacht auf einen mafiösen Hintergrund Vermögenswerte beschlagnahmt werden, in Deutschland ist das nicht möglich. Das Bewusstsein in Politik und Gesellschaft, einer Gefahr durch eine Organisation wie die Mafia ausgesetzt zu sein, ist in Deutschland wenig ausgeprägt. Nach einem spektakulären Mord an sechs Männern 2007 in Solingen stieg zwar die Aufmerksamkeit vorübergehend, hielt aber nur beschränkte Zeit an. Bis 2009 wurden 2,4 Millionen Euro beschlagnahmt, danach waren es in Summe nur mehr einige hunderttausend Euro.[52]

---

bekaempfung/Organisierte-Kriminalitaet/organisierte-kriminalitaet_node.html>.

50 Diehl, Jörg: Organisierte Kriminalität: Deutschland versagt im Kampf gegen die Mafia. In: Spiegel Online, 08.04.2014. <http://www.spiegel.de/panorama/justiz/mafia-in-deutschland-die-geschaefte-der-kriminellen-clans-a-963027.html>.

51 Schraven, David: Mafia in Deutschland. Geschäfte im Inland, Morde im Ausland. <http://www.mafia-in-deutschland.de/>.

52 Schraven, David: Der lachende Solinger. <http://www.mafia-in-deutschland.de/der-lachende-solinger/>.

Organisierte Kriminalität ist nicht unbedingt mit Geschäften verbunden, die unmittelbar gegen das Strafrecht verstoßen wie z.B. Drogenhandel. In Berlin traten Straßenhändler auf, die in Warteschlangen Stehenden Getränkedosen verkauften. Organisierte Gruppierungen übernahmen rasch diese illegale Form des Handels. Die Politikwissenschafterin Regine Schönenberg demonstrierte an diesem Beispiel, dass sich OK „Räumen" bemächtigt, die vom Staat nicht oder unzureichend kontrolliert werden. Die Forscherin gibt in dem Zusammenhang ein weiteres Beispiel: Arbeiter im Bereich der Produktfälschung in China. Nach dem World Trade Organization (WTO)-Beitritt Chinas mussten Chinas Behörden gegen diesen illegalen Produktionszweig vorgehen. Das Problem ist, wenn die in solchen Geschäftszweigen Beschäftigen nicht vom Staat in anderen Bereichen untergebracht werden können, bleiben sie den kriminellen Strukturen verhaftet.[53]

OK ist nicht auf nichtstaatliche Organisationen wie die Mafia beschränkt. Nordkorea hat eine lange Tradition von kriminellen Aktivitäten. 1976 wurden eine Reihe nordkoreanischer Diplomaten, darunter der Botschafter in Norwegen, ausgewiesen, weil sie in umfangreiche Schmuggelgeschäfte mit Alkoholika, Zigaretten und Haschisch verwickelt waren.[54] Im gleichen Jahr wurden andere Diplomaten aus Nordkorea in Ägypten mit 400 Kilo Haschisch erwischt. Offiziell wurden die Fälle als individuelle Fehlleistungen dargestellt, aber allein der Umstand, dass solche Leute nach Jahren noch immer Diplomaten waren, legt ein staatlich organisiertes System nahe.[55] Ab Mitte der 1990er-Jahre dürfte Nordkorea Drogen nur mehr produziert haben, der Verkauf wurde kriminellen Organisationen im Ausland überlassen.[56] Wenn auch durch die Abgeschlossenheit Nordkoreas sichere Informationen nur beschränkt zu gewinnen sind, war doch die Verwicklung von Nordkoreanern in den Drogenhandel so intensiv, dass Fachleute von staatlich organisiertem Drogenhandel ausgegangen sind. In den letzten Jahren dürfte sich die Rolle des Staates geändert haben, er scheint sich

---

53 Endres, Alexandra: Organisierte Kriminalität: „Die Politik ist verstrickt". In: Die Zeit Online, 19.06.2013. <http://www.zeit.de/wirtschaft/2013-06/organisierte-kriminalitaet-interview>.

54 Greitens, Sheena Chestnut: Illicit. North Korea's Evolving Operations to Earn Hard Currency. Committee for Human Rights in North Korea, Washington DC 2014, S. 16. <http://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf>.

55 Ebd., S. 16f.

56 Ebd., S. 18f.

aus dem Drogengeschäft zurückgezogen zu haben, was möglicherweise so zu interpretieren ist, dass er nur mehr Gelder von „privaten" Drogenhändlern entgegennimmt, die sich im Gegenzug auf staatlichen Schutz verlassen können.[57]

3.1.4 Hybride Bedrohungen: zukünftiger Analyse-Bedarf in Europa

Der Vielschichtigkeit hybrider Herausforderungen wird in der ESS Rechnung getragen, denn der „umfassende Sicherheitsansatz" – als Konzept zur Bewältigung solcher Herausforderungen – ist strategische Grundlage der EU für die Abwehr von Bedrohungen.

> „Jede dieser (neuen; Anmerkung des Autors) Bedrohungen erfordert eine Kombination von Instrumenten. [...] Zur Bekämpfung des Terrorismus kann eine Kombination aus Aufklärungsarbeit sowie polizeilichen, justiziellen, militärischen und sonstigen Mitteln erforderlich sein."[58]

Ein vollkommenes Aufbrechen der Trennung in innere Sicherheit, deren Schutz durch Justiz und Polizei erfolgt, und äußere Sicherheit, die durch das Militär sichergestellt wird, ist allerdings auch in den strategischen Grundlagedokumenten noch nicht erreicht. In der Strategie für innere Sicherheit sind die Streitkräfte praktisch nicht erwähnt; lediglich bei internationalen Krisenbewältigungsmissionen wird verlangt, dass für die innere Sicherheit zuständige Stellen „[...] mit allen anderen vor Ort beteiligten Diensten [...] (militärische, diplomatische, Notdienste)" zusammenarbeiten.[59] An anderer Stellte heißt es:

> „Eine Zusammenarbeit der Strafverfolgungs-, Grenz- und Justizbehörden sowie anderer Dienste – beispielsweise Einrichtungen des Gesundheits- und Sozialwesens und des Katastrophenschutzes – ist unerlässlich. Europas Strategie der inneren Sicherheit muss im Hinblick auf die Zusammenarbeit der Strafverfolgungsbehörden,

---

57 Ebd., S. 76ff.

58 Rat der Europäischen Union: Europäische Sicherheitsstrategie. Ein sicheres Europa in einer besseren Welt, S. 7. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568DEC.pdf.>.

59 Generalsekretariat des Rates: Strategie für die innere Sicherheit der Europäischen Union: Auf dem Weg zu einem europäischen Sicherheitsmodell. Luxemburg 2010, S. 30. <http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313DEC.pdf>.

das integrierte Grenzmanagement und die Strafjustiz die potenziellen Synergien nutzen, die in diesen Bereichen bestehen."[60]

Die Verwendung von Streitkräften ist hier nicht vorgesehen. Im Ernstfall wird nicht auf sie verzichtet werden können, man denke nur an natürliche und vom Menschen verursachte Katastrophen (die in der Strategie für innere Sicherheit unter die Bedrohungen gereiht werden) oder schwere Terrorangriffe. In Österreich war mit dem sicherheitspolizeilichen Assistenzeinsatz an der Ostgrenze zur Verhinderung illegaler Grenzübertritte auch die Notwendigkeit zu einem Militäreinsatz abseits eines nationalen Notstandes gegeben.

Allerdings ist für den „chirurgischen" Einsatz der Instrumente auch wichtig zu wissen, wie der Gegner denkt und handelt. Denn die Gegner der EU überlegen sehr genau, welche Maßnahmen innerhalb der EU gesetzt wurden oder noch gesetzt werden könnten, um diese rechtzeitig umgehen zu können. Nordkorea ist ein Beispiel für einen Staat, der große Geschicklichkeit entwickelt haben dürfte, Hindernisse für seine illegalen Geschäfte zu umgehen, indem höchst flexibel Produkte, Produktionsstätten, Transportwege, die Finanzinfrastruktur und die Stellung des Regimes den Erfordernissen angepasst werden. Es sollen „think tanks" eingerichtet worden sein, deren Aufgabe das Studium internationaler Sanktionen ist. Die dort tätigen Fachleute ersinnen Mittel und Wege zur Umgehung dieser Sanktionen, aber sollen auch künftige Maßnahmen im Vorhinein erkennen, um ihnen rechtzeitig ausweichen zu können.[61]

Umgekehrt wäre es für die EU und ihre Mitgliedstaaten wichtig, solche Drohpotentiale zu kennen und sie beim Namen zu nennen, um ein breites Bewusstsein für die Gefahr zu schaffen. Auf diese Weise wäre schon ein Schritt zur früh- und damit rechtzeitigen Bekämpfung getan. Wenn es Staaten betrifft, ist die Entscheidung über eine solche strategische Einschätzung politisch heikel und deswegen schwierig durch europäische Gremien zu bringen. Dass in Europa nicht in schablonenhaften Freund-Feind-Schemen gedacht wird, ist grundsätzlich positiv zu bewerten, weil die Orientierung an Kategorien von „Partnerschaft" Gemeinsamkeiten mit anderen Staaten in den Vordergrund stellt, anhand derer Differenzen überwunden werden können. Doch es wird sicherheitspolitische

---

60 Ebd., S. 8.

61 Greitens, Sheena Chestnut: Illicit. North Korea's Evolving Operations to Earn Hard Currency. Committee for Human Rights in North Korea, Washington DC 2014, S. 106. <http://www.hrnk.org/uploads/pdfs/SCG-FINAL-FINAL.pdf>.

Differenzen mit Akteuren – auch Staaten – geben, die nicht auf dem Verhandlungsweg (allein) beseitigt werden können. Solche Differenzen sollten im europäischen Rahmen offen angesprochen werden können.

Das sicherheitspolitische Denken hat sich in Europa insofern gewandelt, als vernetztes Denken als notwendig erkannt worden ist. Der „kohärente Einsatz unserer Instrumente“[62] wird im Überprüfungsbericht gefordert, aber auch der Gegner setzt seine Instrumente kohärent ein. Ein an hybriden Verfahrensweisen orientiertes Denken ist also nicht nur in Bezug auf die Abwehr von Gefahren wichtig, sondern auch bei der Erkennung von Gefahren. Die Gefahren können so genauer erfasst werden und Gegenmaßnahmen entsprechend getroffen werden. Dies wäre ein wichtiger Beitrag zu einem sicheren Europa, weil bereits frühzeitig auf bedrohliche Entwicklungen reagiert werden könnte und Herausforderungen bzw. Bedrohungen nicht zu komplexen Risiken für die europäische Sicherheit werden würden. Der Begriffsinhalt von „Umfassender Sicherheit“ könnte stärker an praktischen Bedürfnissen orientiert werden, weil auch die Bedrohungen entsprechend „umfassend“ definiert werden würden.

62 Ebd., S. 9.

3.2 Staatliche Unterstützung von Terrororganisationen als Möglichkeit hybrider Bedrohungsprojektion

Ramy Joussef

3.2.1 Einleitende Bemerkungen

Der Krieg sei, so Clausewitz, die Fortsetzung der Politik mit anderen Mitteln. Eine weit verbreitete Lesart interpretiert dieses Diktum so, dass damit eine zeitliche Sequenz gemeint sei, in welcher das Militär an die Stelle der Politik trete, nachdem alle politischen Möglichkeiten einer Konfliktlösung ausgeschlossen wurden. Selbst wenn diese Interpretation Clausewitz richtig wiedergeben würde, wäre sie (jedenfalls unter modernen Bedingungen) empirisch unzutreffend. In dem Maße nämlich, in dem sich ein politisches System nicht nur auf jenen Organisationenkomplex reduzieren lässt, den man klassischerweise als Staat bzw. als staatliche Verwaltung (inklusive Militär) bezeichnet, sondern auch politische Parteien, Gewerkschaften, NGOs, Protestbewegungen und eine im weitesten Sinne politisierte Öffentlichkeit umfasst[1], kann es seine Möglichkeiten steigern, weltpolitische Beziehungen zu anderen politischen Systemen auf unterschiedlichen formellen und informellen Kanälen und Ebenen gleichzeitig einzugehen und (mehr oder weniger konflikthaft) aufrechtzuerhalten. Darüber hinaus sind schon moderne staatliche Verwaltungen für sich genommen intern derart differenziert, dass sie über spezialisierte Teilorganisationen und professionelles Personal sowohl für Kriegführung als auch für Diplomatie verfügen, die weitgehend autonom voneinander operieren können, sodass stets gleichzeitig Krieg geführt und verhandelt werden kann. Eine empirisch zutreffendere (und wesentlich sparsamere) Lesart von Clausewitz könnte dann lauten, dass die Wahl einer bestimmten Strategie zur Beeinflussung eines politischen Systems sowie die Wahl der Mittel kriegerischer Gewaltanwendung immer von der zugrunde liegenden politischen und sozialen Struktur abhängt, in welcher die Kriegsparteien eingebettet sind, also der Kriegsverlauf wesentlich von (innen)politischen und

---

[1] Zur Binnendifferenzierung moderner politischer Systeme siehe Wimmer, Hannes: Die Modernisierung politischer Systeme: Staat, Parteien, Öffentlichkeit. Wien 2000.

gesellschaftlichen Gegebenheiten kodeterminiert wird. Mit dem Wandel dieser Rahmenbedingungen verändert sich nicht nur das Wesen des „Chamäleons" Krieg, sondern auch in einem umfassenderen Sinne die Möglichkeit, in weltpolitischen Beziehungen Bedrohungen zu projizieren. Diese müssen sich dann nicht allein auf militärische Kapazitäten stützen, sondern können gleichzeitig mehrere Ebenen und gesellschaftliche Sektoren miteinbeziehen und deren Leistungen in Anspruch nehmen um weltpolitische Interessen durchzusetzen.

Der Begriff der „hybriden Bedrohung", also die Kapazität, auf mehreren Dimensionen politische und gesellschaftliche Ressourcen zu bündeln und in einem zeitlich abgestimmten Zusammenhang für weltpolitische Ziele einzusetzen, versucht eben diese Phänomene zu erfassen. Die folgenden Überlegungen verstehen sich insofern als Beitrag, diesen Begriff am Beispiel des state-sponsored terrorism (SST) zu erproben. Sie gehen von der Frage aus, wie SST ermöglicht wird, und unter welchen Bedingungen SST im Kontext hybrider Bedrohung eingesetzt werden kann. Dabei wird eher die Perspektive des Sponsoring State (und nicht etwa des target state) eingenommen, da es vordringlicher erscheint, überhaupt erst das Phänomen SST adäquat zu beschreiben und zu verstehen. Zukünftigen Analysen bleibt es überlassen, Implikationen für die Abwehr konkreter Bedrohungsszenarien herauszuarbeiten. Der vorliegende Beitrag vertritt jedenfalls die Annahme, dass SST für einen Staat eine realisierbare Option darstellt, bei welcher mit verhältnismäßig geringen Ressourcen ein Bedrohungspotential aufgebaut werden kann. Gleichwohl hängt aber die Effektivität dieser Strategie vom Grad der Ausdifferenzierung des bedrohten politischen Systems ab, da dieses nicht nur über ein etabliertes Gewaltmonopol verfügen muss, sondern auch über eine politische Öffentlichkeit mit einer freien Berichterstattung, damit Terrorismus seine Wirkung entfalten kann. Darüber hinaus wird vermutet, dass Terrororganisationen nicht in einen anderen Staat implantiert werden können, sondern erst aus Protestbewegungen heraus entstehen müssen, und dieser Prozess nicht von einem Sponsoring State gesteuert werden kann. Diese Vermutungen gilt es nun in mehreren Abschnitten weiterzuentwickeln. Dabei soll der Begriff der hybriden Bedrohung in einem breiteren Kontext der wissenschaftlichen Auseinandersetzung mit Weltpolitik verortet werden (Kapitel 3.2.2), woraufhin Bedingungen der Möglichkeit der Ausdifferenzierung von Terrorismus diskutiert werden sollen (Kapitel 3.2.3). Schließlich soll die besondere Form des SST hinsichtlich seines Bedrohungspotenzials erörtert werden (Kapitel 3.2.4) um die Ergebnisse in einer abschließenden Conclusio zusammenzutragen (Kapitel 3.2.5).

3.2.2 Analytic frame

Ein Blick in die Theoriegeschichte der akademischen Disziplin der Internationalen Beziehungen (IB) verrät, dass die großen Paradigmen von den politischen Konstellationen ihrer Entstehungszeit immer mitgeprägt waren. Vom Ende des Zweiten Weltkrieges bis in die frühen 1990er Jahre hinein wurden Theorien der IB weitgehend von (neo)realistischen Ansätzen geprägt, die Staaten und deren Beziehungen als den ausschließlichen Analysegegenstand betrachteten. Dabei wurde die Staatenwelt bzw. das internationale System als anarchische Struktur betrachtet, die in funktional gleichartige Entitäten (Staaten) dekomponiert gedacht wurde, die sich lediglich hinsichtlich ihrer militärischen Kapazitäten unterschieden. Die Kategorie der Macht wurde in diesem Sinne überwiegend mit militärischer Über- bzw. Unterlegenheit gleichgesetzt. Die dadurch entstehenden Machtasymmetrien in den zwischenstaatlichen Beziehungen würden zur Entstehung von Allianzen führen, die das Ziel hätten, durch Akkordierung und Bündelung von militärischen Machtressourcen politische Ungleichgewichte zu vermeiden und eine balance of power herzustellen.[2] Dieser Theoriestrang mag lange Zeit eine gewisse Berechtigung und empirische Stichhaltigkeit gehabt haben, doch mit dem Ende des Kalten Krieges (und der Unfähigkeit realistischer Theorien dieses vorherzusehen) fand sowohl in der Theoriebildung als auch in der Praxis ein Paradigmenwechsel statt, sodass parallel zum Aufkommen neuer, liberaler und konstruktivistischer Theorien auch ein grundlegender Wechsel des staatlichen policy-making zu beobachten ist. Im Vordergrund stehen seither nicht mehr geopolitische Konkurrenz und die Verteilung von militärischen Ressourcen zur notfalls gewaltsamen Durchsetzung staatlicher Interessen. Staatliche Macht wird auch nicht mehr hauptsächlich über die Verfügbarkeit von Waffentechnologien definiert, sondern auch über ‚weiche' Formen der Durchsetzung von Interessen (soft power)[3]. Neue Formen der Kooperation, insbesondere im Rahmen inter- und supranationaler Organisationen, gewinnen an Bedeutung. Die klassische hierarchische Tätigkeit des bürokratischen Regierens (government) wird durch die neue Praxis solcher Kooperationsformen, die unter dem Schlagwort ‚(global) governance' firmie-

---

2 Vgl. Waltz, Kenneth: Theory of International Politics. Reading et al. 1979.

3 Siehe Nye, Joseph S.: Soft Power. The Means to Success in World Politics. New York 2004.

ren, zwar nicht ersetzt, aber ergänzt. Auch auf substaatlicher Ebene wird das Erscheinen neuer, privater Akteure und das Aufkommen von public-private partnerships erkannt und analysiert. Auf zwischenstaatlicher Ebene ist seit dem Ende des Zweiten Weltkrieges im Zuge der Dekolonisation und des Zusammenbruchs von Entitäten wie der Union der Sozialistischen Sowjetrepubliken (UdSSR) die Entstehung vieler neuer Staaten zu verzeichnen.

Man sieht also insgesamt das Auftreten einer Vielzahl neuer Akteure in der Weltpolitik, die auch grenzüberschreitend agieren und viel leichter wechselseitig in Beziehung treten können, als dies zuvor der Fall war. Nicht zuletzt die Verbreitung neuer Kommunikationsmedien, wie Satellitenfernsehen und Internet erleichtern solche Prozesse, die zur Bildung transnationaler Netzwerke beitragen, in denen alle beteiligten Akteure, seien es Staaten, NGOs, Protestbewegungen, Medien etc. wechselseitig füreinander relevant werden können. Mit der Zunahme der Anzahl relevanter politischer Akteure geht zugleich ein exponentielles Wachstum der sozialen Komplexität einher, die sich mit einer einfachen mathematischen Formel auf den Punkt bringen lässt: Geht man z.B. davon aus, dass bei einer Anzahl von 193 Staaten jeder Staat mit allen anderen Staaten eine Beziehung unterhält, so kann man die Summe der dadurch entstehenden Beziehungen, d.h. die Komplexität c, gemäß der Formel $c= (n^2-n)/2$ errechnen und feststellen, dass in der Staatenwelt 18.528 (mehr oder weniger konfliktanfällige) Beziehungen jederzeit virulent werden können. Komplexitätstheorien haben für solche Fälle das Adjektiv ‚noncomputational' geprägt – eine Systemkomplexität also, die nicht mehr computerunterstützt simuliert werden kann, geschweige denn, dass Prognosen möglich wären. Nun sind Staaten mittlerweile nicht nur wechselseitig miteinander konfrontiert, sondern können auch indirekt Beziehungen zueinander unterhalten, sei es über inter- bzw. supranationale Organisationen oder substaatliche, private Akteure, die für weitere Komplexität in den internationalen Beziehungen sorgen.

Im sicherheitspolitischen Bereich folgt daraus einerseits verstärkte Kooperation durch Allianzen und Verteidigungsbündnisse, sowie militärische Zusammenarbeit in primär nicht-militärischen Organisationen (man denke etwa an battle-groups im Rahmen der Europäischen Sicherheits und Verteidigungspolitik ESVP). Andererseits werden aber auch sub-staatliche, private Gewaltakteure (private Sicherheitsfirmen, Söldnerheere, Terrororganisationen etc.) maßgeblich, mit denen Staaten zur Erreichung bestimm-

ter policy-Ziele kooperieren können. Komplexität in den internationalen Beziehungen ist daher gleichbedeutend mit einer unüberschaubaren Vielfalt an Handlungsoptionen, die einzelnen Akteuren zur Verfügung stehen. Es gibt nicht mehr die klassische Dichotomie Krieg/Diplomatie – falls es diese jemals gab. Vielmehr bieten die Erschließung neuer Räume (und damit: Gefechtsfelder) wie Weltraum und Cyberspace, sowie die Verflechtung staatlicher und privater Akteure neue Möglichkeiten der Interessensdurchsetzung. Man spricht in diesem Zusammenhang mithin nicht mehr nur von Hard/Soft Power, sondern auch von Hybrid Power, also dem akkordierten Einsatz unterschiedlichster militärischer und nicht-militärischer Mittel zur politischen Willensdurchsetzung. Die daraus resultierenden Bedrohungsszenarien in transnationalen Konflikten sind daher auch komplexer, um nicht zu sagen: unvorhersehbar geworden.[4]

Was bedeutet das aber für wissenschaftliche Analysen im Rahmen des IKKM? Man könnte dazu übergehen zu behaupten, dass Prognosen angesichts von Hybridität und Komplexität künftiger Bedrohungsbilder nichts weiter seien als sinnlose Spekulationen, deren Bewahrheitung reiner Zufall sei. Von diesem Standpunkt aus betrachtet würde allerdings jede Antizipation von Bedrohungen sinnlos sein – schließlich liegt es im Wesen von Bedrohungen, dass sie immer auf eine unbekannte Zukunft gerichtet sind.[5] Allerdings befreit das die Politik nicht von der Last, in der Gegenwart Entscheidungen treffen zu müssen, die eben jene Zukunft mitbestimmen. Der Beitrag, den wissenschaftliche Analysen dazu leisten könnten, müsste dann Hybridität und Komplexität selbst ins Zentrum des Forschungsinteresses rücken und darstellen, wie politische Entscheidungsträger angesichts dieser Vielzahl unterschiedlich miteinander verknüpfbarer Machtinstrumente Strategien entwickeln und welche Voraussetzungen erfüllt sein müssen um überhaupt bestimmte Handlungsoptionen sinnvoll einsetzen zu können.

Im Folgenden soll also nun versucht werden, SST als eine mögliche Option von Staaten im Rahmen internationaler Konflikte dahingehend zu untersuchen, ob und unter welchen Bedingungen sie als Element eines hybriden

---

4 Vgl. Wallace, Ian: The Difficulties in Predicting Future Warfare. In: Australian Defence Force Journal, 183/2010, S. 27ff.

5 Vgl. Schirmer, Werner: Bedrohungskommunikation. Eine gesellschaftstheoretische Studie zu Sicherheit und Unsicherheit. Wiesbaden 2008, S. 104f.

Bedrohungsbildes in Frage kommt. Dazu gilt es zunächst, Entstehungsbedingungen von Terrorismus zu diskutieren um daraufhin Möglichkeiten und Probleme der staatlichen Unterstützung von Terrorismus herausarbeiten zu können.

3.2.3 Terrorismus und Protest: Zur Emergenz von Terrororganisationen

Terrorismus im Zusammenhang mit politischen Protestbewegungen zu diskutieren ist in der einschlägigen Literatur keineswegs selbstverständlich.[6] Allerdings gibt es mehrere gute Gründe zumindest kursorisch auf politische Protestbewegungen einzugehen, bevor eine eingehendere Beschreibung des Phänomens Terrorismus erfolgen soll: Zunächst kann man mit Peter Waldmann davon ausgehen, dass „[e]in nur flüchtiger Blick auf terroristische Kampagnen genügt, um auf ihren engen zeitlichen Zusammenhang mit breit angelegten politischen Protestbewegungen aufmerksam zu werden“[7]. Diese empirisch feststellbare Korrelation zwischen dem Auftreten von Protestbewegungen und Terrorismus kann nicht ignoriert werden. Zugleich soll aber davor gewarnt werden, diese Korrelation in ein zwangsläufig unterkomplexes Kausalschema der Sorte „Wenn-dann“ zu pressen. Stattdessen soll versucht werden, eine Möglichkeit aufzuzeigen, mit der man das Auftreten terroristischer Kampagnen als Emergenzphänomen von Protestbewegungen beschreiben und erklären kann. Ein weiterer Grund für die Berücksichtigung von Protestbewegungen liegt in bestimmten Gemeinsamkeiten hinsichtlich der Operationsweise von Protestbewegungen und terroristischen Bewegungen: beide versuchen die politische Öffentlichkeit für bestimmte Anliegen zu mobilisieren, beide sind in dieser Hinsicht in besonderer Weise von Möglichkeiten moderner Massenmedien abhängig und versuchen durch unkonventionelle Kommunikation deren Aufmerksamkeit zu erregen. Auch hinsichtlich ihrer internen Strukturen, die sich keinesfalls auf Organisationen beschränken lassen, sondern eher Netzwerkcharakter annehmen, gibt es signifikante Ähnlichkeiten.[8] Die weit gediehe-

---

6 Vgl. Gunning, Jeroen: Social Movement Theory and the Study of Terrorism. In: Jackson, Richard/Breen Smyth, Marie/Gunning, Jeroen (Hrsg.): Critical Terrorism Studies: A New Research Agenda. London/New York 2009, S. 156ff, hier S. 156f.

7 Waldmann, Peter: Terrorismus. Provokation der Macht. Hamburg 2005, S. 160.

8 Vgl. ebd., S. 161f. Siehe auch Ibrahim-Kudelich, Kardalan: Transnationaler Terroris-

ne Forschungsarbeit, die bisher für die Beschreibung von sozialen Bewegungen bzw. Protestbewegungen geleistet wurde, könnte daher mit Sicherheit interessante Einsichten in die Operationsweise des Terrorismus liefern und der Terrorismusforschung wesentliche Impulse geben. Darüber hinaus lassen sich Phänomene terroristischer Gewalt, die meistens sehr isoliert von der gesellschaftlichen Umwelt betrachtet werden, durch Bezugnahme auf die jeweiligen Protestbewegungen leichter in einen gesellschaftlichen Kontext einbetten.

Terrorismus ist also, so die hier vertretene Hypothese, ein soziales Phänomen, das entstehen kann, wenn es politische Themen gibt, die zum Anlass von Konflikten und breiteren Protestbewegungen werden, im Zuge derer es zu einer Radikalisierung und zur Abspaltung extremistischer Splittergruppen kommt, denn:

> „None of the known terrorist groups started its career by the application of terrorism. Most modern terrorists had reached their terrorism gradually. They had been radicalized into it. [...] Sometimes the history of the radicalization is longer and goes back to older roots of anti-regime struggles and rebelliousness [...]. But whatever the radical past is, it is lesser in intensity and brutality than terrorism and moves to terrorism by gradual evolution."[9]

Terrorismus lässt sich allerdings nicht *als Protest* auffassen. „Das, was dem gewaltsamen Ausarten von ‚Demonstrationen oder spektakulären Aktionen zivilen Ungehorsams' eine klare Grenze zieht: die Bewahrung eines positiven öffentlichen Images, scheint beim Terrorismus außer Kraft gesetzt"[10], so Ibrahim-Kudelich. Das Auftreten von Gewalt delegitimiert Protest und ist eher eine unerwünschte Begleiterscheinung als eine Strategie der demokratischen Durchsetzung von politischen Anliegen. Dem Protest geht es

---

mus als periphere Organisation des politischen Systems? - Zur systemtheoretischen Beobachtbarkeit von Terrorismus. In: Kron, Thomas/Reddig, Melanie (Hrsg.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven. Wiesbaden 2007, S. 194ff, hier S. 200ff.

9 Sprinzak, Ehud: The Process of Delegitimation: Towards a Linkage Theory of Political Terrorism. In: Terrorism and Political Violence, 3(1) 1991, S. 50ff, hier S. 51.

10 Ibrahim-Kudelich, Kardalan: Transnationaler Terrorismus als periphere Organisation des politischen Systems? - Zur systemtheoretischen Beobachtbarkeit von Terrorismus. In: Kron, Thomas/Reddig, Melanie (Hrsg.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven. Wiesbaden 2007, S. 194ff, hier S. 203.

um die Aufforderung zur Änderung kollektiv verbindlicher Entscheidungen die durch Aufbau von Drohmacht durch Mobilisierung von Massen herbeigeführt werden soll. Protestbewegungen bedienen sich gegenüber dem Staat des Politik-typischen Kommunikationsmediums der Macht[11], weil sie es sich erlauben können – sofern sie ein entsprechendes Aufgebot an Individuen und Organisationen mobilisieren können. Terrorismus hingegen ist keine Machtkommunikation sondern vielmehr eine Ohnmachtskommunikation:

> „Zu ihm greift, wer andere Chancen der Einflussausübung nicht hat oder nicht sieht [...]. Das gilt auch und gerade dann, wenn der terroristische Akt gleichzeitig versucht, den Spieß umzudrehen und einem Staat, einer Polizei, einer Bevölkerung ihre Ohnmacht im Umgang mit dieser Gewalt vorzuführen versucht."[12]

Der Einsatz von Gewalt bedeutet das Scheitern jeder Machtkommunikation – politische Macht äußert sich eben darin, auf Gewalt verzichten zu können. Dem Terrorismus bleibt nichts anderes übrig als die „Provokation der Macht", die er dadurch erzielt, dass er

> „punktgenau an einer Ermöglichungsbedingung des Politischen schlechthin ansetzt, am Gewaltmonopol. In gewisser Weise parasitiert er an dieser Bedingung, und das heißt auch, daß er selbst alles andere als politisch ist, wie sehr ihn Politik auch als politisch motiviert thematisieren kann. Es geht ihm nicht um kollektiv bindende Entscheidungen. Er steht irgendwie - daneben."[13]

Proteste gehen also nicht im Terrorismus auf, sondern bleiben weiterhin bestehen oder flauen ab, ohne dass dies dem Terrorismus einen Abbruch tun muss. Insofern ist Terrorismus kein ‚Nebenschauplatz' des Protests, in dem neben den grundsätzlich gewaltfreien Formen der Protestkommunikation gleichermaßen gewalttätig kommuniziert wird um eine Änderung politischer Entscheidungen herbeizuführen, sondern ist ein Konflikt mit einer eigenen Geschichte und einer Eigenlogik, die durch die wechselseitige Anwendung von Gewalt bestimmt wird.

---

11 Vgl. Luhmann, Niklas: Macht. Stuttgart 2000.

12 Baecker, Dirk: Die Gewalt des Terrorismus. In: Aderhold, Jens/Kranz, Olaf (Hrsg.): Intention und Funktion. Probleme der Vermittlung psychischer und sozialer Systeme. Wiesbaden 2007, S. 219ff, hier S. 221.

13 Fuchs, Peter: Das System "Terror". Versuch über eine kommunikative Eskalation der Moderne. Bielefeld 2004, S. 42.

Allerdings kann sich Terrorismus nicht nur ‚zivilisieren', indem er sich durch Deeskalation und Integration wieder dem Zentrum des politischen Systems annähert, sondern kann sich auch von der Politik ablösen. Dies geschieht dann, wenn sich in einem politischen Konflikt bzw. einer Protestbewegung Terroristen abspalten und sich als eigenständige Akteure etablieren. Sobald nämlich dieser Prozess weitgehend abgeschlossen ist – erst dann kann man im eigentlichen Sinne von ‚Terrorismus' sprechen - tritt eine Eigendynamik in Kraft: es geht dann nicht mehr um politisches Entscheiden, um Machtüberlegenheit/Machtunterlegenheit, sondern nur noch um die Differenz Freund/Feind und um die Nullsummenlogik gewaltsamer Anschläge und Gegenschläge, die dazu führt, dass das ursprüngliche Protestthema an Bedeutung verliert und ganz andere Probleme an Bedeutung gewinnen. Man kann dabei insbesondere an die Folgen des ‚Selbsterhaltungstriebes' von Terroristen denken, die, wenn sie bereits in den Untergrund abgetaucht sind, abgesehen von kriminellen Aktivitäten oft nichts anderes mehr tun können, als Anschläge zu verüben, ebenso wie ein Staat einen Anschlag - und damit die Unterminierung des Gewaltmonopols - nicht ungesühnt lassen kann und die Verantwortlichen zur Rechenschaft ziehen muss.

Man kann also beobachten, dass, wenn man Terrorismus als Konfliktsystem begreift, auch der Staat ins Blickfeld rückt, dessen counter-terroristische Maßnahmen ebenso maßgeblich an der Reproduktion von Terrorismus beteiligt sind, wie terroristische Anschläge. Erst durch die Existenz eines Staates macht eine Strategie des Terrorismus Sinn:

> „[T]he 'weapons of the weak' are forceful only when they are backed by *the strength of the other*, which is in most cases a state. Terrorism, because of its lack of resources and its unconventional ways of fighting, is in fact characterized by *a triply indirect instrumentality*. It is *the overreaction of the other (the enemy state)* which is crucial in terrorism. It is that over reaction which is able to produce sympathy for the terrorists' cause by third parties such as populations hostile to the attacked and overreacting state, and other states."[14]

Wenn dies zutrifft, müsste man Terrorismus vielmehr als Zusammenspiel zwischen Staat und Terroristen beschreiben, und nicht als eine Aneinanderreihung von terroristischen Anschlägen. Das bedeutet keineswegs, dass der

---

[14] Schinkel, Willem: Aspects of Violence. A Critical Theory. Basingstoke 2010, S. 146 (Hervorhebungen im Original).

Staat selbst als Terrororganisation tätig werden muss, es sich also um eine Verbindung zwischen Staatsterrorismus und ‚privatem' Terrorismus handelt, sondern dass in einem Konflikt eben immer beide Seiten berücksichtigt werden müssen um ihn verstehen zu können. Das ändert auch nichts daran, dass nach wie vor das einzig wirksame Mittel gegen Terroristen das staatliche Gewaltmonopol ist. Mit dieser Beobachtung wird aber auch eine perverse Paradoxie sichtbar: Dass zwar nur das staatliche Gewaltmonopol dem Terrorismus Einhalt gebieten kann, aber Terrorismus eben nur in Gebieten mit etablierter Staatlichkeit Sinn ergibt, da deren Anschläge genau auf das Gewaltmonopol moderner Staaten abzielen. Der moderne Staat ist also für terroristische Anschläge Verhinderungs- und Entstehungsbedingung zugleich.

3.2.4 State-sponsored terrorism als strategische Option hybrider Bedrohung

Terrorismus wird häufig als eine Form der Kriegsführung beschrieben und im Kontext ‚kleiner', ‚neuer' bzw. ‚asymmetrischer Kriege' diskutiert.[15] Es handelt sich dabei um eine Abgrenzung zum Konzept ‚großer', zwischenstaatlicher Konflikte, in welchen reguläre Armeen einander unter der Achtung völkerrechtlicher Regeln bekämpfen. Mit dem Wandel politischer Rahmenbedingungen, d.h. der unvollständigen Verbreitung von Staatlichkeit und dem Auftreten neuer nicht-staatlicher Gewaltakteure unter Bedingungen globaler kommunikativer Erreichbarkeit in der Weltgesellschaft, verändere sich zugleich auch das Wesen der Kriegführung. Das Aufkommen terroristischer Strategien wird also im Zusammenhang mit der Auflösung der westfälischen Staatenordnung und dem Verlust ihrer kriegseinhegenden Funktion analysiert. Der ‚neue' asymmetrische Krieg löse somit den symmetrischen Staatenkrieg ab und würde zur dominierenden Form gewalttätiger Konfliktaustragung[16]. Allerdings stellt sich dann die Frage, ob es dann nicht zu einer Verwässerung des Kriegsbegriffes kommt, wenn man mit ihm nicht nur den Zweiten Weltkrieg, sondern ebenso terroristische

---

15 Vgl. Münkler, Herfried: Der Wandel des Krieges. Von der Symmetrie zur Asymmetrie. Weilerswist 2006, S. 221ff.

16 Vgl. Kaldor, Mary: New and Old Wars: Organised Violence in a Global Era. Cambridge, Malden 2012.

Kampagnen wie diejenigen der RAF beschreiben möchte. Darüber hinaus ist Terrorismus insofern nicht mit Krieg vergleichbar, als Anschläge ja selten gegen reguläre staatliche Armeen gerichtet sind sondern eben gegen ‚weiche' Ziele. Das schließt zwar nicht aus, dass Terroranschläge dann von Staaten als kriegerischer Angriff geframed werden können, auf den dann militärisch reagiert wird – allerdings sind dann Schlagworte wie ‚war on terrorism' eher als Semantiken in politischen Diskursen zu betrachten und nicht als wissenschaftlich verbindliche Beschreibungen eines Konfliktsystems.

Terroristische Strategien können gleichwohl auch in zwischenstaatlichen Konflikten bedeutsam werden: SST stellt einen Sonderfall eines bewaffneten Konflikts dar, weil sich hier nicht nur ein Staat und eine oder mehrere Terrororganisationen gegenüberstehen, sondern ein weiterer Staat als Konfliktpartei beteiligt ist. Dabei handelt es sich um Überlappungen zweier verschiedener Konflikte: eines Konflikts zwischen einem Staat und einer Terrorbewegung, und eines zwischenstaatlichen Konflikts, in welchem ein Staat eine Terrororganisationen gegen einen verfeindeten Staat zu instrumentalisieren versucht. SST kann dann ein Mittel in einer Strategie der zwischenstaatlichen Konfrontation sein, in welcher „der Einsatz von Streitkräften nicht unmittelbar das feindliche Machtpotential schwächt, sondern mittelbar, d.h. durch die Androhung, Demonstration etc. von Gewalt, den Gegner zur Erfüllung des fremden Willens zwingt."[17] Es handelt sich also insofern um eine Möglichkeit hybrider Bedrohung, als ein Staat versucht nicht nur durch eigene militärische Drohpotentiale Interessen durchzusetzen, sondern zielgerichtet und gleichzeitig sowohl auf politischer Ebene als auch durch nicht-kriegerische Gewaltanwendung eines „proxy" eine Drohkulisse zu projizieren um dadurch seine Interessen gegenüber einem anderen Staat durchzusetzen. Diese Möglichkeit soll nun auf ihre praktischen Bedingungen hin befragt werden, um zu einer genaueren Einschätzung dieses Bedrohungspotentials zu gelangen.

Wie weit Kooperationen zwischen Staaten und Terrororganisationen verbreitet sind, lässt sich schwer sagen. Allerdings lässt sich statistisch feststellen, dass in zwischenstaatlichen Konflikten die Anzahl terroristischer An-

---

[17] Gustenau, Gustav E.: Zum Begriff des bewaffneten Konfliktes. In: Österreichische Militärische Zeitschrift, Heft 1/1992, S. 45ff, hier S. 50.

schläge signifikant höher ist und zumindest begründbare Vermutungen über die staatliche Unterstützung von Terrororganisationen nicht abwegig sind.[18] Die Formen der Unterstützung reichen dabei von Training und Ausbildung, über die Zurverfügungstellung von Geld und Waffen bis hin zur logistischen Unterstützung, etwa durch die Ausstellung von Reisepässen. Am wichtigsten ist allerdings die Bereitstellung eines territorialen Rückzugsgebiets für Terroristen.[19] Terrororganisationen operieren im Regelfall unter Bedingungen der Klandestinität, die ihre Operationsweise zwar einerseits erst ermöglicht, andererseits aber auch stark einschränkt. Der Wegfall solcher Hindernisse würde es ihnen ermöglichen, personell zu wachsen und damit höhere Eigenkomplexität aufzubauen um daraufhin zumindest potentiell wesentlich anspruchsvollere Operationen durchführen zu können.

Was aber ausgeschlossen werden kann ist, dass Terrororganisationen von einem Sponsoring State künstlich ‚erzeugt' werden können um diese dann im politischen System eines verfeindeten Target State zu ‚implantieren'. Dazu ist die Emergenz von Terrororganisationen und einer terroristischen Strategie an zu viele Voraussetzungen gebunden, die hier bereits beschrieben wurden. Staaten unterstützen daher eher bereits vorhandene Protest- bzw. Terrorbewegungen um einen anderen (meistens benachbarten) Staat politisch unter Druck zu setzen.[20] Es handelt sich dabei also nicht um eine kriegerische Auseinandersetzung, sondern vielmehr um ein Druckmittel, welches in zwischenstaatlichen Beziehungen als Taktik im Rahmen einer *coercive diplomacy* eingesetzt wird. Dabei kommt es zwar zur Gewaltausübung durch einen terroristischen „proxy", aber die direkte militärische Konfrontation wird durch Austragung eines Stellvertreterkonflikts vermieden.[21] Terrorismus kann dann ein vergleichsweise effizientes Instrument zur Ausübung von politischem Druck sein, da er kaum Kosten verursacht und

---

18 Vgl. Conrad, Justin: Interstate Rivalry and Terrorism: An Unprobed Link. In: Journal of Conflict Resolution, 55(4) 2011, S. 529ff.

19 Vgl. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, S. 59ff.

20 Vgl. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, S. 37f.

21 vgl. Gal-Or, Noemi: State-Sponsored Terrorism: A Mode of Diplomacy? In: Conflict Quarterly, 13(3) 1993, S. 7ff.

keine besonders raffinierten Technologien benötigt. Das kann insbesondere für solche Staaten interessant sein, die über relativ geringe militärische Kapazitäten verfügen und durch solche Formen des SST Bedrohung weit über den eigenen territorial definierten Einflussraum hinaus projizieren können.[22] Die geheime Unterstützung von Terrororganisationen verschafft Staaten schließlich auch eine *plausible deniability*[23], nämlich die Möglichkeit einerseits Druck auf den target state auszuüben, aber gleichzeitig auf dem diplomatischen Parkett jede Kooperation abstreiten zu können. Man bleibt für diplomatische Kommunikation ansprechbar und kann diese wiederum einsetzen um Interessen gegenüber dem target state durchzusetzen. Bei SST bilden somit Diplomatie und Terrorismus die wichtigsten Komponenten einer Strategie hybrider Bedrohung und Machtprojektion, was die jederzeit mögliche Anwendung militärischer Gewalt aber nicht ausschließt.

Gegen eine solche Strategie würde sprechen, dass Terrororganisationen nur in geringem Ausmaß von staatlicher Unterstützung abhängig sind: ihre Bewaffnung hält sich zumeist in quantitativen und qualitativen Grenzen und geht selten über konventionelle small arms hinaus, die auch auf dem Schwarzmarkt beschafft werden können.[24] Finanzielle Mittel können über kriminelle Aktivitäten[25] und Sympathisantennetzwerke lukriert werden[26] und auch die Ausbildung kann durch Terrororganisationen selbst gewährleistet werden, da hier das notwendige operative know-how kaum über die Anleitung zur Herstellung von Bomben hinausgeht, die auch von einzelnen ‚Privatpersonen' gebaut werden können. So voraussetzungsreich Terrorismus auf der strategischen Ebene ist, so simpel funktioniert er auf der operativen Ebene:

---

22 Vgl. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, S. 38.

23 Vgl. Byman, Daniel/Kreps, Sarah E.: Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, S. 1ff, hier S. 9.

24 Vgl. Schroeder, Matthew: Small Arms, Terrorism and the OAS Firearms Convention. Federation of American Scientists, Occasional Paper No.1, März 2004, S.ff.

25 Siehe Hutchinson, Steven/O'Malley, Pat: A Crime–Terror Nexus? Thinking on Some of the Links between Terrorism and Criminality. In: Studies in Conflict & Terrorism, 30(12) 2007, S. 1095ff.

26 Vgl. Waldmann, Peter: Terrorismus. Provokation der Macht. Hamburg 2005, S. 71ff.

> „Since terrorism is a technique - basically boiling down to killing civilians to influence (impress, provoke, shock, coerce, harm) relevant third parties - it can be used by many different 'players'. All you need is plenty of explosives and no scruples and the conviction that terrorism 'works'."[27]

Darüber hinaus ergeben sich häufig auch Probleme in der Beziehung zwischen Sponsoring State und Terrororganisation, die etwa daraus resultieren können, dass Terrororganisationen ihre Strategien ändern, ohne auf die Interessen ihres Sponsoring State Rücksicht nehmen zu müssen:

Wichtige Mechanismen der internen Anpassung von Terrororganisationen stellen insbesondere ihre Strategien dar, die auch als Zweckprogramme betrachtet werden können, und auf eine stets ungewisse Zukunft gerichtet sind.[28] Diese Zweckprogramme sind aber auch adaptierbar. Es kommt dann häufig zu Zweck/Mittel-Verschiebungen,

> „die Zwecke so stark [...] generalisieren, dass das Erreichen des Zweckes jeden Bezug zu Zeitpunkten verliert und weder positiv noch als Unerreichbarkeit negativ festgestellt werden kann. Zwecke konfundieren dann mit den Werten, die zur Begründung der angestrebten Differenz dienen"[29].

Man sieht dann ein, dass der Zweck, die Niederwerfung des Feindes, zeitlich unbestimmbar wird und konzentriert sich auf die Mittel. Damit wäre die häufige Transformation von Terrororganisationen in kriminelle Geldbeschaffungsorganisationen beschrieben.[30] Auch die steigende Volatilität bei der Auswahl von Terrorzielen kann als Umprogrammierung von Zweckprogrammen gesehen werden. So ist es möglich, dass für eine Terrororganisation wie al-Qaida im Verlauf der Zeit die USA, Israel, arabische Staaten und sogar irakische Schiiten als mögliche Ziele in Betracht kommen können.[31] Strategieänderungen in Terrororganisationen sind darüber hinaus auch stark von internen sozialen Dynamiken geprägt und nicht immer mit

---

27 Schmid, Alex P.: The Routledge Handbook of Terrorism Research. New York 2011, S. 18.

28 Luhmann, Niklas: Organisation und Entscheidung. Opladen 2000, S. 266.

29 Ebd., S. 270.

30 Siehe Dishman, Chris: Terrorism, Crime, and Transformation. In: Studies in Conflict & Terrorism. 24(1) 2001, S. 43ff.

31 Vgl. Schneider, Wolfgang Ludwig: Religio-politischer Terrorismus als Parasit. In: Kron, Thomas/Reddig, Melanie (Hrsg.): Analysen des transnationalen Terrorismus. Soziologische Perspektiven. Wiesbaden 2007, S. 125ff, hier S. 148ff.

der Rationalität staatlicher Organisationen kompatibel. Dennoch müssen Sponsoring States den unterstützten Terrororganisationen weitgehend Autonomie gewähren – nicht zuletzt um im Zweifelsfall jede Kooperation abstreiten zu können.[32] Das kann aber auch bedeuten, dass Staat und Terroristen verschiedene Ziele und Strategien verfolgen. So könnten Terrororganisationen in einem Ausmaß Gewalt anwenden, welches mit dem vom Sponsoring State intendierten Einsatz wohldosierter Anschläge zur Ausübung politischen Drucks auf einen gegnerischen Staat nicht mehr vereinbar ist. Schließlich stehen dem Sponsoring State und den Terrororganisationen jeweils sehr unterschiedliche Informationsquellen zur Verfügung: Staaten verfügen über Geheimdienstapparate und diplomatische Kanäle, wo hingegen Terrororganisationen ihre Informationen überwiegend aus den Massenmedien bzw. aus dem Untergrund beziehen müssen. Diese Informationsasymmetrie schränkt die Kontrollmöglichkeiten des Sponsoring State gegenüber der Terrororganisation stark ein.[33] Um Terroristen dann in ein Abhängigkeitsverhältnis zu zwingen, greifen Staaten sogar zur Möglichkeit, konkurrierende Terrororganisationen einzuspannen um sie gegeneinander auszuspielen bzw. sie sogar dazu zu bringen, einander gegenseitig zu bekämpfen.[34] Sowohl Terrororganisationen als auch Sponsoring States sind dann im Kontext solcher Kooperationen also nicht zwangsläufig zuverlässige Partner.

Im Gegensatz zu SST ist die staatliche Unterstützung von Partisanen bzw. Guerillas[35] und Aufständischen hingegen viel naheliegender und Erfolg versprechender: deren irreguläre Kampfverbände sind in besonderem Maße auf Sponsoring States angewiesen, weil sie für gewöhnlich eine wesentlich höhere Anzahl an Mitgliedern haben, die bewaffnet, versorgt und besoldet werden müssen. Sie benötigen häufig auch schwerer organisierbare Waffen, wie z.B. tragbare Boden-Luft-Raketenwerfer oder Panzerabwehr-Schulterwaffen, die für eine direkte Konfrontation mit regulären Streitkräf-

---

32 Vgl. Byman, Daniel/Kreps, Sarah E.: Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, S. 1ff, hier S. 6.

33 Vgl. ebd., S. 7.

34 Vgl. ebd., S. 11f.

35 Siehe für eine allgemeine Darstellung Ibrahim, Azeem: Conceptualisation of Guerrilla Warfare. In: Small Wars & Insurgencies, 15(3) 2004, S. 112ff.

ten im Zuge einer ‚hit and run'-Strategie ausgerichtet sind, sich aber für den Einsatz bei Anschlägen von Terrororganisationen gegen zivile Einrichtungen kaum eignen. Guerillas haben praktische Kenntnisse der asymmetrischen Kriegsführung, über welche reguläre Armeen kaum verfügen – gerade diese Expertise kann Staaten dazu bewegen, auf die Fähigkeiten von Guerillatruppen zurückzugreifen.[36] Nicht zuletzt ist die Unterstützung von Guerillas im Vergleich zum SST auch deshalb attraktiver, weil hier die Wahrscheinlichkeit viel höher ist, im target state einen regime change herbeizuführen, sofern die aufständischen Guerillas mit ihren Unternehmungen erfolgreich sind.[37] Diese erheben nämlich, im Gegensatz zu Terroristen, einen real verwirklichbaren, territorial definierten Machtanspruch: „Der [...] Guerilla besetzt tendenziell den Raum, um später das Denken gefangen zu nehmen, der Terrorist besetzt das Denken, da er den Raum nicht nehmen kann."[38] Womöglich fällt auch die staatliche Kooperation mit Guerillas insofern leichter, als deren Strukturen denjenigen regulärer Armeen ähnlicher sind und das Vorgehen der Guerillas aufgrund ihres oft relativ hohen Grades der Formalisierung von Kommandostrukturen nicht so stark von internen Beziehungsnetzwerken irritiert werden kann, wie das bei Terrororganisationen der Fall ist. Dennoch kann nicht ausgeschlossen werden, dass Guerillas oder Partisanen auch Anschläge verüben, die dann aber nur ein taktisches Element einer asymmetrischen Kriegsführungsstrategie darstellen und nicht dieselbe Bedeutung haben wie in einer idealtypischen Terrorismusstrategie.

3.2.5 Conclusio

Für Staaten, die im Rahmen einer hybriden Machtprojektion gegnerische Staaten bedrohen, ergeben sich durch die Unterstützung und Instrumenta-

---

36 Vgl. Byman, Daniel/Kreps, Sarah E.: Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism. In: International Studies Perspectives, 11(1) 2010, S. 1ff, hier S. 3f.

37 Vgl. Byman, Daniel: Deadly Connections. States that Sponsor Terrorism. Cambridge et al. 2005, S. 38f.

38 Wördemann, Franz: Terrorismus. Motive, Täter, Strategien. München 1977, S. 57; siehe auch Waldmann, Peter: Terrorismus. Provokation der Macht. Hamburg 2005, S. 19f.

lisierung von Terrororganisationen gewisse Vorteile: Terroristen können durch den Aufbau einer allgegenwärtigen Bedrohungskulisse die Regierung eines verfeindeten Staates politisch schwächen. Dabei können Sponsoring States offiziell jede Kooperation mit Terroristen abstreiten und zugleich dennoch Druck auf einen Target State ausüben. Dadurch kann ein Sponsoring State effektiv Gewalt gegen die zivile Bevölkerung des Target State ausüben, ohne dass es dabei zu einer militärischen Auseinandersetzung und damit zu einer weiteren Eskalation des Konflikts kommt. Diplomatische Kanäle können daher aufrechterhalten bleiben und, im Sinne einer Strategie hybrider Machtprojektion, weiterhin zur Durchsetzung der Interessen des Sponsoring State eingesetzt werden. Es handelt sich bei SST darüber hinaus auch um eine sehr ressourcenschonende Möglichkeit der Machtprojektion, die insbesondere für Staaten mit geringen militärischen Kapazitäten eine Option darstellt. Allerdings bietet SST auch für mittlere Mächte die Chance, eine signifikante Bedrohung darzustellen – und das weit über die Grenzen des eigenen Einflussgebietes (oder über die Reichweite ballistischer Raketen) hinaus.

Allerdings sind Kooperationen zwischen Staaten und Terrororganisationen nicht ohne weiteres möglich: zunächst müssen im politischen System des Target State bestimmte hochdifferenzierte Strukturen vorhanden sein, die den Einsatz einer terroristischen Strategie überhaupt sinnvoll machen. Dazu zählen insbesondere ein etabliertes staatliches Gewaltmonopol sowie eine politische Öffentlichkeit mit einer freien Medienlandschaft, da Terrorismus in Räumen begrenzter Staatlichkeit und ubiquitärer Gewalt nicht die intendierte Schockwirkung entfalten kann, zumal erst die öffentliche Berichterstattung für das Aufgehen einer Terrorstrategie essentiell ist. Des Weiteren kann eine Terrororganisation nicht „künstlich" erzeugt werden, sondern muss erst im Rahmen politischer Proteste im politischen System des Target State selbst emergieren, was ein sehr voraussetzungsreicher und zufallsgesteuerter Prozess ist. Auch eine gewisse ideologische Übereinstimmung zwischen Sponsoring State und Terrororganisation stellt eine wichtige Voraussetzung für eine Zusammenarbeit gegen einen gemeinsamen Gegner dar. Terrororganisationen schließlich, so die hier vertretene Ansicht, sind überdies kaum durch einen Staat steuerbar, weil sie insbesondere durch ihre internen sozialen Dynamiken beeinflusst werden und aus Gründen des Selbsterhaltes und des Zusammenhaltes, oder um interne Machtkonflikte zu vermeiden, von ihrer ursprünglichen Strategie und ihren Feinddefinitionen abrücken können um andere Ziele zu verfolgen, die

mit den Intentionen des Sponsoring State kollidieren können. Schließlich wäre auch denkbar, dass Terroristen Gewalt auch nicht mehr so gering dosiert einsetzen wie vom Sponsoring State geplant wurde, sodass es zur unerwünschten Konflikteskalation kommen kann.

Als viel wahrscheinlicher wurde hier die Unterstützung von Guerillas und Aufständischen eingeschätzt. Diese orientieren sich hinsichtlich ihrer Bewaffnung und internen Verfasstheit am Vorbild regulärer staatlicher Armeen und weisen daher oft große strukturelle Ähnlichkeiten mit ihnen auf. Das erleichtert die Kooperation mit einem Staat wesentlich, zumal größere Kampfverbände wie Guerillas einen höheren Grad der Formalisierung und geringere Volatilität bei der Zielauswahl aufweisen als kleine Terrororganisationen. Darüber hinaus besteht bei entsprechendem Erfolg der Guerillas sogar die Möglichkeit eines Regime Change, die bei der Unterstützung von Terroristen eher unwahrscheinlich wäre. Auch aus völkerrechtlicher Sicht ist die Unterstützung von Guerillas leichter zu rechtfertigen, da diese durch ihren Kombattantenstatus – im Gegensatz zu Terroristen - zumindest einen gewissen Grad der Anerkennung innehaben. In beiden Fällen aber, ob es sich um die Unterstützung von Terroristen oder von Guerillas handelt, stehen die notwendigen Voraussetzungen der hybriden Machtprojektion nicht zur Disposition des Sponsoring State. Ein Staat, der durch Anwendung solcher Druckmittel seinen politischen Willen durchsetzen will, ist in beiden Fällen immer auf eine bereits fortgeschrittene Eskalation von Konflikten im politischen System des target state angewiesen, die er sich zunutze machen kann. Damit unterscheidet sich das Instrument des Sponsoring von Terroristen/Guerillas von anderen Möglichkeiten im Rahmen hybrider Machtprojektion, wie z.B. wirtschaftlichen Sanktionen, geheimdienstlichen Operationen, Angriffen im Cyberspace usw. für welche ein Staat auf seine eigenen Ressourcen und Infrastrukturen zurückgreifen kann.

Die hier vorgeschlagene Beschreibung von SST nahm bewusst die Perspektive des Sponsoring State ein, und fokussierte sich auf dessen Beziehungen zu Terrororganisationen. Was aber konkrete Empfehlungen für den Umgang von Target States mit dieser Form hybrider Bedrohung betrifft, so können diese hier nur als Desiderate gekennzeichnet werden. Das Ziel der hier angestellten Überlegungen war es, einen Beitrag zum Verständnis von Problemzusammenhängen und Bedingungen der Möglichkeit von SST zu liefern. Wenn dieses Ziel erreicht wurde, wäre damit bereits eine wichtige Prämisse für die Entwicklung geeigneter Gegenstrategien gesetzt.

3.3 Cybersecurity – Bewusstseinsbildung in der Gesellschaft

Alfred Gulder

Im Rahmen des Projektes „Hybride Bedrohungspotenziale und daraus resultierende sicherheitspolitische Ableitungen für Kleinstaaten“ am Institut für Friedenssicherung und Konfliktmanagement (IFK) wurde insbesondere der Bedrohungsfaktor Cybersecurity für die drei Referenzstaaten Niederlande[1], Schweden und Slowakei untersucht.

Grundlagen dazu bilden Erkenntnisse aus der IFK-Vorstudie „Hybridität politischer Machtprojektionen“, welche die Einflüsse von hybriden Bedrohungspotenzialen und -faktoren in den Großmächten USA, Russland, China und Indien und deren Strategien zur Bewältigung aufzeigen. Basierend auf diesen Erkenntnissen soll eine Ableitung dieser Machtprojektionsmechanismen auf die oben genannten drei Referenzstaaten erfolgen, um im Anschluss mögliche Rückschlüsse hinsichtlich der Bedrohungsbilder unter besonderer Beobachtung der Cyberkomponente aus österreichischer Perspektive zu ziehen.

> „Mit Machtprojektion bezeichnet man die Fähigkeit einer Nation, alle oder einige ihrer Elemente - politische, wirtschaftliche, militärische oder via Informationssendungen - der nationalen Macht anzuwenden, schnell und effektiv einzusetzen und Kräfte in und aus mehreren verteilten Standorten zu unterstützen, damit diese auf Krisen reagieren, als Abschreckung beitragen und die regionale Stabilität verbessern.“ [2]

Als früheres klassisches Ziel von Machtprojektion ist z.B. der Kampf um Rohstoffe zu nennen, die Durchführung erfolgte in der Vergangenheit mittels Schiffen und Flugzeugen. In der heutigen Zeit sind die Rollen von Ziel und Mittel der Durchführung insbesondere im Bereich der Informati-

---

[1] Da im Rahmen eines Expertengesprächs Datenmaterial zu den Niederlande im Bereich Cybersecurity vorhanden war fiel die Entscheidung, dieses in diesen Beitrag mit einzuarbeiten.

[2] Definition power projection. <http://www.dtic.mil/doctrine/dod_dictionary/data/p/10683.html>, abgerufen am 28.08.2013. Übersetzung.

ons- und Kommunikationstechnologie (IKT) deutlich ausgeprägter. Dabei hängt fast die gesamte Volkswirtschaft (Energieversorgung, Finanzwesen, etc.) von Staaten von einer funktionierenden IKT-Infrastruktur ab, welche es zu schützen gilt. Um jedoch in einem anderen Staat z.B. politische oder wirtschaftliche Interessen als Machtprojektion durchzusetzen, sind genau diese kritischen Bereiche zu schädigen. Eine kurz- oder langfristige Schädigung des IKT-Bereiches kann z.B. durch einen Cyberangriff auf kritische Infrastrukturen erfolgen, deren Auswirkungen bis dato nur theoretisch abschätzbar sind.

In einem IFK-Projekt 2011-2013 wurden erkannte hybride Bedrohungsfaktoren von Großmächten behandelt und erläutert. Daraus wurde Cyberbedrohung schon als ein wesentliches Element der Machtprojektion angeführt. Dieses Element wird nun für die 3 Referenzstaaten in unterschiedlichen Themenbereichen näher analysiert. Die Themenbereiche wurden anhand der Handlungsfelder, welche in der „Österreichischen Strategie für Cybersicherheit“[3] genannt werden, sinnvoll angepasst und als Grundlage für die Fragestellung verwendet. Die folgenden Themenbereiche wurden evaluiert und das Ergebnis ist auf den nachfolgenden Seiten tabellarisch dargestellt.

- Wie sieht das Bedrohungsszenario aus?
- Sind Gesamtkonzepte/Lösungsansätze definiert?
- Sind strategische Ziele definiert?
- Sind Strukturen und Prozesse aufgesetzt? (Rollen, Zuständigkeiten, Kompetenzen von staatlichen und nicht-staatlichen Akteuren)
- Ist eine Kooperation zwischen Staat, Wirtschaft und Gesellschaft aufgesetzt?
- Wie erfolgt die nationale Zusammenarbeit mit dem Militär?
- Wie erfolgt eine internationale Zusammenarbeit bzw. wie sieht die Einbettung in Sicherheitsorganisationen (z.B. NATO) aus?

---

[3] Bundeskanzleramt Österreich: Österreichische Strategie für Cyber Sicherheit. <http://www.bka.gv.at/DocView.axd?CobId=50748>, abgerufen am 26.08.2013.

- Wie erfolgt die Sensibilisierung und Ausbildung?
- Wie erfolgt die Forschung und Entwicklung?
- Wie erfolgt der Schutz kritischer Infrastrukturen?

Erkenntnisse aus der Analyse der drei Referenzstaaten Niederlande, Schweden und Slowakei (Details siehe Tabelle 5):

In den letzten Jahren wurden in allen drei Staaten Assessments durchgeführt, um ein detailliertes nationales Lagebild und *Bedrohungsszenario* bezüglich Cybersecurity zu erarbeiten. Als Kernelemente werden der Verlust der Vertraulichkeit von Informationen, die digitale Spionage und das Einschleusen von Computerviren genannt. Die Cyberkriminalität hat ebenfalls einen steigenden Stellenwert, jedoch mit dem Hintergrund eines Betruges von professionellen Kriminellen und ist weniger als Machtprojektion zu bewerten.

Aus den Assessments heraus wurden *Lösungsansätze* und strategische Ziele definiert, welche in allen drei Staaten in einem nationalen Cyberstrategie-Dokument niedergeschrieben wurden. Die Anzahl der definierten strategischen Ziele liegt zwischen drei in der Slowakei und fünf in den Niederlanden und Schweden.

Die *strategischen Ziele* der Niederlande fokussieren auf eine verstärke nationale und internationale Zusammenarbeit, der Schweden ebenfalls auf Zusammenarbeit und Bereitstellung von Fähigkeiten und der Slowakei auf Prävention und Leistungsbereitschaft.

Betreffend Bündelung der Cybersecurity-Aktiviäten und *Schaffung nationaler Strukturen* wurde in den Niederlanden bereits Anfang 2012 ein National Cyber Security Centre operationell in Betrieb genommen, in Schweden und Slowakei sind mehrere Ansprechstellen in unterschiedlichen Ministerien aktiv. Schwedens Civil Contingencies Agency (MSB) soll in Zukunft die Einrichtung einer nationalen operationellen Koordinationsstelle für Cybersecurity übernehmen. Damit wurde erkannt, dass zu viele Stakeholder mit teilweise unklaren Aufgaben und Schnittstellen nicht effektiv arbeiten können.

Alle Staaten haben ein international vernetztes Computer Emergency Response Team (CERT) als *Ansprechpartner für die Wirtschaft* operationell in Betrieb.

Die *nationale Zusammenarbeit mit dem Militär* erfolgt in allen drei Staaten ähnlich. In den Niederlanden ist zusätzlich eine „Defense Strategy for Operating in Cyberspace" mit sechs Handlungsbereichen definiert worden. In Schweden erfolgt die militärische Zusammenarbeit und der Austausch der Informationen über eine National Cyber Defense Organisation, in der Slowakei über das Institute of Security and Defence Studies des Verteidigungsministeriums.

Die *internationale zivile Zusammenarbeit* erfolgt bei allen 3 Staaten über das European Government Computer Emergency Response Team. Die *militärische Kooperation* erfolgt über eine bilaterale Kommunikation und dem Austausch von best practices mit dem wichtigsten Partner NATO und dem NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estland. Weiters sind lokale Vernetzungen mit den Nachbarstaaten in Schweden durch die Nordic Defence Cooperation (Norwegen, Finnland, Schweden, Island, Dänemark) gegeben.

Trainingskurse zur Aus- und Weiterbildung sind über das Internet abrufbar und in allen drei Staaten mit eigenen Trainingszentren gut ausgebaut. Unterschiedliche Dokumente und Schriftenreihen werden angeboten.

Beim Thema *Forschung und Entwicklung* erfolgt in den Niederlanden die Koordination von Forschungsprogrammen zwischen Institutionen und Privatwirtschaft über das National Cyber Security Council, in Schweden über die militärische Einrichtung der Swedish Defence Research Agency und in der Slowakei über zumindest 3 Universitäten.

Für den *Schutz kritischer Infrastrukturen* ist in den Niederlanden eine Plattform (Centre for Protection of National Infrastructure) für den Bereich kritischer Sektoren für den Austausch von Informationen über Vorfälle, Bedrohungen, Schwachstellen und guten Praktiken im Bereich Cybercrime und Cybersecurity errichtet worden. In Schweden wurde bereits 2005 die National Telecommunications Coordination Group gegründet, welche zur Unterstützung der Wiederherstellung der nationalen Infrastruktur für die elektronische Kommunikation unterstützend tätig ist. In der Slowakei er-

folgt diese Aufgabe über das Governmental Computer Security Incident Response Team.

Rückschlüsse und Ableitungen für Österreich:

Im Bereich Cybersecurity ist Österreich national und international[4] aktiv tätig. Eine Cybersecurity-Strategie ist mit März 2013 aufgesetzt worden und definiert die folgenden sieben Handlungsfelder:

- Strukturen und Prozesse
- Governance
- Kooperation von Staat, Wirtschaft und Gesellschaft
- Schutz kritischer Infrastrukturen
- Sensibilisierung und Ausbildung
- Forschung und Entwicklung
- Internationale Zusammenarbeit

Das Bedrohungsbild für Österreich ist im Anhang 1 der Cybersecurity-Strategie als Cyber-Risikomatrix 2011 aufgezeigt. Als Bedrohungen mit katastrophalen Auswirkungen mit hoher Eintrittswahrscheinlichkeit sind u.a. nicht erkannte IKT-Anomalien, bösartige Software und Cyberspionage genannt.

Die „Nationale IKT-Sicherheitsstrategie Österreich“ [5] wurde 2012 veröffentlicht und beschreibt die strategischen Zielsetzungen und Maßnahmen in fünf Kernbereichen:

---

[4] European Network and Information Security Agency (ENISA): Austria country report, 2011. <http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Austria.pdf/at_download/file>, abgerufen am 29.08.2013

[5] Bundeskanzleramt Österreich: Nationale IKT-Sicherheitsstrategie Österreich, 2012. <http://www.oesterreich.gv.at/DocView.axd?CobId=47986>, abgerufen am 27.08.2013.

- Stakeholder und Strukturen
- Kritische Infrastrukturen
- Risikomanagement und Lagebild
- Bildung und Forschung
- Awareness

Die Sicherheitsstrategie benennt alle involvierten Stakeholder und deren Zusammenarbeit. Inwieweit die praktische Umsetzung der Zusammenarbeit wahrgenommen wird, kann nicht verifiziert werden. Zumindest sind in Österreich sehr viele Initiativen zur Zusammenarbeit zwischen Gesellschaft, Wirtschaft, Interessensvertretungen, Wissenschaft und öffentliche Hand als auch Projekte zur Bildung von „Awareness" aufgesetzt.

Ein Masterplan zum Schutz kritischer Infrastruktur (APCIP = Austrian Program for Critical Infrastructure Protection) wurde 2008 vom Ministerrat beschlossen und legt die Grundsätze, Verantwortlichkeiten und die einzelnen Arbeitsschritte zur Entwicklung eines österreichischen Programms zum Schutz kritischer Infrastrukturen fest und war somit Ausgangspunkt für den Umsetzungsprozess auf nationaler Ebene.[6]

Das nationale Sicherheitsforschungsprogramm KIRAS dient zur Förderung der Sicherheitsforschung in Österreich und unterstützt nationale Forschungsvorhaben mit dem Ziel der Erhöhung der Sicherheit Österreichs und seiner Bevölkerung.

Betreffend die Zusammenarbeit mit dem NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallin, Estland, nahmen österreichische Experten bereits an der im Jahre 2012 abgehaltenen Übung „Locked Shields 2012" teil. Ein Kooperationsvertrag mit der NATO (ähnlich wie ihn die Slowakei hat), wonach Österreich im Falle eines Cyberangriffes mit anderen NATO-Staaten kooperieren könnte und bei der Entwicklung

---

[6] Vgl. Austrian Program for Critical Infrastructure Protection - Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP).Beschlossen am 02.04.2008 vom Ministerrat. <http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf>.

von Leitlinien für die praktische Kooperation im Bereich Cybersecurity mit anderen NATO-Partnern unterstützend tätig ist, wäre dingend anzudenken.

Fazit

- Im Vergleich zu den Referenzländern Niederlande, Schweden und Slowakei ist Österreich gut aufgestellt und zeigt theoretisch klare Strukturen und Verantwortlichkeiten auf.
- Die Zusammenarbeit mit den unterschiedlichen Stakeholdern ist mittels Durchführung praktischer Cyber Security Assessments – ähnlich wie das jährlich durchgeführte Assessment in den Niederlanden – zu überprüfen und kritisch zu hinterfragen.
- Eine Bündelung der österreichischen Cybersecurity-Aktivitäten in einem nationalen Koordinationszentrum – wie es bereits in den Niederlanden erfolgt und in Schweden derzeit aufgebaut wird – sollte ebenfalls überdacht werden.
- Die zivile und militärische Zusammenarbeit bzw. der Ausbau des Informationsaustausches auf nationaler und internationaler Ebene wie z.B. mit dem NATO-Zentrum CCDCOE ist einer der Schlüsselfaktoren, um Cyberangriffe in Österreich zeitgerechter und effektiver bekämpfen oder präventiv verhindern zu können.

Themenbereich	Niederlande	Schweden	Slowakei
1. Bedrohungsszenario	Die Niederlande führen seit 2011 jährlich das sogenannte Cyber Security Assessment Netherlands in Kooperation mit Ministerien, Militär, Wirtschaft und Forschungsinstitutionen durch, um Akteure, Bedrohungen, Verwundbarkeiten, Widerstandsfähigkeiten und verwendete Werkzeuge und Methoden zu überprüfen. Als Hauptgefahren sind im Ergebnisbericht die digitale Spionage (insbesondere aus den Staaten Russland, China und Iran), eine Störung als Folge von Malware Infektion und Spam und digitaler (Identitäts-) Betrug genannt. Das Assessment 2013 ergab, dass die größten Gefahren immer noch durch geheime Aktivitäten von professionellen Kriminellen und Staaten entstehen. Die größte Bedrohung für die Regierung betrifft die Vertraulichkeit der Informationen und die Kontinuität des Dienstes.	Im Jahre 2009 wurde ein Situational Assessment betreffend Informationssicherheit in Schweden durchgeführt. Als Bedrohungsszenarien wurden damals Cybercrime, und der Verlust der Vertraulichkeit von Informationen angegeben. Aktuellere Daten konnten nicht gefunden werden.	In der „National Strategy for Information Security of the Slovak Republic“ sind die als am stärksten wachsenden Bedrohungen die Verwundbarkeit der Informations- und Kommunikationssysteme, ihre Überlastung, der unberechtigte Zugriff auf Informationen, die Verbreitung von Computerviren und Fehlinformationen identifiziert worden.

Themenbereich	Niederlande	Schweden	Slowakei
2. Gesamtkonzept/ Lösungs-ansätze	Mit Juni 2011 wurde das Dokument „The National Cyber Security Strategy (NCSS)“ von der Niederländischen Regierung angenommen und beschreibt das Gesamtkonzept betreffend der Cyberstrategie inkl. der handelnden Akteure.	Am 1. Februar 2010 ist die MSB (Swedish Civil Contingencies Agency)-Verordnung über Informationssicherheit bei Behörden (MSBFS 2009:10) in Kraft getreten. Die Regierung hat MSB mit der Verwaltung des nationalen Aktionsplans für die Informationssicherheit (aktualisiert im Jahr 2010) beauftragt. Vier Bereiche wurden als Schwerpunkte festgelegt: - Es besteht ein Bedarf für eine verbesserte multisektorielle und sektorübergreifende Arbeit an gesellschaftlicher Informationssicherheit. - Ein grundlegender Sicherheitsstandard für die Sicherheit von Informationen muss eingerichtet werden. - Die Gesellschaft muss in der Lage sein, mit umfangreichen IT-bezogenen Störungen und Krisen umzugehen. - Es besteht ein Mangel an Information Security Know-how auf allen Ebenen der Gesellschaft. Weitreichende Investitionen in die Qualifizierung in diesem Bereich sind notwendig.	Das Dokument „National Strategy for Information Security of the Slovak Republic“ wurde im August 2008 von der Slowakischen Regierung genehmigt. Die nationale Strategie für die Informationssicherheit umfasst die Sicherheit für kritische Infrastrukturen, betont die Vermeidung von Angriffen, den Aufbau einer Verteidigung und die Aufrechterhaltung einer nachhaltigen Infrastruktur.

Themenbereich	Niederlande	Schweden	Slowakei
3. Sind strategische Ziele definiert?	Das Dokument „The National Cyber Security Strategy (NCSS)“, Juni 2011) beschreibt die folgenden 5 strategischen Ziele: - - Initiativen zu verlinken und zu verstärken - Förderung der individuellen Verantwortung - Schaffung von öffentlich-privaten Partnerschaften - Internationale Zusammenarbeit fördern - Balance zwischen Selbst-Regulierung und Gesetzgebung schaffen	Das Dokument „STRATEGY FOR SOCIETAL INFORMATION SECURITY 2010 – 2015“ zeigt folgende 5 strategische Bereiche auf: - Informationssicherheit in Unternehmen - Bereitstellung von Fähigkeiten - Austausch von Informationen, Zusammenarbeit und Antworten - Sicherheit in der Kommunikation - Sicherheit von Produkten und Systemen	Das Dokument „National Strategy for Information Security of the Slovak Republic“ umfasst 3 strategische Ziele: - Prävention (um einen angemessenen Schutz zu erreichen und um das Auftreten von sicherheitsrelevanten Ereignissen zu minimieren) - Leistungsbereitschaft (ausreichende Kapazitäten aufbauen, um eine wirksame Reaktion auf sicherheitsrelevante Ereignisse zu liefern, um ihre Auswirkungen zu minimieren und um eine frühzeitige Wiederherstellung der beschädigten Systeme zu ermöglichen) - Kontinuierliches und nachhaltiges Niveau bei INFOSEC (Aufbau, Pflege und Entwicklung von Know-how)

Themenbereich	Niederlande	Schweden	Slowakei
4. Sind Strukturen und Prozesse aufgesetzt? (Rollen, Zuständigkeiten, Kompetenzen von Staat und nichtstaatlichen Akteuren)	Das Cyber Security Council und das National Cyber Security Centre (NCSC) sind seit 01.01.2012 aktiv tätig und als nationale Ansprechstelle zuständig. Das Centre umfasst ebenfalls das GOVCERT.NL. Folgende Zuständigkeiten sind definiert: Das Innenministerium koordiniert abteilungsübergreifend das Thema Cybersecurity zwischen verschiedenen zivilen und militärischen Einheiten, die für Cyber-Themen zuständig sind. Weiters ist das Innenmisterium für die interministerielle Koordination betreffend Cybersecurity durch das National Security Programm zuständig.	Derzeit teilen sich verschiedene Institutionen die Aufgaben und Kompetenzen: Das Ministerium für Unternehmen, Energie und Kommunikation, das Justizministerium und das Verteidigungsministerium sind zuständig für die Koordination der Entwicklung der nationalen Informations-Sicherheitspolitik/Strategie, Gesetzgebung und Forschung im Bereich Cybersecurity. Die Ausführung der strategischen Politik wird von den Organisationen, die von den genannten Ministerien beaufsichtigt werden, durchgeführt.	Folgende Zuständigkeiten sind erkannt worden: Das Finanzministerium ist als zuständige nationale Informationssicherheitsstelle für den Bereich der nichtklassifizierten Informationen genannt. Die National Security Authority, eine unabhängige staatliche Stelle, ist als nationale Sicherheitsagentur für den Bereich von Verschlusssachen zuständig. Das Government Plenipotentiary for Information Society ist verantwortlich für die Koordination der Information Society.

Themenbereich	Niederlande	Schweden	Slowakei
	Cyber-Kriminalität wird durch das Justizministerium behandelt. Cyber Terrorism fällt unter die nationale Koordination der Terrorismusbekämpfung (NCTB). Cyber Defense ist eine gemeinsame Verantwortung zwischen dem Verteidigungsministerium und dem Innenministerium. Behörden (wie OPTA und Netherlands Consumer Authority), Government inspectorates (wie Health Care Inspectorate), private Firmen (wie ISPs und security vendors), und nationale und internationale Knowledge- und Research- Institutionen	Derzeit teilen sich verschiedene Institutionen die Aufgaben und Kompetenzen: Das Ministerium für Unternehmen, Energie und Kommunikation, das Justizministerium und das Verteidigungsministerium sind zuständig für die Koordination der Entwicklung der nationalen Informations-Sicherheitspolitik/Strategie, Gesetzgebung und Forschung im Bereich Cybersecurity. Die Ausführung der strategischen Politik wird von den Organisationen, die von den genannten Ministerien beaufsichtigt werden, durchgeführt.	Die Commission for Information Security unter dem Finanzministerium fungiert zusammen mit der slowakischen Regierung als nationale Entscheidungsprozessbehörde in der Entwicklung der Politik für Informationssicherheit. Die Kommission ist eine Arbeitsgruppe bestehend aus den Mitarbeitern des Finanzministeriums, nationalen Netzwerk- und Informationensicherheits-interessensgruppen (wie andere Ministerien) und externen Experten auf dem Gebiet der Informationssicherheit.

Themenbereich	Niederlande	Schweden	Slowakei
	Kritische nationale Infrastruktur wird durch das Wirtschaftsministerium gehandhabt Weiters sind u.a. folgende Stellen aufzuzählen: - AIVD (General Intelligence and Security Service) - MIVD (Military Intelligence and Security Service) - Polizei, Special investigative services (wie FIOD und SIOD), Aufsichtsbehörden (wie OPTA und Netherlands Consumer Authority), Government inspectorates (wie Health Care Inspectorate), Private Firmen (wie ISPs and security vendors), und National and international knowledge and research Institutions.	Die Cooperation Group for Information Security (SAMFI) besteht aus: - Swedish Civil Contingencies Agency (MSB), zuständig für die Verbesserung und Unterstützung der gesellschaftliche Kapazitäten für die Vorbereitung und Prävention von Notfällen und Krisen - Swedish Post and Telecom Agency (PTS) wirkt als Aufsichtsbehörde für die Sicherheit in der elektronischen Kommunion (Telekommunikation, Internet und Radio) und bei der Nutzung von elektronischen Signaturen - Swedish National Defence Radio Establishment (FRA) ist in der Informationssicherheit tätig. Auf Wunsch unterstützt die Försvarets radioanstalt (FRAU) Behörden und staatlichen Unternehmen bei aktuellen IT-Bedrohungen und gibt allgemeine Ratschläge zur Verbesserung der Sicherheit.	Die Kommission arbeitet mit der Slovak Telecom, dem Personal Data Protection Office, dem Innenministerium und der National Security Authority zusammen. Die Kommission ist verantwortlich für die Bewertung der vorgeschlagenen Sicherheitsstandards für den Schutz der Informationssicherheitssysteme der öffentlichen Verwaltung im Rahmen der nicht-klassifizierten Informationen, der Einreichung von Vorschlägen von Sicherheitsstandards, der Änderung oder Modifikation von bestehenden Sicherheitsstandards für Informationssicherheitssysteme der öffentlichen Verwaltung.

Themenbereich	Niederlande	Schweden	Slowakei
		- Das Swedish Security Service (Säpo) und Swedish Criminal Investigation Service (RKP) sind für Cybercrime zuständig - Die Swedish Defence Materiel Administration (FMV) / Swedish Certification Body for IT Security (CSEC) ist für die Aufsichtsbehörde hinsichtlich der elektromagnetischen Verträglichkeit (EMV) - Swedish Armed Forces (FM)/Military Intelligence and Security Service (MUST) für militärische Aspekte der Cybersecurity und Cyberwar.	

Themenbereich	Niederlande	Schweden	Slowakei
5. Ist eine Kooperation zwischen Staat, Wirtschaft und Gesellschaft aufgesetzt?	Das NCSC umfasst ebenfalls das GOVCERT.NL (Computer Emergency Response Team) und gilt ebenfalls als Ansprechpartner für Wirtschaft und Gesellschaft via dem ICT Response Board (IRB). Siehe auch Punkt Strukturen: eine CERT.NL für die zivile Komponente ist aufgesetzt.	Eine Kooperation erfolgt über die Cooperation Group for Information Security (SAMFI) und besteht aus den oben genannten Organisationen. Es erfolgt alle 2 Monate ein Abstimmungsmeeting. Publikationen für Wirtschaft und Gesellschaft unter <https://www.msb.se/en/Prevention/Information-security/Information-security-publications/> Weiters ist eine CERT-SE seit 01.01.2011 aufgesetzt.	CSIRT.SK (Computer Security Incident Response Team), das überwiegend für die Regierung bei Attacken auf nationale kritische Infrastrukturen sowie auf die öffentliche Verwaltung und die Privatwirtschaft aktiv wird (nicht für Verschlusssachen und militärische Zwischenfälle). Eine CERT.SK für die zivilen Belange ist ebenfalls operationell tätig.

Themenbereich	Niederlande	Schweden	Slowakei
6. Wie erfolgt die nationale Zusammen-arbeit mit dem Militär?	Kooperation mit dem Defence Computer Emergency Response Team (DefCERT). Weiters umfasst das Dokument „Defence Strategy for Operating in Cyberspace“ vom Juni 2012 die folgenden sechs Handlungsbereiche: Anwendung eines umfassenden Ansatzes; Stärkung der Cyberverteidigung der Defence Organisation (defensive Element) Entwicklung der militärischen Fähigkeiten, um Cyber-Operationen (offensive Element) durchzuführen Stärkung der Position in Cyberspace Intelligenz (intelligence Element) Stärkung des Fachwissens und der Innovationskraft betreffend Abwehrorganisation im Cyberspace, einschließlich der Rekrutierung und Bindung von qualifiziertem Personal (adaptive und innovative Elements); Intensivierung der Zusammenarbeit, sowohl national als auch international (cooperation Element).	Die Zusammenarbeit erfolgt mit dem Swedish Armed Forces (FM)/Military Intelligence and Security Service (MUST) und dem Swedish National Defence Radio Establishment (FRA). Im Jänner 2013 wurde eine National Cyber Defense Organisation, welche die Informationen aus den Cyber-Einheiten der Organisationen FRA, MUST und dem nationalen Nachrichtendienst und SÄPO untereinander austauschen, formiert. Weiters besteht im Rahmen der Nordic Defense Cooperation (NORDEFCO) zwischen Norwegen, Finnland, Schweden, Island und Dänemark eine Zusammenarbeit im Bereich Cyber Defence und Cyber Security.	Die Zusammenarbeit erfolgt mit dem Institute of Security and Defence Studies des Verteidigungsministeriums. Das Institut ist verantwortlich für die professionelle Vorbereitung der Unterlagen für Entscheidungen im Bereich der Sicherheit, Verteidigung und Krisenmanagement.

Themenbereich	Niederlande	Schweden	Slowakei
7. Wie erfolgt eine inter-nationale Zusammen-arbeit bzw. wie sieht die Einbettung in Sicherheits-Organisationen (z.B. NATO) aus?	Internationale Vernetzung u.a. mit: - European Government CERTs, ENISA (European Network and Information Security Agency) - International Watch and - Warning Network (IWWN) - International network of Computer Security and Incident Response Teams (CSIRTs); insbesondere Polen, Australien, den USA und Japan. - Bilaterale Kommunikation und Austausch von best practices mit dem wichtigsten Partner NATO und dem NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estland	Internationale Vernetzung u.a. mit: - European Government CERTs, ENISA (European Network and Information Security Agency) - Bilaterale Kommunikation und Austausch von best practices mit der NATO über eine Kooperationsvertrag und mit dem NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) in Tallinn, Estland - Militärische Vernetzung Rahmen der Nordic Defense Cooperation (NORDEFCO) zwischen Norwegen, Finnland, Schweden, Island und Dänemark.	Die Slowakei ist neben Estland, Deutschland, Ungarn, Italien, Lettland, Litauen, Niederlande, Polen, Spanien und den USA Sponsor des NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estland. Weiters hat die Slowakei mit der NATO einen Vertrag unterzeichnet, sodass diese im Falle eines Cyberangriffes mit anderen NATO-Staaten kooperieren kann und bei der Entwicklung von Leitlinien für die praktische Kooperation im Bereich der Cybersecurity mit anderen NATO Partnern unterstützend tätig sein kann.

Themenbereich	Niederlande	Schweden	Slowakei
8. Wie erfolgt die Sensibili-sierung und Ausbildung?	Das NCSS beschreibt eine cyber security education und betreibt ein Trainingszentrum. Weiters können sich User über die Homepage <http://www.waarschuwingsdienst.nl/> registrieren und Alarmierungen automatisch zugesendet bekommen.	Die Swedish Post and Telecom Agency kann folgende Strategie für die Ausbildung und Übungen im Bereich der Cybersecurity aufweisen: - Eine Schriftenreihe über den Schutz für Information Security ist auf der Hompage der MSB (<www.msb.se/en/Prevention/>) einzusehen, welche auch für den Katastrophenschutz zuständig ist. - In 2011 wurde der "National Response Plan for Serious IT Incidents", welcher kooperative Ansätze mit der Industrie und anderen Einrichtungen zur Minimierung der Störung beschreibt, veröffentlicht.	Die Slovak Association for Information Security (SASIB) hat als Ziel das rechtlichen Bewusstsein und Know-How betreffend Informationssicherheit und Softwareschutz seiner Mitglieder – im professionellen und öffentlichen Bereich – zu unterstützen. Trainingskurse werden auch vom SCIRT.SK laut Internetseite <https://www.csirt.gov.sk> angeboten.

Themenbereich	Niederlande	Schweden	Slowakei
9. Wie erfolgt die Forschung und Entwicklung?	Durch den National Cyber Security Council erfolgt die Koordination von Forschungsprogrammen zwischen Institutionen und der Privatwirtschaft.	Forschung erfolgt im öffentlichen Sektor u.a. in der Swedish Defence Research Agency (FOI), einer führenden europäischen Forschungseinrichtungen im Verteidigungs- und Sicherheitsbereich. FOI entwickelt auch Systeme für das Krisenmanagement im Zusammenhang mit schweren Unfällen und Katastrophen. Als Beispiel ist das laufende Projekt SCADA (Supervisory Control and Data Acquisition) zu nennen, welche die Erforschung der Sicherheit industrieller Steuerungs- und Überwachungssysteme beinhaltet.	Forschung und Ausbildung erfolgen u.a. auf folgenden Universitäten: - Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University - Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava - Faculty of Electrical Engineering and Informatics, Technical University of Kosice

Themenbereich	Niederlande	Schweden	Slowakei
10. Wie erfolgt der Schutz kritischer Infrastrukturen?	Das Centre for Protection of National Infrastructure (CPNI) ist eine Plattform, auf der kritische Sektoren und öffentliche Stellen Informationen in einer vertrauenswürdigen Umgebung über Vorfälle, Bedrohungen, Schwachstellen und gute Praktiken in den Bereichen Cybercrime und Cybersicherheit teilen können. Ziel ist die Erhöhung der Widerstandsfähigkeit gegen Störungen insbesondere im Energiesektor (EyeforEnergie). Das AIVD's (General Intelligence and Security Service) National Communications Security Agency (NBV) fördert den Schutz von speziellen Informationen durch die Bereitstellung und Unterstützung bei der Implementierung genehmigter Security-Produkte, erstellt Vorschriften und Standards und ist beratend zum Thema Informationssicherheit tätig.	Die National Telecommunications Coordination Group (NTSG) wurde im August 2005 gegründet und ist eine freiwillige Kooperationsplattform zur Unterstützung der Wiederherstellung der nationalen Infrastruktur für die elektronische Kommunikation im Zusammenhang mit außergewöhnlichen Ereignissen in der Gesellschaft. Das Kriterium für die Mitgliedschaft bei der NTSG ist, dass Betreiber/Organisationen, die in Schweden kritische Infrastrukturen für elektronische Kommunikationsmittel betreiben, ihre eigenen technischen Ausrüstungen, Fähigkeiten oder Ressourcen mit einbringen müssen.	Der Schutz kritischer Informationsinfrastruktur ist Aufgabe von CSIRT.SK (governmental Computer Security Incident Response Team), welche auch nationale Übungen in diesem Bereich durchführt

Tabelle 5: Cybersecurity - Vergleichstabelle Niederlande, Schweden, Slowakei
Alfred Gulder

3.4 Rechtsanwaltskanzleien als Beispiel hybrider Bedrohung

Christoph R. Cede

Die zunehmende Hybridität der Interaktionen von Akteuren zeichnet ein vollkommen neues Bild von Konflikten, im Zuge dessen das gebräuchliche Bedrohungsbild überdacht werden sollte. Die Kombination von militärischen und nicht-militärischen Mitteln wird in Zukunft eine noch größere Rolle spielen als bisher. Es verschwimmen die Grenzen zwischen Aggression und Wettbewerb, zwischen Gewaltanwendung und (scheinbarer) Gewaltlosigkeit.

Um in diesem sich abzeichnenden komplexen Umfeld als Akteur die Lage korrekt beurteilen zu können, ist es wichtig, vernetzt zu denken und dementsprechend auch ressortübergreifend zu handeln. Große Staaten mit aggressiver Außenpolitik, wie z.B. Russland[1], haben dies bereits erkannt und richten ihre Handlungen bereits danach aus. Im Folgenden wird das Wesen der Hybridität daher am Beispiel chinesischer Cyber-Angriffe veranschaulicht und gezeigt, wie unkonventionelles Denken und Kreativität China einen erheblichen Vorteil gegenüber den USA einräumen.

3.4.1 Warum Kanzleien?

Das Verhältnis USA - China ist geprägt von Konkurrenz und fortwährendem diplomatischen Dialog, wobei der „*U.S.-China Strategic and Economic Dialogue*" eine wichtige Rolle einnimmt. Es sollen in dauerhaften Verhandlungen Interessen abgestimmt werden und so für beide Seiten positive Ergebnisse erzielt werden.[2] Gleichzeitig ist es offensichtlich, dass das aufstre-

---

1 Gerasimov V. zitiert nach Galeotti, Mark: The 'Gerasimov Doctrine' and Russian Non-Linear War. <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>, abgerufen am 15.06.2015.

2 The White House, Office of the Press Secretary: Statement on Bilateral Meeting with President Hu of China. 01.04.2009.

bende China und die Weltmacht USA oft widerstrebende Interessen haben und dadurch Konfliktpotential besteht.

Im privaten Sektor der USA sind Abwehraktionen gegen chinesische Industriespionage[3] seit Jahren üblich[4], wobei diese nicht mehr direkt sondern in hybrider Form betrieben wird. In der Vergangenheit war die Absicht von Industriespionage oft geistiges Eigentum zu erwerben, um sich so einen Wettbewerbsvorteil zu verschaffen. Jedoch wird jetzt zusätzlich ein verstärktes Augenmerk darauf gelegt den Konkurrenten direkt zu schädigen.

Die chinesische Regierung betraut private Hacker, wie etwa die Gruppe Deep Panda, oder direkt das chinesische Militär damit, Daten bestimmter Anwaltskanzleien durch Cyber-Angriffe abzusaugen. Die hiervon betroffenen Anwaltskanzleien vertreten und beraten Ausländer in Verhandlungen mit chinesischen Unternehmen. Da die Sicherheitsvorkehrungen der unmittelbaren Verhandlungspartner aufgrund von Erfahrungen mit Industriespionage in der Regel sehr hoch sind, werden deren Anwälte als nächstbestes Ziel ausgewählt.[5]

---

3 Der Begriff "Industriespionage" ist bisweilen umstritten. Gemeint ist das Vorgehen eines Staates gegen ein Unternehmen. Bei Wirtschaftsspionage ist das Ziel, allgemeine volkswirtschaftliche Daten aus dem staatlichen Bereich zu erwerben. Vgl. zur Diskussion Cede, Christoph: Industrial Espionage under Public International Law: A Legal Smoke and Mirrors Game. In: Journal for Intelligence Propaganda and Security Studies 1/2015, S. 70ff, hier S. 71; Cede, Christoph: Völkerrechtliche Betrachtungsweisen staatlicher Industriespionage. Diplomarbeit, Karl-Franzens Universität Graz 2015, S. 9f; Sule, Satish: Spionage: Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage. Saarbrücken 2005, S. 30.

4 U.S. said to be target of massive cyber-espionage campaign. In: The Washington Post, 10.02.2013. <http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html>, abgerufen am 16.07.2014.

5 Paller, Alan: Conversations About Cybersecurity. SANS Institute. The Diplomat: China Expands Cyber Spying; The Diplomat: Why Are Chinese Cyberspies Targeting US Think Tanks? <http://www.sans.org/security-resources/cybersecurity-conversations>, abgerufen am 09.08.2014.

Aufgrund der Struktur großer Kanzleien (Lawfirms), deren Arbeitsweise, der oft anzutreffenden Trägheit in Bezug auf den Umgang mit IT und der daraus resultierenden relativ niedrigen Sicherheit gegenüber Cyber-Angriffen stellen diese ein leichteres Ziel als ihre Klienten dar. Partner haben innerhalb der streng hierarchisch organisierten Kanzleien großen Einfluss und ihre Entscheidungen werden kaum in Frage gestellt. Auch wird infolge großen Zeitdrucks oft von zu Hause aus oder auf Dienstreisen gearbeitet, weswegen vertrauenswürdige Klientendaten im Intranet von Kanzleien im Umlauf sind oder per E-Mail verschickt werden. Dies erhöht die Anfälligkeit gegenüber Cyber-Angriffen.[6]

Kanzleien sind somit ein lohnendes Ziel für Spionage, da Hacker aufgrund der erlangten Unterlagen Zugang zu vertraulichen Informationen haben und dadurch im Vorfeld von Verhandlungen den Handlungsspielraum und daher die Verhandlungsstrategie des Gegenüber erkennen können. Dadurch verschafft die chinesische Regierung gewissen chinesischen Unternehmen in Verhandlungen mit ausländischen Konkurrenten einen immensen Vorteil und schädigt deren Gegenüber.[7]

Regierungen reagieren darauf mit einem Aufruf an Kanzleien, bedrohliche Cyber-Attacken zu melden; in Großbritannien wurde sogar eine dementsprechende Verpflichtung diskutiert[8]. Ein diesbezüglicher an die Öffentlichkeit gelangter Bericht würde jedoch immense nachteilige Konsequenzen für die berichtende Kanzlei nach sich ziehen, wie z.B. Schadenersatzklagen,

---

6 Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, S. 48ff, hier S. 52 und 54; Ames, Jonathan: Cyber security: Lawyers are the weakest link. In: The Lawyer, 28.10.2013. <http://www.thelawyer.com/analysis/cyber-security-lawyers-are-the-weakest-link/3011315.article>, abgerufen am 15.07.2014.

7 Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31.01.2012. <http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms> abgerufen am 16.07.2014; Mintz, M.: Cyberattacks on Law Firms-a Growing Threat. In: Martindale-Hubell-Blog, 19.03.2012. <http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat>, abgerufen am 09.08.2014.

8 Big businesses should reveal cyber attacks, says Labour's defence spokesman. In: The Independent, 31.03.2014. <http://www.independent.co.uk/news/uk/politics/big-businesses-should-reveal-cyber-attacks-says-labours-defence-spokesman-9210260.html>, abgerufen am 15.07.2014.

da diese das Vertrauensverhältnis zum Klienten nicht ausreichend geschützt hätte und in weiterer Folge Wettbewerbsnachteile. Daher informieren Regierungen der betroffenen Staaten in Anwaltskreisen über die Gefahr und schaffen ein Risiko-Bewusstsein durch entsprechende regelmäßige Warnungen und Kooperationen mit den Rechtsanwaltskammern.[9]

3.4.2 Der staatliche Bereich

All dies berührt jedoch nur den privaten Sektor. Um daraus eine hybride Bedrohung herleiten zu können, stellt sich die Frage, inwieweit der staatliche Bereich davon betroffen ist und für ihn negative Konsequenzen eintreten. Von derartigen Cyber-Attacken gegen Anwaltskanzleien kann ein Staat auf zwei Arten bedroht werden: mittelbar und unmittelbar. Unmittelbar würde konkret bedeuten, dass der Staat selbst Klient der Kanzlei ist oder wenn das von der angegriffenen Kanzlei vertretene Unternehmen für den bedrohten Staat systemrelevant wäre oder im (Teil-)Eigentum des Staates stünde. Eine mittelbare Bedrohung ist viel abstrakter; es liegt in ihrer Art, dass der bedrohende Akteur nur indirekte Folgen intendiert.

Inwieweit im vorliegenden Fall China die USA wirklich unmittelbar bedroht, ist aufgrund der Quellenlage nicht feststellbar. Es finden sich jedoch die nachstehend aufgezeigten Muster, die abseits bereits bestehender Meinungen in U.S.-Sicherheitskreisen den Schluss nahelegen, dass Angriffe auf ausländische Kanzleien von der chinesischen Zentralregierung orchestriert werden. Es ist ständig zu beachten, dass China neben Russland der wahrscheinlichste Herausforderer der amerikanischen Vormachtstellung ist und

---

9 Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31.01.2012. <http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms> abgerufen am 16.07.2014; FBI Warns Of Spear Phishing Attacks On U.S. Law Firms and Public Relations Firms. In: Dark Reading, 18.11.2009. <http://www.darkreading.com/vulnerabilities---threats/fbi-warns-of-spear-phishing-attacks-on-us-law-firms-and-public-relations-firms/d/d-id/1132421?>, abgerufen am 14.07.2014; Mintz, M.: Cyberattacks on Law Firms-a Growing Threat. In: Martindale-Hubell-Blog, 19.03.2012. <http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat>, abgerufen am 09.08.2014.

dennoch ständig in Verhandlungen mit den USA steht, nicht zuletzt aufgrund des fortwährenden „*U.S.-China Strategic and Economic Dialogue*". Jegliche Stärkung der chinesischen Position bedeutet daher eine Schwächung der amerikanischen. In diesem Fall ist die mittelbare Bedrohung ein Erstarken des Gegners, auf wessen Rechnung auch immer.

Es besteht ausreichend Grund zu Annahme, dass die chinesische Regierung Angst vor übermäßigem ausländischem Einfluss in ihrem Land hat, denn die Angriffe sind keineswegs nur gegen U.S.-amerikanische, sondern vielmehr auch gegen britische und kanadische Kanzleien gerichtet. Hybride Bedrohungen können auch unbeabsichtigte Folgen haben und es gilt daher nicht mehr in Begriffen von Aktion und Reaktion, sondern vielmehr vernetzt zu denken. Darum bleibt nur, lediglich Muster aufzuzeigen, die nahelegen, dass Cyberaktivitäten China zuzurechnen sind, indem diese Handlungen zu chinesischen Interessen in Relation gesetzt werden.

China erfährt zur Zeit eine Aufschwungsphase. Die Wirtschaft wächst, auch wenn Wachstumszahlen im Vergleich zu vergangenen Jahren leicht rückläufig sind, ebenso wie die Bevölkerung. Politisch werden Ambitionen gehegt, mittelfristig zu einer regionalen Hegemoniemacht im Pazifik aufzusteigen. Die wachsende Bevölkerung muss zum einen versorgt werden, zum anderen stützt sich die chinesische Regierung bisweilen auch auf repressive Maßnahmen, um Unruhen unter Kontrolle zu bekommen. Die chinesische Volkswirtschaft hat aufgrund ihrer Größe und ihrer steigenden Konjunktur verstärkten Bedarf im Gesundheitswesen, in der Umwelttechnologie und Nahrungsmittelindustrie[10] ebenso wie an Rohstoffen oder Kommunikations- und Transportinfrastruktur.

Um diesen Bedarf zu decken, ist China zumindest in absehbarer Zukunft von Importen und daher auch von guten Beziehungen zu seinen strategischen Partnern und Nachbarn abhängig. Dies ist jedoch ein schwieriger Balanceakt, da regionale Hegemonie sich kaum mit friedlicher Entwicklung vereinbaren lässt. Die neue Führung in Peking, die seit November 2012 im

---

[10] Shuanghui wraps up Smithfield deal, China's largest US takeover. In: China Daily, 26.09.2013. <http://usa.chinadaily.com.cn/business/2013-09/26/content_16995767.htm>, abgerufen am 16.07.2014.

Amt ist, hat daher einen aggressiveren Weg in der Außenpolitik eingeschlagen als die vorangegangene. So wurde etwa eine Staats-Sicherheits-Kommission gegründet, und der Senkaku-Konflikt mit Japan wurde auch von China weiter angeheizt. Gemeinsam mit einem aggressiveren Auftreten der Volksbefreiungsarmee macht eine solche Politik zurückhaltende Diplomatie schwer möglich. Folge davon sind schlechtere Beziehungen zu den Nachbarn Chinas, die Angst davor haben, dass ein chinesischer Aufstieg auf ihre Kosten gehen könnte und daher geneigt sind, sich an die USA als Schutzmacht zu wenden. China versucht dies mit allen Mitteln zu verhindern und hat daher das *„Friedliche Entwicklung-Programm"* ins Leben gerufen.[11]

3.4.3 Gezielte Angriffe

Diese Situation gibt den Rahmen vor, innerhalb dessen das Bild der Cyber-Angriffe zu zeichnen ist. Die Meldungen über angegriffene Kanzleien sind zum Teil eindeutig, da einige Kanzleien Angriffe auf sie bestätigen, zum Teil existieren aber auch nur starke Hinweise, wie z.B. eine abrupte Verstärkung eines vormals unzureichenden Cybersicherheitssystems oder eine häufige Nennung einer Kanzlei bei einschlägigen Veranstaltungen ohne jeglichen Beweis eines Angriffs. Ob ein Angriff erfolgreich war oder nicht, spielt bei der Frage nach der Koordinierung im Grunde keine Rolle. Laut Medienberichten existieren unterschiedliche Angaben zur Zahl der Angriffe: sieben erfolgreiche Angriffe auf wichtige kanadische Kanzleien im September 2010[12], 80 Kanzleien in New York im Jahre 2011[13], tausende erfolg-

---

11 China's foreign policy faces acute challenges. In: The Daily Star, 25.07.2014. <http://www.dailystar.com.lb/Opinion/Commentary/2014/Jul-25/265049-chinas-foreign-policy-faces-acute-challenges.ashx>, abgerufen am 15.08.2014; Paal, D.: Contradictions in China's Foreign Policy. In: Carnegie Endowment, 13.12.2013. <http://carnegieendowment.org/2013/12/13/contradictions-in-china-s-foreign-policy>, abgerufen am 11.08.2014.

12 Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, S. 48ff, hier S. 50.

13 Mandiant Corporation, zitiert nach M Melnitzer J.: Law Firms: Cyber Target #1. In: Lexpert Magazine April 2013, S. 48ff, hier S. 50.

lose Versuche in Ontario im Jahre 2013[14] etc. Es lassen sich sogar einige angegriffene Kanzleien genauer identifizieren. Aufschluss über das Interesse der chinesischen Regierung an ihnen gewinnt man, wenn man ihre Tätigkeitsfelder im Zusammenhang mit der Zeit der Cyber-Angriffe betrachtet.

Im Jänner 2010 lassen sich die ersten Cyber-Angriffe auf Anwaltskanzleien festmachen. Die angegriffene U.S.-amerikanische Kanzlei ließ eine Woche zuvor verlautbaren, dass sie das amerikanische Unternehmen CYBERsitter in einer 2,2 Mrd. U.S. Dollar-Schadenersatzklage gegen die chinesische Regierung vertrete. Der Grund: CYBERsitter behauptete, dass Zensur-Filterprogramme, die von der chinesischen Regierung entwickelt und gesetzlich für User in China vorgeschrieben worden sind, über 3.000 Zeilen plagiierter Codes enthielten.[15] Somit handelt es sich hierbei um eine Urheberrechtsfrage. Vom analytischen Standpunkt liegt noch wenig vernetztes Denken vor: Ein Privater geht gegen die Regierung vor, die daraufhin vermutlich die Vertretung des Privaten hackt.

Der zweite Fall vom Jänner 2010 ist ähnlich simpel. Eine internationale Anwaltskanzlei, deren Wurzeln in den USA liegen, beriet die „1st Amendment Coalition" – eine Gruppe mit der Auffassung, dass Chinas Internet-Regulierung eine Verletzung von WTO-Recht darstellt[16]. Auch hier erfolgt die Reaktion Chinas linear und ist, wie im zuvor geschilderten Fall, kaum als Bedrohung aufzufassen: Eine private Interessensgruppe ist der Meinung, dass der chinesische Staat widerrechtlich handelt und versucht seine Auffassung rechtlich zu fundieren. Chinesische Hacker greifen daraufhin

---

14 Cybercrime and law firms: The risks and dangers are real. In: LawPRO Magazine 2013 Vol.12 no.4, 2013, S. 6ff, hier S. 6.

15 China and the Law: Did Chinese Hackers Attack LA Law Firm? In: The Wall Street Journal Law Blog, 14.01.2010. <http://blogs.wsj.com/law/2010/01/14/china-and-the-law-did-chinese-hackers-attack-la-law-firm/>, abgerufen am 11.08.2014; L.A. Law Firm Reports Cyber Attacks. In: The Wall Street Journal, 15.01.2010. <http://www.wsj.com/articles/SB10001424052748704363504575002301498625456> , abgerufen am 15.07.2014.

16 Kelly F. in einem Interview mit Kaplan G., Australian Broadcasting Cooperation, zitiert nach King & Spalding: The Great Wall of China. 27.01.2010. <http://www.kslaw.com/News-and-Insights/NewsDetail?us_nsc_id=150>, abgerufen am 11.08.2014.

dessen Rechtsbeistand, der sich u.a. auf Industriespionage spezialisiert hat, an[17].

Ein halbes Jahr später, im September 2010, ereignete sich der nächste umfassendere Angriff auf kanadische Regierungseinheiten, Think Tanks, und sieben große Rechtsanwaltskanzleien in Toronto[18]. Im November 2010 erfolgte ein Aufsehen erregendes Angebot, das im Jänner 2011 nach rechtlichen Schwierigkeiten endgültig aus steuerlichen Gründen und teilweise aufgrund des Widerstandes von Politik und Zivilgesellschaft vereitelt wurde: BHP Billiton, das weltgrößte Minen-Unternehmen, wollte Potash Corporation, den weltgrößten Düngemittelerzeuger, feindlich übernehmen.[19] Im November 2011, also gut ein Jahr später, gelangten Experten zur Überzeugung, dass der Angriff nur zur Verschleierung des tatsächlichen Zieles – nämlich der beiden Kanzleien, die die Parteien vertraten – diente[20]. Demnach waren von den sieben angegriffenen Kanzleien nur zwei tatsächliche Ziele. Die ehemals in chinesischem Staatseigentum stehende Sinochem-Gruppe beauftragte die Deutsche Bank und Citigroup im September 2010, also im Monat des Angriffes, herauszufinden, wie die geplante Übernahme bestmöglich verhindert werden könnte. Zum Zeitpunkt des Angriffs herrschte in der chinesischen Volkswirtschaft erhöhter Bedarf an Agrochemikalien. Anfragen an die chinesische Botschaft dazu wurden nicht sofort beantwortet.[21]

---

17 Law Firms Under Siege. In: Dark Reading, 04.06.2011. <http://www.darkreading.com/attacks-breaches/law-firms-under-siege/d/d-id/1135516?>, abgerufen am 05.09.2014.

18 Weston, Greg: Foreign hackers targeted Canadian firms. CBC news, 29.11.2011. <http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810>, abgerufen am 03.09.2014.

19 Jones, Day: Potash Corporation of Saskatchewan successfully defends historic $43.1 billion hostile takeover bid. Jänner 2011. <http://www.jonesday.com/potash-corporation-of-saskatchewan-successfully-defends-historic-431-billion-hostile-takeover-bid/>, abgerufen am 11.08.2014.

20 Weston, Greg: Foreign hackers targeted Canadian firms. CBC news, 29.11.2011. <http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810>, abgerufen am 03.09.2014.

21 Riley, Michael A./Pearson, Sophia: China-Based Hackers Target Law Firms to Get Secret Deal Data. In: Bloomberg Business, 31.01.2012.

Als Fazit bleibt: Zwei ausländische private Wettbewerbsteilnehmer wollen miteinander einen Vertrag abschließen und China sieht seine Interessen gefährdet, weswegen es versucht, den Vertrag zu sabotieren. Dies ist im Vergleich zu den beiden vorherigen Fällen schon eher als Bedrohung Kanadas einzustufen, da mit Sicherheit die kanadische Volkswirtschaft aufgrund des Volumens der Verhandlungen (40 Mrd. $[22]) in ihrer Gesamtheit betroffen war. Auch wenn China prima facie nicht von den Verhandlungen betroffen war, so hat es dennoch ein wesentliches Interesse daran, dass seine ständig wachsende Bevölkerung nicht mit einer Nahrungsmittelknappheit (Potash Corporation ist er weltgrößte Düngemittelproduzent) konfrontiert wird.

Im Juli 2011 kam es wieder zu einer Angriffsserie. Diesmal konnte genau erfasst werden, wann die Angriffe stattfanden. Die Serie verteilte sich auf den Zeitraum zwischen 29. Juni 2011 und 21. Juli 2011, wobei kein einziger Angriff an einem Wochenende stattfand. Dies lässt auf professionelle vollzeitbeschäftigte Hacker schließen. Zwei von neun Angriffen in diesem Zeitraum waren gegen Kanzleien gerichtet, wobei unter den Opfern etwas mehr als ein Viertel Anwälte waren. Eine betroffene Kanzlei beriet U.S.-Unternehmen, vertrat Interessen in internationalen Handelsfragen und hat darüber hinaus aktiv chinesische Export-Restriktionen auf Rohstoffe vor dem Office of the United States Trade Representative und der WTO angesprochen[23]. Ihre betroffenen Anwälte waren allesamt im internationalen Handelsrecht tätig. Die betroffenen Anwälte der anderen Kanzlei beschäftigten sich mit geistigem Eigentum und Urheberrecht und hielten Vorträge über China.[24] In diesem Fall waren die Angriffe somit gegen Kanzleien

---

<http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms> abgerufen am 16.07.2014.

22 Ebd.

23 Price A./Brightbill T./El-Sabaawi L: WTO Panel Says China's Raw Materials Export Restrictions Violate WTO Obligations. Wiley Rein, 05.06.2011. <http://www.wileyrein.com/publications.cfm?sp=articles&id=7192>, abgerufen am 11.08.2014.

24 Whiteaker, Chloe: China Hackers Activity Logged Reveals Multiple Victims Worldwide. In: Bloomberg Online, 25.07.2012. <http://go.bloomberg.com/multimedia/china-hackers-activity-logged-reveals-multiple-victims-worldwide/>, abgerufen am 04.08.2014.

gerichtet, die unter Umständen chinesische Interessen direkt und nicht nur als Vertretung für ihre Klienten behindern könnten.

Danach kam es wiederholt zu kleineren Angriffen, wobei die strategischen Ziele nicht genau eruierbar sind. Vier Kanzleien, die im Oktober 2013 einräumten, wiederholt Ziel von Angriffen zu sein[25], waren jedoch im Zeitraum davor in nennenswerte Aktivitäten involviert.

Stewart Baker, ehemaliger Assistant Secretary im Department of Homeland Security, wurde im Februar 2013 in Bezug auf U.S.-Regierungsarbeit, die im Zusammenhang mit Cyberattacken und einem härteren U.S.-Standpunkt gegenüber China steht, von Medien zitiert[26]. Im März 2013 zitierte Reuters Phil West, einen ehemaligen Berater im Treasury Department, in einem Artikel, der ein Steuerabkommen zwischen den USA und China als „elusive" bezeichnet[27]. Im April 2013 investierte Kuwait Petroleum in einem Joint Venture mit Sinopec, einem der größten chinesischen Mineralölunternehmen, in der Guangdong-Provinz[28] und wurde in den Verhandlungen von einer der vier angegriffenen Kanzleien vertreten. Auch wurde im April Stewart Baker noch einmal zitiert; dieses Mal ging es um das Verbot der U.S.-Bundesregierung, IT von chinesischen, (ehemals) staatsnahen Unternehmen zu erwerben. Dieses Verbot wird mit chinesi-

---

25 Greengard, Samuel: Law Firm Defends Itself Against Cyber-Threats. In: Baseline, 08.11.2013. <http://www.baselinemag.com/security/law-firm-defends-itself-against-cyber-threats.html>, abgerufen am 05.08.2014; Benzing, Jeffrey: Law Firms 'Low-Hanging Fruit' for Cyber Thieves. In: Main Justice, 01.11.2013. <http://www.mainjustice.com/2013/11/01/law-firms-low-hanging-fruit-for-cyber-thieves/>, abgerufen am 06.08.2014; Ames, Jonathan: Top City firm fights off cyber attack. In: The Lawyer, 28.10.2013. <http://www.thelawyer.com/analysis/the-lawyer-management/top-city-firm-fights-off-cyber-attack/3011549.article>, abgerufen am 27.07.2014.

26 Steptoe & Johnson: Associated Press Quotes Stewart Baker on Chinese Cyberattacks on US. 05.02.2013, <http://www.steptoe.com/news-1333.html>, abgerufen am 12.08.2014.

27 Temple-West,Patrick/Lee, Yimou: U.S.-China anti-tax evasion deal seen as crucial, but elusive. In: Reuters, 14.03.2013. <http://in.reuters.com/article/2013/03/13/usa-tax-fatca-idINL1N0BYH9520130313>, abgerufen am 12.08.2014.

28 Ling S./Zhou O.: Petrodollars: the Sinopec-KPC refinery is hitting some rough spots. In: The Barrel, blog, 15.04.2013. <http://blogs.platts.com/2013/04/15/sinopec-kpc/>, abgerufen am 12.08.2014.

scher Cyberspionage in Verbindung gebracht.[29] Im Mai 2013 beriet eine der angegriffenen Kanzleien PAI Partners beim Verkauf der FTE Automotive GmbH an Bain Capital. Über den genauen Kaufpreis haben die Parteien Stillschweigen vereinbart.[30] Im Juli 2013 wurde Spreadtrum Communications in der 1,78 Mrd. $-Übernahme durch Tsinghua Unigroup (einem staatsnahen chinesischen Drahtlos-Kommunikation-Hersteller) von einer angegriffenen Kanzlei vertreten[31]. Eric Emerson, Anwalt bei derselben Kanzlei, die seit Februar schon dreimal in den Medien im Zusammenhang mit Expertenmeinungen zu China zitiert worden war, sprach im Juli 2013 in Washington über „Perspectives on the U.S.-China Investment Relationship"[32].

Im September 2013 kaufte Shuanghui den weltgrößten Schweineproduzenten Smithfields. Dies stellt bis dahin die größte Übernahme durch ein chinesisches Unternehmen (4,7 Mrd $) dar, wobei eine der angegriffenen Kanzleien federführend mitwirkte[33]. Ein Anwalt derselben Kanzlei, deren Anwälte wiederholt in der Presse als Experten zitiert wurden, meinte dazu, dass die U.S.-Regierung dieser Übernahme wahrscheinlich zustimmen wer-

---

29 Steptoe & Johnson: Media Quotes Stewart Baker on US Ban on Chinese IT Equipment. 09.04.2013, <http://www.steptoe.com/news-1408.html>, abgerufen am 12.08.2014.

30 Clifford Chance: Clifford Chance advised PAI Partners on the Sale of FTE Automotive GmbH. 14.05.2013. <http://www.cliffordchance.com/news/news/2013/05/clifford_chance_advisedpaipartnersonthesaleoffteautomotivegmbh.html>, abgerufen am 12.08.2014.

31 Fenwick & West: Fenwick & West is Representing Spreadtrum Communications in its Acquisition by Tsinghua Unigroup for $1.78B. 12.07.2013. <http://www.fenwick.com/experience/Pages/Fenwick-Represents-Spreadtrum-Communications-in-its-Announced-Acquisition-by-Tsinghua-Unigroup-for-$1.78B.aspx>, abgerufen am 12.08.2014.

32 Steptoe & Johnson: Perspectives on the US-China Investment Relationship, Global Business Dialogue Members' Lunch. 18.07.2013. <http://www.steptoe.com/news-events-2477.html>, abgerufen am 12.08.2014.

33 Allen & Overy: IFLR Americas' M&A Deal of the Year award for Shuanghui's acquisition of Smithfield Foods. 09.04.2014. <http://www.allenovery.com/news/en-gb/articles/Pages/IFLR-Americas%E2%80%99-MA-Deal-of-the-Year-award-for-Shuanghui%E2%80%99s-acquisition-of-Smithfield-Foods-.aspx>, abgerufen am 12.08.2014.

de[34]. Eine andere der vier Kanzleien beriet im September 2013 Carlyle Asia Growth Partners IV bei einem 365 Mio. HK$-Investment in Tenwow International Holdings, einen der größten Fertignahrung-Produzenten Chinas[35], und außerdem AMP Capital bei einem Joint Venture mit einer Tochter von China Life Insurance China access to China (Group) Company, der weltgrößten Versicherungsgesellschaft (gemessen am Kapital)[36]. Dieselbe Kanzlei beriet im Oktober 2013 auch Siemens beim Verkauf der TLT-Turbo GmbH an Power Construction Corporation of China. Über den Kaufpreis haben die Parteien Stillschweigen vereinbart.[37]

Eine der betroffenen Kanzleien hat einen breiten Angestelltenkreis mit Regierungserfahrung und tritt in den Medien China gegenüber kritisch auf. Die drei anderen vertraten in Verhandlungen mit chinesischen Unternehmen die ausländische Seite, wobei die betroffenen Sektoren – Treibstoff, Automobilindustrie, Kommunikationstechnologie, Nahrung, Gesundheitsversorgung und Umwelttechnologie – allesamt aufgrund der großen Bevölkerungsanzahl im strategischen Interesse der chinesischen Volkswirtschaft und dadurch auch der Pekinger Regierung liegen.

Es bleibt also in allen angeführten Fällen festzustellen, dass die genau determinierbaren Cyber-Angriffe auf jene Kanzleien geführt wurden, die zum

---

34 US likely to clear $4.7bn Smithfield deal. In: The Financial Times, 05.09.2013. <http://www.ft.com/intl/cms/s/171c3046-15b6-11e3-b519-00144feabdc0,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F171c3046-15b6-11e3-b519-00144feabdc0.html%3Fsiteedition%3Dintl&siteedition=intl&_i_referer=>, abgerufen am 05.08.2014.

35 Clifford Chance: Clifford Chance advises Carlyle on HK$365 million cornerstone investment in Tenwow International Holdings. 30.09.2013. <http://www.cliffordchance.com/news/news/2013/09/clifford_chance_advisescarlyleonhk365millioncornerstoneinvestmen.html>, abgerufen am 12.08.2014.

36 Clifford Chance: Clifford Chance advises AMP Capital on China funds management joint venture with China Life. 05.09.2013. <http://www.cliffordchance.com/news/news/2013/09/clifford_chance_advisesampcapitalonchinafundsmanagementjointvent.html>, abgerufen am 12.08.2014.

37 Clifford Chance: Clifford Chance advises Siemens AG on the sale of TLT-Turbo. 29.10.2013. <http://www.cliffordchance.com/news/news/2013/10/clifford_chance_advisessiemensagonthesaleoftlt-turbo.html>, abgerufen am 12.08.2014.

Zeitpunkt des Angriffes auf einem Gebiet tätig waren, das mit China in einem Zusammenhang steht. Traten die Cyber-Attacken anfangs nur gezielt gegen jene Kanzleien auf, die gegen China vorgingen, so wurden rasch auch andere angegriffen, um die wahren Ziele zu verschleiern.

Nicht nur die Anzahl der Ziele, sondern auch die Komplexität der Angriffe nahm zu; es wurde versucht, die identifizierten außenpolitischen Ziele durch ein erhöhtes Maß an Kreativität zu erreichen. Waren anfangs die Angriffe direkt gegen einen juristischen Gegner Chinas gerichtet, so ist in jüngerer Zeit zu konstatieren, dass die Ziele der Cyber-Angriffe oft nur mittelbar Chinas volkswirtschaftlichen Interessen im Wege standen. Neben der Anzahl der Ziele und der Komplexität der gezielt geführten Angriffe nahm auch deren Häufigkeit zu. Dabei ist zu beachten, dass der Führungswechsel in der chinesischen Regierung im November 2012 von einem Aussetzen der Angriffe und einem Schwenk in Richtung aggressivere Außenpolitik[38] begleitet wurde. Die Anzahl der gezielten und mittels öffentlich zugänglicher Information nachvollziehbaren Angriffe (ohne Finten) stieg unmittelbar danach, im Zeitraum Jänner bis März 2013, sprunghaft an. Es konnten nur bis November 2013 Daten gefunden werden, die auf gezielte Angriffe schließen lassen.[39]

---

[38] China's foreign policy faces acute challenges. In: The Daily Star, 25.07.2014. <http://www.dailystar.com.lb/Opinion/Commentary/2014/Jul-25/265049-chinas-foreign-policy-faces-acute-challenges.ashx>, abgerufen am 15.08.2014; Paal, D.: Contradictions in China's Foreign Policy. In: Carnegie Endowment, 13.12.2013. <http://carnegieendowment.org/2013/12/13/contradictions-in-china-s-foreign-policy>, abgerufen am 11.08.2014.

[39] Erstellt von Christoph Cede, nach Auswertung von 33 Webseiten und ausschließlich open-source (!) Meldungen, Beobachtungszeitraum: Juni-Juli 2014.

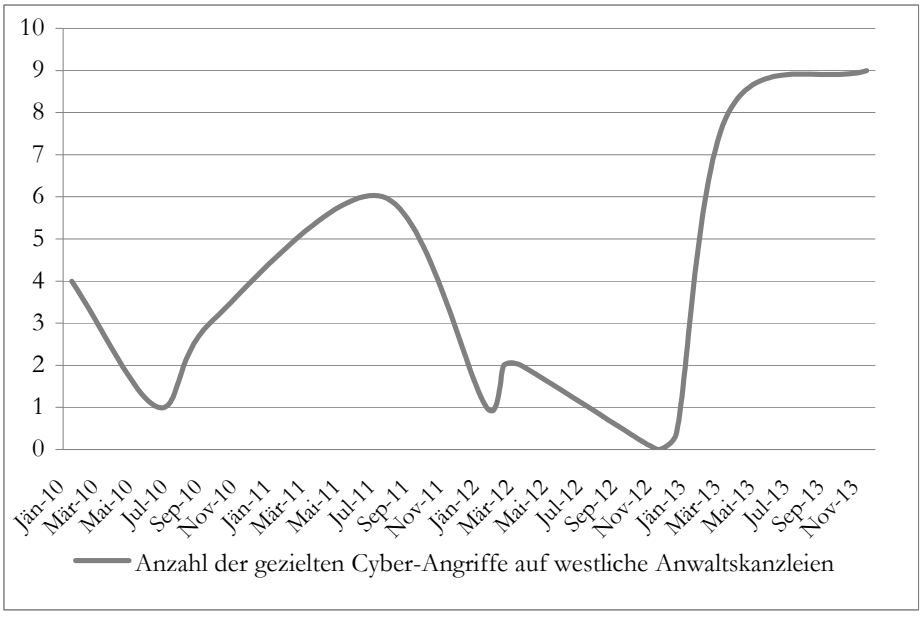


Tabelle 6: Gezielte und nachvollziehbare Cyber-Angriffe auf westliche Anwaltskanzleien
Christoph Cede

All diese Umstände legen nahe, dass hinter den Angriffen ein der chinesischen Regierung freundlich gesinnter Akteur steht, der, durch den Vorteil, den er China verschafft, die USA in ihrem Handlungsspielraum mittelbar beeinträchtigt. Auch wenn die Angriffe allein bei Weitem nicht die strategische Schwelle erreichen, die für eine hybride Bedrohung notwendig ist, so könnten sie verbunden mit diplomatischen Schachzügen und entsprechend abgestimmten Verhandlungen im „*U.S.-China Strategic and Economic Dialogue*" die USA dennoch bedrohen.

3.4.4 Ableitungen

Die Frage, die sich für Österreich und europäische Kleinstaaten stellt, ist, welche Lehren daraus zu ziehen sind. Zunächst gilt es zu klären, ob derartige Angriffe auf österreichische Kanzleien vorliegen (die Rechtsanwalts-

kammer beantwortet hierzu keine Anfragen) und ob sich diese auf ähnliche Weise zurückverfolgen lassen.

In Bezug auf Kanzleien werden von der Rechtsanwaltskammer kaum andere Schritte gesetzt werden können, als bei größeren Staaten: informieren, warnen und zur Kooperation aufrufen. Es gilt, die Bedrohung von Daten herauszustreichen und an ein gesteigertes Sicherheitsbewusstsein zu appellieren. Schlussendlich können verlorene Daten nicht nur Kanzleien sondern unter Umständen auch Österreich zum Nachteil gereichen, indem der Staat in Kombination mit einem anderen Mittel hybrid bedroht wird.

Entscheidungsträger im staatlichen Bereich (und in teilweise im Staatseigentum stehenden Unternehmen) sollten sich des vorhandenen Risikos bewusst sein, wenn Kanzleien in bilaterale Verhandlungen und vor allem unmittelbar in Vertragsabschlüsse eingebunden werden.

Sollten freiberufliche Rechtsbeistände vom Staat in ausgewählten Materien zu Rate gezogen werden, erscheint es ratsam, ein besonderes Augenmerk auf deren Sicherheitsstandard zu legen und dies den betreffenden Kanzleien auch als Erwartungshaltung an sie zu kommunizieren. Doch selbst erhöhte Sicherheit bietet nur insoweit Schutz, als Angreifer sich nicht darauf eingestellt haben. Langfristig sollten daher Strategien erarbeitet werden, wie mit einer derartigen Bedrohung umzugehen ist.

3.5 Völkerrechtliche Implikationen hybrider Bedrohungen

Christoph R. Cede,
Reinmar Nindler und
Paul Schliefsteiner

Bei den folgenden Überlegungen handelt es sich um mögliche völkerrechtliche Implikationen in Bezug auf das Konzept der „hybriden Bedrohungen". Es handelt sich lediglich um einen ersten Problemaufriss, der gewiss einer tiefergehenden Betrachtung bedarf. Dabei beschäftigt sich dieser Problemaufriss einerseits mit völkerrechtlichen Ableitungen, die bereits aus den Definitionselementen des Begriffes der „hybriden Bedrohungen" resultieren und andererseits mit möglichen völkerrechtlichen Implikationen, die sich aus dem Wesen der Hybridität von Bedrohungen ergeben.

Bereits die Definition des Konzeptes der hybriden Bedrohung enthält (völker-) rechtliche Begriffe. So ist etwa ein „Staat" im Völkerrecht durch die Drei-Elemente-Lehre nach Jellinek durch Staatsvolk, Staatsgebiet und Staatsgewalt gekennzeichnet. Hybride Bedrohungen gegenüber einem *failed state*, einem *failing state* oder einem *De-facto-Regime* könnten völkerrechtlich abweichend zu behandeln sein.

Die Zielgerichtetheit der Bedrohungshandlung kann völkerrechtlich etwa im Zusammenhang mit dem Gewaltverbot eine bedeutende Rolle spielen. Die Begriffe „Vermögen", „Potenzial" und „zeitlich abgestimmt" sind völkerrechtlich hingegen irrelevant, da in Bezug auf die völkerrechtliche Beurteilung einer Situation ausschließlich auf eine faktenbasierte Lage abzustellen ist.

Neben jenen Begriffen, welche völkerrechtlich klar definiert sind, kommen jedoch auch einige Begriffe in der Definition vor, welche völkerrechtlich in jedem Einzelfall näher betrachtet werden müssen. So ist bei einem „Akteur" zwischen staatlichen und nicht-staatlichen Akteuren streng zu unterscheiden, da diese Kategorien oftmals unterschiedliche Rechtsfolgen nach sich ziehen. Nicht-staatliche Akteure, wie z.B. bewaffnete Gruppen im Sinne des humanitären Völkerrechts, Einzelpersonen oder De-facto-Regime, sind oft einem Staat politisch zuzuordnen und in gewissen Fällen

auch rechtlich zuzurechnen. Es kann sein, dass ein bloßes Unterlassen ausreicht, um rechtlich relevante Zurechenbarkeit zu begründen, oder aber, dass eine aktive Handlung dafür vorliegen muss. Wenn eine Handlung vorliegt, ist auch zu fragen, inwieweit sie Staatenverantwortlichkeit begründet, da vom Internationalen Gerichtshof (IGH) bzw. vom Internationalen Strafgerichtshof für das ehemalige Jugoslawien (ICTY) „effective control" bzw. „overall control" gefordert werden. Es ist daher auf die Ausdifferenziertheit der Befehlskette sowie auf andere völkerrechtlich relevante Merkmale abzustellen, wobei in der Praxis auch die Frage der Beweisbarkeit bedeutend werden kann. Dies kann vor allem dann zu einem Problem werden, wenn der bedrohte Staat Maßnahmen (etwa: Retorsion oder Repressalie) ergreift und sie mit der Bedrohung durch einen Akteur, dessen Zurechenbarkeit nicht beweisbar ist, begründet. Abgesehen von der allgemein völkerrechtlich relevanten Frage der Zurechenbarkeit privater Handlungen und anderer nicht-staatlicher Handlungen, stellt sich in Bezug auf hybride Bedrohungen speziell die Frage, wie vorzugehen ist, wenn einzelne Bedrohungsebenen verschiedenen Staaten zuzurechnen sind.

Auch ist das Begriffspaar Gefährdung/Bedrohung nicht näher ausdefiniert, wobei sich hier aus völkerrechtlicher Sicht etwa die Frage der Unmittelbarkeit stellt d.h. ob die Gefährdung/Bedrohung tatsächlich vorliegt, etwa ein militärischer Angriff unmittelbar bevorsteht oder ob bloß ein hypothetisches Bedrohungspotential in der Zukunft vorhanden ist. Völkerrechtliche Konsequenzen lassen sich in keinem Fall alleine aus der Definition einer Bedrohung als „hybrid" herleiten; in Bezug auf jede völkerrechtliche Konsequenz ist immer auf den Sachverhalt im Einzelfall abzustellen. So etwa im Hinblick auf die Gewaltschwelle, welche erreicht werden muss, damit ein bewaffneter Angriff im Sinne des Völkerrechts vorliegt. In Bezug auf das eng damit verknüpfte Recht zur Selbstverteidigung ist daher auch in Bezug auf hybride Bedrohungen zu klären, inwieweit diese die völkerrechtlichen Voraussetzungen für eine völkerrechtskonforme Anwendung verschiedener Arten von Gegenmaßnahmen rechtfertigen.

Eine besondere mögliche völkerrechtliche Folge der Hybridität einer Bedrohung besteht darin, dass die Bedrohungshandlung auf manchen oder gar unter Umständen auf allen Ebenen im Einzelnen rechtskonform sein könnte, während allerdings die daraus in ihrer Gesamtheit entstehende Bedrohung völkerrechtswidrig sein könnte.

4 Zusammenfassung und Conclusio

Anton Dengg

Unsere Gesellschaft wird durch eine zunehmend stärkere Vernetzungsstruktur – in nahezu allen Lebensbereichen – immer verletzungsanfälliger. Je höher der Vernetzungsgrad von Strukturen ist, desto augenscheinlicher treten hybride Bedrohungsmöglichkeiten zutage. Die zunehmende Unsicherheit über Bedrohungen und Akteure wird auch das zukünftige Bedrohungsbild prägen. Unser Bedrohungsbild der Zukunft wird von vielfältigen Einflussfaktoren bestimmt sein, wie auch in der österreichischen Teilstrategie Verteidigungspolitik festgehalten ist.[1]

In internationalen Publikationen[2] wird allerdings vermehrt hybride Kriegsführung als neue Bedrohung thematisiert. Im gegenwärtigen Ukrainekonflikt zeigt sich jedoch, dass Auseinandersetzungen nicht nur mittels Kriegsführung im konventionellen – militärischen – Sinne ausgetragen werden, sondern auch andere vielfältige Kategorien der Machtausübung angewandt bestehen. Durch die Möglichkeit der Anwendung von staatlichen Machtprojektionsoptionen zur Beeinflussung der Handlungsfähigkeit anderer Staaten ergeben sich daher neue staatliche Bedrohungsfelder.

4.1 Zusammenfassung

Das Institut für Friedenssicherung und Konfliktmanagement (IFK) der Landesverteidigungsakademie beschäftigt sich schon seit 2011 in der Forschungsthematik „Zukünftige Konflikt- und Bedrohungsbilder" mit hybriden Bedrohungen. Schwerpunkt dabei bildet das neue, insbesondere durch technische Errungenschaften ermöglichte, staatliche Potenzial zur Ausübung von Macht auf andere Staaten. Ursprünglich stand für das IFK die

---

1 BMLVS: Teilstrategie Verteidigungspolitik, S. 5. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf>, abgerufen am 13.11.2014.

2 Z.B. Frank G. Hoffman: Hybrid Warfare and Challenges. JFQ, issue 52, 1st quarter 2009.

Möglichkeit der Machtprojektion großer Staaten (USA, Russland, China und Indien) im Zentrum des Forschungsinteresses. 2013 wählte man für eine weitere Vertiefung in die Forschungsthematik aus den industrialisierten europäischen Kleinstaaten drei mit Österreich aufgrund Struktur, Heeresgröße, Auslandsengagement etc. vergleichbare Staaten aus: die Slowakei und Schweden. Zudem sollten die ausgewählten Staaten nicht nur Ähnlichkeiten aufweisen und dadurch vergleichbar sein, sondern durchaus auch unterschiedlichen Bündnissen angehören (z.B. UNO, NATO, Bündnisfreiheit). Untersucht werden sollte demnach ebenso, ob sich die ausgewählten Staaten eventuell bei hybriden Bedrohungen eher auf Bündnispartner abstützen.

Erste Analysen im Vorfeld des Projekts „Hybride Bedrohungspotentiale und daraus resultierende sicherheitspolitische Ableitungen für Kleinstaaten" zeigten, dass zwar vermehrt Inhalte zu „hybrider Kriegsführung" („Hybrid Warfare") existierten, jedoch kaum Erkenntnisse zu hybriden Bedrohungen, welche nach Meinung des IFK über „hybride Kriegsführung" hinausgehen, vorhanden waren.

Ziel des Projekts war die Beleuchtung sicherheitspolitische Konzepte ausgewählter Kleinstaaten hinsichtlich ihrer Einschätzung zu aktuellen Bedrohungen. Erkenntnisse und Rückschlüsse vor allem in puncto Bedrohungsbilder und möglicher Schutz- bzw. Abwehrmaßnahmen sollten in Ableitungen für Kleinstaaten und insbesondere für Österreich münden. Forschungsfragen im Projekt waren:

- Wie weit werden hybride Bedrohungsmöglichkeiten auf gesamtstaatlicher Ebene erfasst und welche Strategien beziehungsweise Konzepte bestehen zu deren Bewältigung?
- Welche Bedeutung kommt der Einbettung in Sicherheitsorganisationen, z.B. der NATO zu?
- Wird eine Wechselwirkung zwischen Beteiligung am IKKM und den damit verbundenen Risiken im Entsendestaat als Bedrohung wahrgenommen und welche Auswirkungen hat dies im Rahmen der gesamtstaatlichen Sicherheitsvorsorge?

Da zu hybriden Bedrohungen kaum internationale Forschungsergebnisse vorhanden waren, musste zu Projektbeginn eine Arbeitsdefinition von „hybriden Bedrohungen" entwickelt werden. In mehreren Arbeitssitzungen

wurde schließlich das Verständnis von hybrider Bedrohung überprüft und schließlich eine Arbeitsdefinition festgelegt:

Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen.[3]

Als wesentlicher Aspekt kommt bei dieser Arbeitsdefinition hinzu, dass dabei die Bedrohungshandlung die „strategische Schwelle" eines Staates überschreiten muss. Dies ist nach dem IFK Verständnis dann der Fall, wenn die Handlungs- und Entscheidungsfreiheit eines angegriffenen Staates in substanzieller Weise einschränkt ist. Es müssen zumindest zwei Kategorien hybrider Bedrohungen angewandt werden bzw. zu deren Abwehr mindestens zwei Ministerien betroffen sein.

Der Hard- und Softpower-Ansatz von Joseph S. Nye bildete die Basis für das IFK-Projekt. Für Nye kann Macht dann ausgeübt werden, wenn man im Besitz erforderlicher Möglichkeiten oder entsprechender Ressourcen ist, um angemessenen Einfluss auszuüben.[4] Somit kann eine Bedrohung nur von jenen Akteuren ausgehen, die neben dem Willen auch die notwendigen Mittel haben, um Macht anzuwenden. Nach Nye kann durch zwei Bereiche Macht ausgeübt werden: durch Hard und Soft Power. Eine weitere Macht – Smart Power, eine Mischung aus den bereits erwähnten – kommt, so Nye, hinzu. Hard Power beschreibt Nye als eine Anreiz/Drohungs-Taktik („Karotte und Stock")[5], während er Soft Power eher als Überzeugungsarbeit zum Streben nach als ideal angesehenen Werten beschreibt. Soft Power wird dann erfolgreich angewendet, wenn ein Akteur, von den eingesetzten Argumenten überzeugt wird und diesen nacheifert. Soft Power beruht auf kulturellen und politischen Idealen sowie

---

[3] Arbeitsdefinition entwickelt durch das Institut für Friedenssicherung und Konfliktmanagement der Landesverteidigungsakademie (Dengg/Feichtinger/Schurian) in Anlehnung an: Buchbender, Ortwin/Bühl, Hartmut/Kujat, Harald/Schreiner, Karl H. und Bruzek, Oliver. Wörterbuch zur Sicherheitspolitik mit Stichworten zur Bundeswehr. Hamburg, Berlin, Bonn 2000.

[4] Vgl. Nye, Joseph S. Jr.: Soft Power. The Means to Success in World Politics. PublicAffairs 2004, p. 3.

[5] Ebd. S. 5.

auf Außenpolitik, wenn diese als legitim bewertet wird. Smart Power hingegen ist „[...] the ability to combine hard and soft power into a successful strategy."[6]

Die Thematik hybride Bedrohungen wird in dieser Publikation umfangreich unter mehreren Aspekten, mit Beispielen vertiefend, betrachtet. Bewusstseinsbildung für den Bereich hybride Bedrohungen als zukünftige Herausforderung war oberstes Ziel dieser Arbeit. Zentrale Aussagen werden aus verschiedenen Blickwinkeln zusammengefasst und mögliche Ableitungen für Sicherheitsakteure getroffen. Mit einem empirisch-analytischen Ansatz wurden im Projekt konkrete Inhalte in den Sicherheitsanalysen von zwei ausgewählten Referenzstaaten (Schweden und Slowakei) auf das Vorhandensein von hybriden Bedrohungen abgefragt und auf „weiße Flecken" identifiziert. Im Analyseteil wird kurz auch auf die österreichische Sicherheitsstrategie reflektiert und auf deren Bezug zur Thematik „hybride Bedrohungen" überprüft.

Ergebnisse der Analyse

Bisher ist diese Art von Bedrohungen in sicherheitsstrategischen Papieren noch unterrepräsentiert. Wie bereits erwähnt, befassen sich gegenwärtig sicherheitspolitische Experten vorwiegend mit dem Begriff „hybride Kriegsführung", was jedoch in die Domäne von „Hard Power" einzuordnen ist. Bei notwendigen Gegenstrategien liegt der Hauptfokus folglich eher auf einer einfachen Ursache-Wirkung-Ebene: Eine als Bedrohung eingestufte Handlung wird mit einer linearen Gegenreaktion beantwortet. So wird z.B. Terrorismus mit einer Antiterrorismusstrategie bekämpft; auf die organisierte Kriminalität wird mit entsprechenden innenministeriellen Sicherheitsstrukturen reagiert; auf Angriffe, geführt mit militärischen Mitteln, wird mit Streitkräften geantwortet. Verschiedene Wechselwirkungen komplexer Systeme und die sich daraus ergebenden sicherheitspolitisch relevanten Emergenzen sind in unseren Denkschemata kaum verankert. Bedrohungsperzeptionen sind geprägt von Hard Power-Konzepten, wor-

---

6 Nye, Joseph: Smart Power. The Blog. <http://www.huffingtonpost.com/joseph-nye/smart-power_b_74725.html>, abgerufen am 29.11.2014.

auf die notwendigen Gegenreaktionen ausgerichtet sind. Der Bedrohung durch Soft Power wird kaum Beachtung geschenkt. Besondere sicherheitspolitische Beachtung sollte eigentlich der technologischen Entwicklungen geschenkt werden. Z.B. das Internet und damit auch die Cyberkomponente kann sowohl Hard- als auch Soft Power-Effekte gewaltig verstärken.

Hybride Bedrohungen sind in nahezu keinen staatlichen Sicherheitsanalysen zu finden. Lediglich in der schwedischen Militärdoktrin 2012 und in der österreichischen Teilstrategie Verteidigungspolitik 2014 findet der Begriff hybride Kriegsführung beziehungsweise hybride Bedrohungen Erwähnung. Geht man davon aus, dass hybride Bedrohung mehr als hybride Kampfführung ist, impliziert dieses Bedrohungsbild auch die Notwendigkeit von umfassenden gesamtstaatlichen Gegenmaßnahmen. Der gesamtstaatliche Ansatz benötigt neben der inter- und intraministeriellen auch eine Kooperation mit weiteren Experten (oftmals auf interdisziplinärer Ebene). Nötig wäre sowohl ein nationales als auch ein zumindest EU-weites Gremium, welches durch eine ständige Lagebildbeurteilung einen hybriden Bedrohungsansatz zunächst erkennt und folglich angepasste Gegenmaßnahmen/Reaktionen entweder einleitet, oder nationale (internationale) Sicherheitsexperten sowie gegebenenfalls die Bevölkerung entsprechend informiert. Beim Internationalen Krisen und Konfliktmanagement (IKKM) ist der Faktor „hybride Bedrohung" stets mit zu beurteilen. Nur allzu leicht können nationale Akteure, die interministeriell zusammengesetzt sind, in Friedensmissionen hybriden Bedrohungen ausgesetzt sein und wiederum Kettenreaktionen auf das jeweilige Heimatland auslösen. So können hybride Bedrohungen auf den eigenen Staat überschwappen und zu verschiedenen Multiplikatoreffekten führen. Von hohem Interesse sind Analysen in Hinblick auf hybride Bedrohungen insbesondere dann, wenn unterschiedliche Nationen an Friedensmissionen teilnehmen. Dies vor allem dann, wenn Staaten unterschiedlichen Bedrohungsstufen ausgesetzt sind und zunächst weniger betroffene Staaten vom erhöhtem Sicherheitsrisiko anderer Staaten tangiert werden. In den verschiedenen Sicherheitsanalysen werden zwar Akteure, die eine mögliche Bedrohung für Staaten darstellen können, erwähnt, ihr mögliches Zusammenwirken beziehungsweise sich daraus herauskristallisierende Synergieeffekte finden sich darin allerdings nicht. Herausforderungen ergeben sich im Kontext hybrider Ansätze insbesondere in

Bezug auf kritische Infrastrukturen[7] wie z.B. dem Cyberbereich, der Energiebereitstellung oder bei den Transport- und Verbindungswegen. Verkürzt dargestellt: Hybride Bedrohungen stellen stets einen Angriff auf die kritische Infrastruktur dar. Daher ist der Schutz der kritischen Infrastruktur auch als Schutz gegen hybride Bedrohungen zu sehen. Derzeit werden Bedrohungen im Allgemeinen entweder als serielle (und unzusammenhängende) oder als einzelne, sektoral zu betrachtende Herausforderungen wahrgenommen. Folglich sind auch Gegenstrategien seriell und auf den individuellen Akteur ausgerichtet. Gerade bei hybriden Bedrohungsmustern muss aber einen Paradigmenwechsel geben.

Das NATO Allied Command Transformation (NATO ACT) Szenarien-Experiment zu „Countering Hybrid Threats" zeigt, dass für eine adäquate Gegenstrategie zu hybriden Bedrohungen nur ein „Comprehensive Approach"[8] zielführend ist. Aus dieser Einschätzung der NATO ist abzuleiten, dass eine umfassende Zusammenarbeit nicht nur auf nationaler, sondern insbesondere auf internationaler Ebene zu fordern ist, um hybriden Bedrohungen zu begegnen.

---

7 Unter kritischer Infrastruktur versteht die Europäische Kommission: „Kritische Infrastrukturen sind materielle und informationstechnologische Einrichtungen, Netze, Dienste und Anlagegüter, deren Störung oder Vernichtung gravierende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche Wohlergehen der Bürger sowie auf das effiziente Funktionieren der Regierungen in den Mitgliedstaaten hätte."; Kommission der Europäischen Gemeinschaften: Mitteilung der Kommission an den Rat und das Europäische Parlament; Brüssel, 20.10.2004, KOM(2004) 702 endgültig. <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52004DC0702&from=DE>, abgerufen am 16.12.2014.

8 „Der Comprehensive Approach bezeichnet ein gemeinschaftliches Bemühen um eine koordinierte und komplementäre Vorgehensweise im Rahmen des IKKM auf internationaler Ebene." (siehe Feichtinger, Walter/Braumandl-Dujardin, Wolfgang: Teil 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/Braumandl-Dujardin und Gauster, Markus (Hrsg.): Comprehensive Approach. Vom strategischen Leitgedanken zur vernetzten Politik. Schriftenreihe der Landesverteidigungsakademie 8/2011. Wien 2011, S. 23). In diesem Beitrag wird der Begriff auch für einen umfassenden koordinierten Einsatz aller zur Abwehr hybrider Bedrohung eingesetzter innerstaatlichen Kräfte und Mittel verstanden.

Auch wenn die EU in ihrer Sicherheitsstrategie von der möglichen Bedrohung durch eine Summierung verschiedener Elemente ausgeht[9], liegt auf „hybriden Bedrohungen" kein sicherheitspolitischer Fokus. Lediglich beim Schutz kritischer Infrastruktur kann man Ansätze zur Bewältigung hybrider Bedrohungen erkennen. Demgegenüber geht Österreich in seiner Sicherheitsstrategie zwar auf einen umfassenden Sicherheitsansatz ein, jedoch werden hybride Bedrohungen im Konkreten nicht thematisiert.

Die österreichische Sicherheitsstrategie

Die gegenwärtig gültige Österreichische Sicherheitsstrategie (ÖSS) besagt, dass die „[...] sicherheitspolitische Situation in Europa durch neue Herausforderungen, Risiken und Bedrohungen bestimmt"[10] ist. Es gibt keine Hinweise auf mögliche hybride Bedrohungen. Dennoch kommt Österreich in seiner Sicherheitsstrategie zum Schluss, dass die Herausforderungen komplexer werden, stärker miteinander vernetzt und zusätzlich weniger vorhersehbar sind.[11] Es wird auf die Tatsache verwiesen, dass komplexe Probleme in Sicherheitsfragen nur mehr durch internationale Kooperationen zu lösen sind.[12] Genau dies trifft auf die neuen Herausforderungen im 21. Jahrhundert zu, die vorwiegend hybrider Natur sein werden. In der ÖSS sind zahlreiche Bedrohungen aufgelistet. Nicht berücksichtigt ist ein vernetztes Zusammenspiel mehrerer der aufgezählten Bedrohungen, was eine beträchtliche Erhöhung der Komplexität ergäbe. Damit wäre eine verstärkte Unvorhersagbarkeit von Entwicklungen und wiederum eine erschwerte Planung von Gegenreaktionen verknüpft.

Das in der ÖSS angesprochene Konfliktbild ist umfassend, dennoch – auch wenn das gleichzeitige Auftreten der einzelnen Bedrohungen per se nicht ausgeschlossen wurde – eher in einer für sich geschlossenen Handlung gesehen. Ein zielgerichtetes, mehrdimensionales und zeitlich abgestimmtes

---

9 Rat der Europäischen Union, Ein sicheres Europa in einer besseren Welt, S. 6. <http://data.consilium.europa.eu/doc/document/ST-10881-2003-INIT/de/pdf>, abgerufen am 27.10.2014.

10 Bundeskanzleramt Österreich, Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten. Wien 2013, S. 4.

11 Ebd., S. 4.

12 Ebd., S. 5.

Vorgehen eines Akteurs wurde nicht explizit analysiert. Hervorzuheben ist jedoch das breite Sicherheitsverständnis, welches „[...] umfassend und integriert angelegt, aktiv gestaltet und solidarisch umgesetzt werden“[13] muss – Grundvoraussetzungen also, um hybriden Bedrohungen zu begegnen. Auch hier wird sowohl dem „Whole-of-Nation“[14]-, dem „Whole of Government“[15]- und dem „Comprehensive Approach“- Ansatz eine große Bedeutung beigemessen. Wobei davon ausgegangen wird, dass der diesbezügliche Stellenwert von Einzelstaaten abnimmt. Gleichzeitig wird aber auch auf die zunehmende wirtschaftliche und sicherheitspolitische Relevanz einiger Mächte verwiesen.[16]

Auf der Basis der Erkenntnis, dass ein

> „[...] umfassendes Lagebild aller Akteure und ein darauf aufbauendes gemeinsames Lageverständnis notwendige Grundlagen für sicherheitspolitische Entscheidungen auf nationaler und internationaler Ebene sind, [...] sollen Synergien im Sicherheitsbereich im Rahmen eines gesamtstaatlichen »Sicherheitsclusters« erzielt werden“[17].

---

13 Ebd., S. 4.

14 „Werden in einem bestimmten Fall von staatlicher Seite auch NGOs eingebunden, dann erfolgt eine gesamtstaatliche Koordination. In diesem Fall wird von einem Whole of Nation Approach (WoNA) gesprochen.“ (siehe siehe Feichtinger, Walter/Braumandl-Dujardin, Wolfgang: Teil 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/Braumandl-Dujardin und Gauster, Markus (Hrsg.): Comprehensive Approach. Vom strategischen Leitgedanken zur vernetzten Politik. Schriftenreihe der Landesverteidigungsakademie 8/2011. Wien 2011, S. 24).

15 „Im Bereich des WoGA *(Anm.: Whole of Government)* werden staatliche Maßnahmen für die internationale Friedensarbeit erfasst und inter- sowie intra-ministeriell koordiniert. Im WGA legt der einzelne CA-Beitragsleister fest, welche Mittel er in welcher Form und Umfang zur Verfügung stellen kann, um das internationale Engagement zu unterstützen.“ (siehe Feichtinger, Walter/Braumandl-Dujardin, Wolfgang: Teil 1 – Theoretische Aspekte eines Comprehensive Approach. In: Feichtinger, Walter/Braumandl-Dujardin und Gauster, Markus (Hrsg.): Comprehensive Approach. Vom strategischen Leitgedanken zur vernetzten Politik. Schriftenreihe der Landesverteidigungsakademie 8/2011. Wien 2011, S. 24). In dieser Arbeit wird mit diesem Begriff auch die inter- und intra-ministerielle Koordination zur Abwehr im Inneren verknüpft.

16 Bundeskanzleramt Österreich, Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten. Wien 2013, S. 5.

17 Ebd., S. 10.

Auch dies stellt eine Basis für den Umgang mit hybriden Bedrohungen dar. Dennoch werden konzertierte zielgerichtete, mehrdimensionale und in einem zeitlich abgestimmten Zusammenhang stehende hybride Machtprojektionen – wie auch in anderen analysierten ausländischen sicherheitspolitischen Strategiepapieren – nicht thematisiert.

Einen Schritt weiter als die ÖSS geht die österreichische „Teilstrategie Verteidigungspolitik 2014". Hier wird der hybride Faktor mehrfach erwähnt, auch wenn eher in einem Hard Power-Verständnis.

Sicherheitspolitische Strategien der Slowakei und Schwedens

Nahezu ausnahmslos ergaben sich aus den analysierten staatlichen Sicherheitsstrategien unterschiedliche Offensivakteure. Hybride Bedrohungen selbst wurden weder als generelles Phänomen noch exemplarisch erfasst. Es ergeben sich aber entsprechende Akteure, die das Potenzial haben, einen Staat hybrid zu bedrohen. Darunter finden sich nicht nur Staaten, sondern auch nicht-staatliche Akteure, wie z.B. Terrororganisationen oder global agierende Wirtschaftskonzerne. Eine Konnotation dieser Akteure mit hybriden Bedrohungen ist jedoch nicht auszumachen. Selbst eine mögliche „Abstützung" eines Akteurs auf z.B. terroristische Organisationen zur eigenen Zielerreichung wird in den analysierten Strategiepapieren nicht angedacht.

Die Thematik kritische Infrastruktur wird von den untersuchten Staaten unterschiedlich gewichtet, was von der Häufigkeit des genannten Terminus in den Strategien abgeleitet werden kann. Die Staaten entwickelten aber eigene Konzepte zum Schutz kritischer Infrastruktur (SKI), welche sich eingehender mit der Materie befassen. Für umsetzbare praktikable Lösungskonzepte zum SKI lässt sich auch in den Strategiepapieren der untersuchten Staaten wiederum die Notwendigkeit eines innerstaatlichen Comprehensive Approach-Ansatzes erkennen. Demnach ähneln die Konzepte der analysierten Staaten für eine umfassende staatliche Sicherheitsvorsorge zum Schutz der kritischen Infrastruktur noch am ehesten möglichen Gegenstrategien gegen hybride Bedrohungen. Einer erhöhten Aufmerksamkeit ist in der ÖSS auf den SKI gerichtet. Hier konzentriert man sich insbesondere auf die „[...] Bedrohung im und aus dem Cyberraum

durch staatliche und nicht staatliche Akteure [...]“[18]. Gesamtstaatliche Übungen werden gefordert.[19] Eine Kooperation zwischen staatlichen und nicht-staatlichen Bereichen wird auch in Sicherheitsstrategien eingefordert. Die Zusammenarbeit innerhalb der internationalen Gemeinschaft erhält bei globalen sicherheitspolitischen Herausforderungen einen erhöhten Stellenwert.

Zwar wird die Notwendigkeit einer interministeriellen Kooperation zur Gewährleistung staatlicher Sicherheit in den analysierten staatlichen Strategien erkannt, man sucht jedoch vergebens nach einer Ministerienübergreifenden gemeinsamen Lagebeurteilung. Gefordert wird eine solche in der ÖSS, wodurch „[...] Abläufe auf ihre Funktionalität im Hinblick auf einen umfassenden Sicherheitsansatz [...] modernisiert und angepasst werden“[20] sollen. Darin wird auch eine Optimierung des Zusammenwirkens aller sicherheitspolitischen Akteure bei der Analyse und Bewertung sicherheitsrelevanter Situationen[21] verlangt, was als wichtiger Schritt zum Erkennen und zur Bewältigung von hybriden Bedrohungen zu werten ist. Insbesondere bei militärischen Einsätzen im IKKM zeigt sich eine erhöhte Kooperationsbereitschaft und -notwendigkeit. Jedoch werden „hybride Bedrohungen“ nicht erschöpfend thematisiert.

4.2 Conclusio

Zur Thematik „Vernetzte Sicherheit“ findet sich auf der Österreichisches Bundesheer (ÖBH)-Homepage, dass „[...] eine arbeitsteilige Kooperation von Internationalen Organisationen und Foren und deren Zusammenwirken im Sinne eines „Comprehensive Approach“ (vernetzte Sicherheit) für Österreich immer bedeutender“[22] wird. Dies trifft insbesondere bei der neuen Herausforderung „hybride Bedrohung“ umso mehr zu. Es gilt, diesen mit einem umfassenden Sicherheitsansatz gezielt zu begegnen. Generell

---

18 Ebd., S. 17.
19 Ebd.
20 Ebd.
21 Ebd., S. 18.
22 Österreichisches Bundesheer: Direktion für Sicherheitspolitik. <http://www.bmlv.gv.at/wissen-forschung/bsp/index.shtml>, abgerufen am 29.09.2014.

zeigt sich anhand der Analysen der Sicherheitsstrategien aller Länder die besondere Bedeutung des innerstaatlichen „Comprehensive Approach".

Die im Zusammenhang mit in der Europäischen Sicherheitsstrategie (ESS) stets erwähnten Petersberg-Aufgaben zielen eher auf Missionen in Konfliktregionen außerhalb Europas ab, wobei der EU das gesamte Spektrum eines militärischen Engagements offen steht.[23] „Einsätze zur Verteidigung des nationalen Hoheitsgebiets der Mitgliedsstaaten sind in Ermangelung einer gemeinsamen europäischen Verteidigung nicht erfasst."[24] Hierbei handelt es sich lediglich um eine Hard Power-Bedrohung, Soft Power findet sich hier aber nicht. Will man zukünftig gegen hybride Bedrohungen gewappnet sein, müssen sich nicht nur Kleinstaaten, sondern insbesondere die EU mit derartigen Szenarien vermehrt auseinandersetzen. Dabei wären notwendige Maßnahmen gemäß der im Vertrag von Lissabon festgehaltenen kollektiven Verteidigungsklausel (Artikel 42 Absatz 7 des Vertrages über die Europäische Union) sowie der Solidaritätsklausel in ihrer Tragweite bezüglich hybrider Bedrohungen zu analysieren.

Verstärken sich bei gezielter Machtprojektion unvorhergesehene (zunächst nicht intendierte) negative Auswirkungen spricht man von einem Multiplikatoreffekt. Diese erschweren vermehrt sicherheitspolitische Analysen. Medien haben bei hybriden Bedrohungen einen wesentlichen Anteil am Erfolg oder Misserfolg dieser Strategie. Sie verstärken – wenn auch ungewollt – durch ihre Berichterstattung die mediale Präsenz z.B. terroristischer Akteure. Dabei kann es etwa zum signifikanten Ausfall von Umsätzen beim Tourismus und dadurch zu verringerten Steuereinahmen kommen. Eine solche negative finanzielle Entwicklung ließe wiederum weniger staatliche Ausgaben in verschiedenen anderen (sozialen) Bereichen erwarten. Weitere Multiplikatoreffekte können durch Sanktionen gegen Zulieferunternehmen (Uranminenabbau; Transport und Nuklear-Entsorgung) auftreten und so den Druck gegenüber bestimmte Branchen (z.B. Energiewirtschaft) erhöhen. Medien und ihrer Berichterstattung kommt deswegen bei der Minimierung sicherheitspolitischer Auswirkungen

---

[23] Ondarza, Nicolai von: Petersberg-Aufgaben. In: Bergmann (Hrsg.), Handlexikon der Europäischen Union. Baden-Baden 2012. <http://www.europarl.europa.eu/brussels/website/media/Lexikon/Pdf/Petersberg-Aufgaben.pdf>, abgerufen am 13.11.2014.

[24] Ebd.

höchste Bedeutung zu. Verantwortungsvolle journalistische Recherchearbeit, gepaart mit dem Ziel einer objektiven Berichterstattung, kann als wesentlicher Beitrag gegen hybride Bedrohungen gewertet werden.

Maßnahmen für eine effektive Strategie gegen hybride Bedrohungen können in mehrere Phasen unterteilt werden:

Bewusstseinsbildungsphase

- Eine hybride Bedrohung wird nur dann als Bedrohung empfunden, wenn eine strategische Schwelle überschritten wird, somit ist dieser Wert qualitativ und quantitativ festzulegen, was durch die Politik zu erfolgen hat. Dazu wird vorgeschlagen, dass die strategische Schwelle dann eine Herausforderung darstellt, wenn zumindest zwei Ministerien zur Bewältigung dieser Bedrohung involviert sind[25].
- Generell wurden in den Sicherheitsstrategien zwar auf zukünftige Bedrohungen reflektiert, auf defensive Maßnahmen gegen hybride Bedrohungen wurde bisher jedoch nicht der Schwerpunkt gelegt. Nur so ist die westliche Konsterniertheit zu erklären, mit der gegenwärtig auf hybride Ansätze in der Ukrainekrise reagiert wird. Ein Verständnis der Vielfältigkeit möglicher hybrider Vorgehensweisen ist die Voraussetzung, um adäquate Lösungsstrategien zu entwickeln (Awareness Building).
- Ein sicherheitspolitisches Umdenken auf allen Ebenen muss zu einem konzertierten staatlichen Ansatz zur Bekämpfung der dynamischen Bedrohung führen.

Der zunehmenden Bedrohung im Soft- und Smart Power-Bereich ist unbedingt Rechnung zu tragen und sollte in Lagebeurteilungen einfließen.

Früherkennungs-, Frühwarnungsphase

- Es gilt eine interministerielle Analysegruppe zu schaffen, die die Lageentwicklungen und Bedrohungsszenarien ständig bewertet.
- Eine Benchmark zur Feststellung einer Überschreitung der strategischen Schwelle ist zu identifizieren. Dazu wird vorgeschlagen,

[25] Zu berücksichtigen ist, dass es sich dabei nur um vorsätzlich herbeigeführte Schadensfälle handelt; Naturkatastrophen sind davon ausgenommen.

dass dies dann der Fall ist, wenn zumindest zwei Sektoren der hybriden Bedrohungen vorhanden beziehungsweise zu deren Abwehr mindestens zwei Ministerien involviert sind.

- Insbesondere IKKM-Kräfte (zusammengesetzt aus unterschiedlichen Ressorts) können mit hybriden Bedrohungen rasch konfrontiert werden. Zum Schutz von IKKM-Kräften, der Gewährleistung einer erfolgreichen Mission sowie zum Schutz vor Dominoeffekten im Heimatland der IKKM-Teilnehmer haben Lagebeurteilungen ständig zu erfolgen.
- Eine effektive Bewältigung hybrider Bedrohung ist lediglich mittels eines staatlichen „Comprehensive Approach" zu gewährleisten. Der Früherkennung kommt hier die größte Bedeutung zu. Dabei ist nicht nur ein entsprechendes Analysetool erforderlich, sondern auch ein auf höchster politischer Ebene angesiedeltes Expertengremium, welches ihre Analysetätigkeit stetig durchführt und in einer Art Krisenstab Lösungskonzepte entwickelt. Verstärkt nachzukommen ist der in der „österreichischen Teilstrategie Verteidigungspolitik" geforderten

  > „[...] ressortübergreifenden Analyse-, Planungs- und Führungsprozessen und gesamtstaatlichen sicherheitspolitischen Struktur sowie die Fähigkeit, Krisen und Änderungen im strategischen Umfeld rechtzeitig zu erkennen und sich im Rahmen des gesamtstaatlichen Ansatzes entsprechend zu engagieren"[26].

  Dies erfordert mehr als eine Abstützung auf den nachrichtendienstlichen Informationsaustausch.
- Es bedarf einer intensiven nationalen Koordination, um einen konzertierten hybriden Ansatz eines Akteurs zu erkennen.

Einer extremen Herausforderung unterliegen Freund-Feind-Differenzierungen bei Cyberattacken. Dabei zeigt sich nicht nur die Problematik der territorialen Ortung des Ausgangspunktes von Angriffen, sondern ebenso bei der Zuordnung zu einem Akteur. Sollte der Ursprung des Anschlags auf ein Land hindeuten, stellt sich die Frage, ob dieses tatsächlich als Urheber der Aktivität verantwortlich zu machen ist. Möglicherweise stützt sich ein anderer Akteur lediglich auf dessen Infrastruktur ab.

---

[26] BMLVS: Teilstrategie Verteidigungspolitik. S. 8. <http://www.bmlv.gv.at/pdf_pool/publikationen/teilstrategie_verteidigungspolitik.pdf >, abgerufen am 13.11.2014.

Bewältigungs- und Wiederherstellungsphase

- Nur eine gelebte staatliche inter- und intra-ministerielle Koordination („Whole-of-Government") stellt eine adäquate Gegenstrategie zu hybriden Bedrohungen dar.
- Eine auf gleicher Augenhöhe stehende zivil-militärische Zusammenarbeit ist die Basis für einen erfolgreichen gesamtstaatlichen Ansatz.
- Ein auf allen Ebenen funktionierender Informationsaustausch auf nationalen und internationalen Ebenen trägt zur Risikominimierung bei. Ein koordinierter Ansatz zwischen Sicherheitsorganen, Wirtschaftstreibenden, der Zivilgesellschaft, Experten auf allen Ebenen, Diplomaten sowie Politikern etc. trägt zu einer erfolgversprechenden Bewältigung hybrider Bedrohungen bei.
- Für eine erfolgreiche Verteidigung ist eine für sich abgekapselte einzelne Sicherheitsarchitektur eines Staates ungeeignet. Komplexe Systeme erfordern komplexe Gegenreaktionen und können nur durch eine umfassende inter- und intra-ministeriell Koordination plus einem qualitativ hochwertigen „Whole-of-Nation"-Ansatz sichergestellt werden.

Insbesondere die ausreichende Ressourcenbereitstellung auf allen Bereichen und Ebenen ist ein wesentlicher Teil zur Bekämpfung hybrider Bedrohungen und somit eine gute Investition in einen funktionierenden Staat.

Allgemeine Ableitungen

Die bisherigen Analysen lassen Ableitungen sowohl auf struktureller als auch auf operativer Ebene zu. Diese sind:

Ableitungen auf struktureller „strategischer" Ebene

- Eine Differenzierung zwischen innerer und äußerer Bedrohung ist nur mehr bedingt durchführbar. Ein brauchbares Lösungskonzept ist daher lediglich durch innerstaatliche Koordination aller für Sicherheit Zuständiger zu erreichen.
- Kein Ministerium oder andere Institution kann gegen hybride Bedrohungen isoliert für sich agieren. Ressortübergreifendes,

vernetztes sowie kooperatives Denken ist Grundvoraussetzung für ein funktionierendes staatliches Krisenmanagement.
- Das geforderte Expertengremium muss auf oberster politischer Ebene angesiedelt sein und als Analyse- wie auch Steuerungselement den gesamtstaatlichen Ansatz für eine Abwehr der hybriden Bedrohung aufbereiten.
- Völkerrechtlich sind hybride Bedrohungen und speziell jene, die von Soft Power ausgehen, kaum abgebildet, bedürfen aber im Einzelfall einer eingehenden völkerrechtlichen Analyse.
- Eine gelungene Bewältigung von hybriden Bedrohungen bedarf umfassender rechtlicher Rahmenbedingungen, um angemessen reagieren zu können. Hindernissen beziehungsweise Erschwernissen bei interministeriellen Verwaltungszuständigkeiten gilt es vorzubeugen. Die Kooperation zwischen staatlichen und nicht-staatlichen Sicherheitsbereichen muss ebenso geregelt sein.

Ein „Memorandum of Understanding" ist die Voraussetzung für überregionale und internationale Gegenreaktionen bei hybriden Ansätzen. Ob dies auch für eine bessere nationale Kooperation einen brauchbaren Weg darstellt, ist zu prüfen.

Ableitungen auf operativer Ebene

- Kleinstaaten wie auch internationale Organisationen und Institutionen müssen sich zukünftig in ihren Lagebeurteilungen vermehrt den Möglichkeiten hybrider Bedrohungen widmen.
- Hybride Bedrohungen gehen weit über militärisch verstandenen „Hybrid Warfare" hinaus und verlangen eine umfassende gesamtstaatliche Sicherheitsvorsorge. Um eine Prävention gegen hybride Bedrohungen zur erreichen, muss der Kooperationsgedanke auch auf operativer Ebene mit internationalen Institutionen gelebt werden.
- Nationale als auch internationale Sicherheitsarchitekturen dürfen nicht als separat abgekoppelte Stränge existieren.
- International ist eine starke Kooperation zwischen den EU-Mitgliedsstaaten, verknüpft mit weiteren sicherheitsrelevanten Organisationen, zur effektiven Bewältigung hybrider Bedrohungen unumgänglich.
- Streitkräfte müssen auf hybride Bedrohungen ausgerichtet werden.

Aufgrund der umfassenden Bedrohungsmöglichkeit ist zur Erlangung eines effizienten Mitteleinsatzes mit verstärkter Flexibilität zu antworten. Streitkräften ist für den Kampf gegen hybride Bedrohungen ein adäquater Auftrag zuzuweisen. Im Sinne eines „Whole-of-Governement"-Ansatzes gilt es Nischenaufgaben zu finden. Für Streitkräfte wird vorgeschlagen, sich ähnlich wie für den Schutz kritischer Infrastruktur auszurichten. Auch hier gilt es, rechtliche und materielle Voraussetzungen für einen reibungslosen Einsatz zu schaffen.

- Einige Staaten sehen ihre Sicherheit eng mit sicherheitsrelevanten Partnern und Verbündeten verknüpft. Kooperation kann einerseits die Sicherheit erhöhen, andererseits aber genau das Gegenteil bewirken.[27] Daher muss bei Kooperationsentscheidungen auch der hybride Faktor mitbeurteilt werden.
- Die verstärkte Unsicherheit, die bei komplexen Systemen[28] mitschwingt, bedarf eines intensiven gesamtstaatlichen Ansatzes. Dabei ist insbesondere auf die kritische Infrastruktur Bedacht zu nehmen. Je vernetzter Infrastrukturen sind – was besonders bei der Energiebereitstellung sowie im Cyberbereich zutrifft – desto mehr ist darauf der Fokus zu legen.

Eine Bewusstseinsbildung bei Medien für die Thematik „hybride Bedrohungen" ist anzustreben.

Ableitungen für das IKKM

Ableitungen ergeben sich ebenso für das IKKM. Diese decken sich in Teilbereichen mit den allgemeinen Ableitungen. Auch hier ergeben sich Ableitungen auf struktureller und auf operativer Ebene.

---

[27] Zum Beispiel zeigt sich gegenwärtig, dass Staaten durch ihr internationales Engagement zur Zielscheibe von international agierenden Terrororganisationen werden. Bei hybriden Bedrohungen seitens Staaten kann dies ebenfalls eintreten.

[28] Hybride Bedrohungen sind als komplexes System zu betrachten.

Ableitungen auf struktureller Ebene

- Ebenso wenig kann im IKKM ein Ministerium, eine Institution oder ein Staat gegen hybride Bedrohungen isoliert agieren. Vernetztes und kooperatives Denken ist auch hier Grundvoraussetzung für ein funktionierendes internationales Krisenmanagement.
- Das geforderte Expertengremium zur Lagefeststellung muss politisch möglichst hoch angesiedelt sein und die vor Ort eingesetzten IKKM-Kräfte als Analyse- und Steuerungselement bei der Abwehr hybrider Bedrohungen unterstützen.
- Die völkerrechtliche Komponente bei hybriden Bedrohungen bedarf ebenso einer eingehenden Analyse.
- Ein gelungenes IKKM erfordert in Hinblick auf hybride Bedrohungen umfassende rechtliche Rahmenbedingung, um den eingesetzten Kräften ein angemessenes Reagieren zu ermöglichen. Die Kooperation zwischen staatlichen, nicht-staatlichen und internationalen Elementen muss rechtlich geregelt sein.
- Brauchbare Lösungskonzepte sind nur mehr durch „Comprehensive"-, „Whole of Government"- und „Whole-of-Nation"- Ansätze vorstellbar.

Ein „Memorandum of Understanding" ist die Voraussetzung für internationale Gegenreaktionen bei hybriden Ansätzen.

Ableitungen auf operativer Ebene

- Internationale Organisationen und Institutionen müssen sich zukünftig in ihren Lagebeurteilungen vermehrt den Möglichkeiten hybrider Bedrohungen widmen.
- International agierende Institutionen müssen sich mit anderen vor Ort befindlichen internationalen Organisationen zur effektiven Bewältigung hybrider Bedrohungen abstimmen.
- Im IKKM eingesetzte Streitkräfte müssen auf hybride Bedrohungen ausgerichtet werden. Aufgrund der umfassenden Bedrohungsmöglichkeit ist zur Erlangung eines effizienten Mitteleinsatzes mit verstärkter Flexibilität zu antworten. Den IKKM-Kräften ist für den Kampf gegen hybride Bedrohungen ein adäquater Auftrag zuzuweisen. Im Sinne eines „Whole-of-Nation"-Ansatzes gilt es auch hier Nischenaufgaben zu finden.
- Werden andere als die eigenen am IKKM eingesetzten Kräfte hybrid

bedroht, wirkt sich dies möglicherweise zweifach aus: auf die eigenen IKKM-Kräfte im Einsatzort und auf das entsendete Heimatland. Daher ist noch vor der Entscheidung Kräfte ins internationale IKKM zu entsenden der hybride Bedrohungsfaktor mit zu beurteilen.

Es ist anzustreben, Medien möglichst frühzeitig auch auf operativer Ebene in das IKKM einzubinden, um hybride Bedrohungen zu minimieren.

Sind in Sicherheitsdokumenten gewisse Bedrohungsperzeptionen nicht abgebildet, heißt dies nicht, dass diese nicht vorhanden sind. Terroranschläge wie jene von 9/11 wurden vor dem 11. September 2001 als sehr unrealistisch eingestuft, dennoch erfolgten sie. Geht man nicht rechtzeitig auf neue Formen der Bedrohung ein, setzt man sich einem erhöhten Risiko aus. Nur wer entsprechend gewappnet ist, wird in der Lage sein, zu agieren.

Um in einem Kleinstaat den Bürgern weiterhin einen umfassenden Schutz sowie die territoriale Integrität und Handlungsfreiheit zu bieten, bedarf es der „Sicherstellung der Verfügbarkeit lebensnotwendiger Ressourcen“[29]. Des Weiteren muss man sich zur „Aufrechterhaltung einer leistungsfähigen Volkswirtschaft und Vorsorge gegen krisenbedingte Störungen der Wirtschaft“[30] vorbereitet. Eine intensive Beschäftigung mit hybriden Bedrohungen sowie deren Möglichkeiten und Auswirkungen ist daher unabdingbar. Ein enges interministerielles Zusammenwirken, wie eine vermehrte Kooperation mit dem privaten Sektor ist zur Erreichung von Synergieeffekten unumgänglich. Umfassende Sicherheitsvorsorge muss in allen Staaten als eine kooperativ gelebte Materie empfunden werden.

> „Österreich wird durch einen gesamtstaatlichen Ansatz der zuständigen Bundesministerien sicherstellen, dass seine IKT Infrastrukturen sicher und resilient gegen Gefährdungen sind. Die staatlichen Stellen werden dabei eng und partnerschaftlich mit dem privaten Sektor zusammenarbeiten.“[31]

Was bereits in der österreichischen Cybersicherheitsstrategie verankert ist, ist auch für den Bereich hybride Bedrohungen zu fordern.

---

[29] Bundeskanzleramt Österreich, Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten. Wien 2013, S. 9.

[30] Ebd., S. 9.

[31] Bundeskanzleramt Österreich: Österreichische Strategie für Cyber Sicherheit., Wien 2013,
S. 9.

5 Anhang

5.1 Power Projection by Pipeline: Russia, Sweden, and the Hybrid Threat from the Nord Stream Project, 2005-2009

Michael Fredholm

By late 2005, Sweden suddenly faced what it perceived as a hard security threat, in the unexpected form of a Russian pipeline project across the Baltic Sea which, it was suspected, could be used as a sensor platform for Russian military intelligence. The pipeline would be ideally located for use as a tripwire sensor chain through which Russia could monitor all movements of aircraft, surface vessels, and submarines across the Baltic. However, the pipeline project was a commercial venture, which could not be opposed through regular security strategies due to international law. For this reason, the Ministry of Defence commissioned a study of the implications of the project and an inter-ministerial working group from the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment was put together to address the threat and assess counterstrategies to contain it.[1]

When faced with Swedish opposition, Russia responded with its own multidimensional counter-counterstrategy, which for reasons which will be explained included several major EU member states. In effect, Russia used hybrid means to influence the media, society, and ministries of neighbouring states to gain permission for a strategic industrial infrastructure project. There were elements of what used to be known as an influence campaign in these efforts, but a broad spectrum of actors was used to achieve the objective of building the pipeline, which corresponded to Russia's, not Sweden's, strategic interests. In effect, the

---

[1] Swedish state television eventually exposed an internal Swedish government document on the working group's suggested strategies against the proposed pipeline. Sveriges Television (SVT), Nyheter, 07.12.2006. The internal document was a Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006.

two sides can be said to have lined up their respective principal powers as follows:

Russian Actors	**Task**	**Swedish Actors**	**Task**
Russian President	Decision-making	**Ministry of Defence**	Coordination
State-controlled Firm: Gazprom	Coordination	**Ministry of Justice**	EIA Approval (legal issues)
State-controlled Consortium: Nord Stream AG	Pipeline construction	**Ministry of Environment**	EIA Approval (environmental issues)
Intelligence Services	Intelligence collection	**Intelligence Services**	Intelligence collection
State Institutions	Seabed Survey	**Ministry of Defence**	Upholding state sovereignty
Naval Forces	Support to Seabed Survey	**Ministry of Defence**	Upholding state sovereignty
Diplomatic Power - Russia - Germany - Britain - France - Netherlands - Denmark	Political support: Continuous Continuous Initially Limited Limited Limited	**Foreign Ministry**	Political support
Media Power **- Nord Stream AG** **- State Media** **- PR Agencies**	 Lobbying Media campaigns Recruitment of policy makers	**FOI (Think Tank)** **Media Houses**	 Media campaigns Media campaigns

Table 7: Russian and Swedish Actors
Michael Fredholm

To the Swedish government, the natural gas pipeline project was perceived to be the very embodiment of a hybrid threat. With a hybrid threat defined as

> "a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests,"[2]

this was hardly surprising. As a commercial endeavour, the proposed pipeline would have to be treated as any other commercial project. Yet, foreign state organizations (the Russian diplomatic corps, aided to a certain extent primarily by its German counterpart; the Russian Navy; Russian state-controlled commercial enterprises such as Russia's natural gas pipeline export monopoly Gazprom; and much of the Russian media) were deeply involved in promoting the project.

The proposed pipeline was perceived as a threat to several Swedish core interests. Sweden's Defence Minister Mikael Odenberg summarized the hybrid nature of the threat in a national public radio interview: "the gas pipeline brings implications for energy policy, environmental policy, as well as security policy."[3] The Swedish government was particularly concerned over three core interests: the desire, based on environmental reasons, to gradually end European reliance on hydrocarbons as a key source of energy; the ambition (again for environmental reasons) to protect the Baltic Sea environment from the effects of pollution, the disturbing of old munitions and hazardous materials on the seabed, and if possible through a reduction in the overall level of shipping; and the desire to minimize naval activities in the Baltic (and, one could easily argue, in particular the presence of Russian naval units). In addition, the Swedish government felt duty-bound to support the views of Poland and the Baltic states, which opposed the project for reasons of their own, mainly having to do with their relations with Russia and Poland's role as a transit state for Russian natural gas supplies to

---

2 As defined by the National Defence Academy (Landesverteidungsakademie), Vienna: "Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen."

3 Sveriges Radio (Sweden), 14.11.2006.

Western Europe. Moreover, the proposed pipeline was regarded as a hard security threat in and of itself, since the Swedish Ministry of Defence realized at an early stage that it might be used as a platform for Russian military intelligence collection against Swedish targets. Additionally, the means eventually employed by the pipeline consortium to promote the pipeline project were also perceived as threatening to Swedish political culture. Here was indeed a commercial project which violated Sweden's core interests, yet it was beyond the control of the Swedish government—something hitherto almost unheard of so close to Sweden's borders. Instead it was regarded as sponsored by two neighbouring great powers, Germany and Russia, both of which had their own agendas and their own core interests which in this particular case conflicted with those of several smaller neighbours, among them Sweden.

This paper is divided into two parts. The first will describe the background of the Nord Stream pipeline and primarily serves to summarize the evidence for the pipeline project being a Russian government initiative and not a straightforward private business venture, as was generally argued by its proponents. In fact, to counter the response that the Swedish perception of the pipeline project was an unfortunate overreaction to a mere commercial venture, and an international one at that, it will be necessary to give a lengthy (and to the non-expert, admittedly somewhat tedious) description of the Russian energy sector and Russian energy policy. In addition, this part of the case study serves to illustrate the difficulty in recognizing and pinning down state participation in hybrid power projection employing commercial entities.

Those who wish may skip the first part and go straight to the second which will examine the pipeline project in its role as a hybrid threat to Swedish core interests. This part will describe the variety of actors involved, and their offensive means to promote the venture. In addition, it will examine the defensive means, also of a hybrid nature, employed by Swedish state actors in their attempt to thwart the project, an attempt which ultimately failed, yet succeeded in eliminating or at least reducing the project's potential to threaten Sweden's national security interests. On the surface, both the Swedish and Russian sides presented their cases as overt and transparent, and themselves as studiously reasonable and legalistic, yet both sides engaged in activities which could only be interpreted as hostile to the other. The devil was in the details, and a full description of the events which ac-

companied the Nord Stream project is necessary to perceive the hybrid means employed by both sides to enforce their will.

5.1.1 Part 1: The Pipeline Project as a Russian Government Initiative

National and Commercial Interests in the Pipeline Project

A major energy infrastructure project such as the Nord Stream pipeline cannot be understood without an analysis of the national and commercial interests of the states and corporations involved. For Russia, the pipeline project was the natural outcome of its national energy strategy.[4]

Few governments wish to be dependent on forces outside their control, even if the dependence is mutual. This is particularly noticeable within the field of energy security. While Russia is dependent on revenues from its energy exports, many European countries are equally or more dependent on Russia as a supplier of natural gas in particular. When possible, the Russian state strives, through its energy policy, to avoid dependence on other states and at the same time to dominate its domestic market as well as, when possible, the international market. Russia sees a particular strategic need to control the export and transit means for its exports to the international market. Russia thus works to create export infrastructure on Russian territory or across international waters that will eliminate the need to transit energy deliveries through other states.

Besides, state control over much of the Russian energy infrastructure means that Russia finds its energy policy a vital component in various issues of national security policy. The Russian desire to avoid dependence, for instance, makes its

---

[4] Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006; Fredholm, Michael: Strategies of Energy and Security in Contemporary Eurasia: Vulnerabilities and Opportunities in Russia's Energy Relationships with Europe, Central Asia, and China. In: Sreemati Ganguli (ed.): Strategising Energy: An Asian Perspective. New Delhi 2014, p. 163ff.

leaders preoccupied with a wide range of perceived strategic threats in the same way that some European Union (EU) countries instead perceive Russia as a threat. Russia will under no circumstances accept a position of dependence towards any other country, considering this a threat to its own national security. The Kremlin is no more immune to the demands of national security than the countries of the EU, or for that matter any other country.

Under the leadership of Vladimir Putin and Dmitry Medvedev, Russia developed, approved, and published its energy strategies in documents which carried legal status. The 2003 Russian energy strategy expressed key goals for Russia within the energy sector.[5] The results of its direction could be seen in several subsequent infrastructure projects carried out within the state-controlled Russian energy firms.[6] In addition, Russia, as a state, tends to take legislation such as the energy strategy seriously and tends to follow official policy expressed therein.[7]

The 2003 Russian energy strategy concluded that the goals of the Russian energy policy with regard to foreign countries included the need to strengthen the position of Russia in the global energy market and maximize the efficiency of the export possibilities of the Russian energy sector, and to ensure that Russian companies had equal access to foreign markets, technology, and financing.[8] Russia would use its unique geographical and geopolitical location. The energy factor would be a fundamental element within Russian diplomacy, for the foreign policy realization of the energy strategy and through diplomatic support to the interests of the Russian energy companies abroad. The energy strategy occa-

---

5 Energeticheskaya strategiya Rossii na period do 2020 goda ("Energy Strategy of Russia to the Year 2020"), Government of the Russian Federation Decree No. 1234-r, 28.08.2003. Approved on 23.05.2003 and confirmed by the Russian government on 28.08.2003.

6 Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005.

7 See, e.g. Fredholm, Michael: Russia and Central Asian Security. In: Schlyter, Birgit N. (ed.): Prospects for Democracy in Central Asia. Istanbul: Swedish Research Institute in Istanbul Transactions Vol. 15, 2005, p. 97ff; on the Russian National Security Concept and Foreign Policy Concept, pieces of legislation enacted for similar reasons as the energy strategy.

8 Energeticheskaya strategiya (2003), p. 40f.

sionally used language reminiscent of military strategy: the state would support the Russian companies in the struggle for resources and markets.[9]

Parts of the conclusions of the 2003 energy strategy, primarily those concerned with foreign markets, sounded alarming to Russia's neighbours.[10] The strategy listed the objective of securing Russia's political interests, in Europe and the neighbouring countries and within the Asia-Pacific region with natural gas, and throughout the entire world with oil.[11] However, it also contained the objective to remain a stable and reliable partner for the European countries and for the whole world community with regard to the export of energy.[12]

But was Russia a stable and reliable partner? Many have argued the opposite. In fact, Russia has often been accused of using its "energy weapon" against the importing countries to secure advantages of various kinds. Accusations have been many and varied, but they can be summarized as follows. Russia is said to wish to secure political dominance over neighbouring countries; secure an economic monopoly there; and limit the West's influence in Eastern Europe.[13]

Yet, from the Russian point of view, it was Russia, not the EU states, that was vulnerable to foreign policy pressure in the energy field. This was intimately linked to Russia's role as an exporter, because Russia itself depended on transit routes to move the energy to its destination. In other words, Russia regarded itself as suffering from transit dependence. This expressed itself in the energy strategy, which singled out foreign threats (geopolitics, macroeconomics, and business conditions) to Russian security, and furthermore indicated the need to

---

9 Ibid., p. 42f. It was not only the energy strategy that occasionally used language reminiscent of military strategy. At the 3rd Russian Petroleum & Gas Congress in Moscow on 21-23.06.2005, Semyon Vainshtok, then president of the Russian oil pipeline monopoly Transneft, quoted the famous 18th-century field marshal, Count Alexander Suvorov, to make a point.

10 Yet, it should in all fairness be pointed out that the 2003 strategy devoted the bulk of its text to domestic Russian concerns. In addition to several references to energy security, the energy strategy also, for instance, indicated the need for environmental security. Energeticheskaya strategiya (2003), p. 26.

11 Ibid., p. 61 and 71.

12 Ibid., p. 41.

13 See, e.g. Hedlund, Stefan: Russia as a Neighborhood Energy Bully. In: Russian Analytical Digest 100 (26.07.2011), p. 2ff.

have export port terminals not under the control of foreign powers.[14] Transit dependence means dependence on a foreign power, thus making Russia vulnerable not only to swings in business conditions but more importantly, to economic or political blackmail—making Russia the victim of precisely the policy of which others have accused Russia.

By laying a natural gas pipeline to Germany across the Baltic Sea, Russia wanted to escape transit dependence. Besides, pipelines are both cheaper and environmentally safer than other modes of shipping. However, the investment cost to build a pipeline is huge. Furthermore, when a pipeline has been built, it cannot be moved. To invest in a pipeline leading to a single customer makes the supplier vulnerable to demands from the customer to re-negotiate the price of energy or cancel imports, after the investments have already been made and the project is committed. This was the lesson Russia learned with regard to the Gazprom-sponsored gas pipeline to Turkey known as Blue Stream. This pipeline began operations in December 2002, but as early as March 2003, the Turkish side suspended imports (reportedly because of this country's recession) in order to re-negotiate the agreement in its favour. Geopolitical factors also complicated the deal, because of the Turkish support for the American-sponsored South Caucasus Pipeline from Azerbaijan to Turkey.[15]

A key strategic concern when projecting an international pipeline is thus whether the pipeline will connect directly to the end consumer, or whether it will pass through transit states. If so, will political decisions or the international context affect how the pipeline can be used, at present or in the future? Because of perceived problems in its relations with the present transit states (primarily Poland, Ukraine, and Belarus), Russia was in the process of developing a system of natural gas pipelines (Nord Stream across the Baltic and South Stream across the Black Sea) that would bypass the transit states and instead deliver gas straight to the West European markets. From the point of view of state power, these pipeline projects were often regarded as hostile to the transit states through which the Russian energy exports to Western Europe so far flowed. Several of them were not only transit states but also, in their turn, dependent on imported Russian energy. Would Russia use threats of the suspension of energy exports as a

---

14 Energeticheskaya strategiya (2003), p. 17 and 68.

15 Torbakov, Igor: Russian Gas Company Makes Concessions in Bid to Resolve Pipeline Dispute with Turkey. In: Business & Economics, 09.07.2003.

means to impose its will on other countries, and if so, would Russia be successful? In the 1990s, a few cases had occurred in which Russia attempted to gain concessions, for instance from Lithuania, Ukraine, and Moldova. However, none of these attempts were successful. Russia gained nothing from its attempts.[16] Despite frequent claims to the contrary, there were no similar cases since the 2003 formulation of an energy strategy—with one exception. Russia repeatedly used energy deliveries as a foreign-policy instrument against one particular foreign state, Belarus.[17] This was perhaps not surprising. First, Belarus was a state that since the signing of a treaty on 8 December 1999 envisioning greater political and economic integration was formally united to Russia in a two-state union. Second, Belarus had for domestic political reasons no support whatsoever to expect from the West, even if it cried foul.

There were, however, frequent commercial disputes, in which politics at times played a role. Several disputes involved Ukraine. The trade in natural gas from Russia and Turkmenistan to Ukraine was characterized by opaque relationships, secret contracts, and hidden beneficiaries, which, most observers concluded, engendered substantial corruption, with serious losses to both the Russian and Ukrainian states as well as consumers and shareholders there and elsewhere in Europe.[18]

Some political analysts in Europe and elsewhere went further and claimed that what Russia really wanted was to limit the growth of democracy in Eastern Europe and use Eastern Europe as a first step in the creation of a new global empire.[19] Such arguments were firmly rooted in the field of politics. Ultimately, this interpretation of Russia's energy export policy became an issue of faith. Either

---

16 Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005.

17 See, e.g. IWPR's Belarus Reporting Service 53, 02.03.2004, for one case among many. See also Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok. Moscow: Kommersant/Eksmo 2009, 39ff.

18 Fredholm, Michael: Natural-Gas Trade between Russia, Turkmenistan, and Ukraine: Agreements and Disputes. Asian Cultures and Modernity Research Report 15. Stockholm University 2008.

19 See, e.g. Cohen, Ariel: Rethinking Reset: Re-Examining the Obama Administration Russia Policy. Testimony before the U.S. House of Representatives. Committee on Foreign Affairs, 07.07.2011.

you believed in the threat, or you did not. It was hardly coincidental that the most extreme views on Russia as an energy supplier, whether positive or negative, tended to be found in those countries that by force of geography and history depended on Russian natural gas supplies and lacked most or all other options.

Sweden was among those neighbouring countries which to some extent were alarmed by the 2003 Russian energy strategy. Sweden accordingly paid a certain level of attention to the developments of the Russian energy sector. Sweden was not a transit country, nor was Sweden dependent on Russian energy. Natural gas provided only approximately 2 per cent of Sweden's total energy consumption, and all gas deliveries came from Denmark.[20] Sweden imported Russian crude oil and petroleum products, as well as some electricity, but had several sources of supply and was in no way dependent on deliveries from Russia.[21] Then why was Sweden so concerned? The explanation can be found in the project which was first called North Transgas but soon would become known as the North European Gas Pipeline (NEGP) and eventually—Nord Stream.

North Transgas and the North European Gas Pipeline Project

The idea to build a northern natural gas export pipeline from Russia across the Baltic Sea originated in Finland and had been discussed since 1993.[22] Finland, already dependent on Russian natural gas supplies, saw itself as a future transit country and wished to host a major export pipeline from northwestern Russia to Germany. A feasibility studies for such a venture was carried out in 1997-1999, when Gazprom and the Finnish firm Fortum (then Neste Oy) set up a parity joint venture, North Transgas Oy, to study the expediency of building such a

---

20 Energimyndigheten (Swedish Energy Agency): Europas naturgasberoende: Åtgärder för tryggad naturgasförsörjning. Eskilstuna 2006, p. 23ff; Energimyndigheten: Hur trygg är vår energiförsörjning? En översiktlig analys av hot, risker och sårbarheter inom energisektorn år 2006. Eskilstuna 2007, p. 25.

21 See, e.g. Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 41ff.

22 Sinijärv, Riivo: The NEGP. Estonian Perspective. In: Baltic Mosaic. St. Petersburg Winter-Spring 2006), p. 6ff, here 6. Also noted by Jonathan Stern in Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 30. Stern may refer to the same source.

pipeline.[23] Sweden was regarded as an important market as well. On 3 December 1997, Russia and Sweden, represented by Russian First Deputy Prime Minister Boris Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Anders Sundström, respectively, signed a protocol about Sweden's involvement in the construction of the pipeline.[24]

Little came out of this joint venture, yet work continued in Russia. Although Gazprom was organised as a joint-stock company and despite having some limited foreign ownership, Gazprom in many ways operated as a government agency, combining commercial and regulatory functions.[25] Envisaged as a new route for Russian natural gas exports to Western Europe, it was eventually decided in Moscow that the projected pipeline system would pass beneath the Baltic Sea from, not Finland, but Russia's Portovaya Bay near Vyborg in the Gulf of Finland to Synergiepark Lubmin, near Greifswald on the coast of Germany. The ambitious plan at that time included branch lines to be built to feed natural gas to consumers in Finland, Sweden (with an entry point at Nyköping), and the Russian Kaliningrad enclave.[26] Yet, the main beneficiaries of the gas supplies would be Germany, the Netherlands, and ultimately Britain. In Germany, two projected pipelines would receive the gas and move it further. One was the Norddeutsche Erdgas-Leitung (NEL) to Rehden in Lower Saxony. The other was the Ostsee-Pipeline-Anbindungs-Leitung (OPAL) to Olbernhau near the Czech border (and on to Brandov in the Czech Republic).[27] However, the final

---

23 NEGP web site <www.negp.info> (defunct), last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), p. 30; Neft' i kapital 10, 2004, p.113; Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15.

24 ITAR-TASS, 03.12.1997; Izvestiya, 17.11.1998.

25 See, e.g. Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

26 See, e.g. Izvestiya, 17.11.1998; International Energy Agency (IEA): Russia Energy Survey 2002. Paris 2002, 139. On Nyköping, see Nord Stream AG, Project Information Document – Swedish Version (November 2006), dated 24.10.2006, p. 26. This was the document submitted with the notification to the littoral states of the Baltic Sea on 14.11.2006.

27 Nord Stream: Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 247; Nord Stream AG, Project Information Document – Swedish Version (November 2006), dated 24.10.2006, p. 8. This was the document submitted with the notification to the littoral states of the Baltic Sea on 1411.2006. Both pipelines would be owned and managed by E.ON Ruhrgas and Wingas GmbH, the latter a joint

terminus of the projected pipeline would be Britain, accessed through the Interconnector pipeline from Zeebrügge (Belgium) to Bacton (UK) or, eventually, the BBL pipeline from Balgzand (Netherlands) to Bacton (UK).[28] Other countries including Denmark would receive gas as well. In December 2000, the European Commission accordingly awarded the project Trans-European Network (TEN) status, which would assist in attracting funding from international financial institutes including the European Bank for Reconstruction and Development (EBRD) and European Investment Bank. In January 2001, the chairmen of Gazprom and Fortum submitted a joint letter to the prime ministers of Finland and Russia, requesting support of both governments and the EU for the pipeline project. Two German companies, Ruhrgas and Wintershall, were invited into the project and an agreement between the participating companies on a joint study of the project to build the pipeline was signed in Moscow in April 2001.[29] Cooperation between Ruhrgas and Gazprom went back to 1970 when Ruhrgas, together with several other German industrial companies and banks, helped construct natural gas pipelines to acquire gas from Siberia for sale to Western Europe.[30] Wintershall and Gazprom had begun working together in 1990, when the Soviet Union and the Federal Republic of Germany signed an international agreement for cooperation in the gas industry.[31]

During the Russia-EU summit in Brussels on 11 November 2002, a working meeting took place between Alexei Miller, Gazprom Chief Executive Officer

---

venture between Wintershall and Gazprom. See also Wingas Transport GmbH & Co. KG, press release, 08.10.2007.

28 See, e.g. Northwest Russia Commercial News Update <www.bisnis.doc.gov>, 1-31.12.2002. On the Zeebrügge-Bacton Interconnector, see the firm's web site, <www.interconnector.com>. On the Balgzand-Bacton-Line (BBL), operational since 2006, see the firm's web site, <www.bblcompany.com.> Gasunie has a 60 per cent share in BBL, while Belgian gas transport company Fluxys and E.ON Ruhrgas each have 20 per cent shares. Gazprom has an option to buy a 9 per cent stake in BBL, with the shares coming from Gasunie, leaving the latter with a majority 51 per cent. See, e.g., Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 121.

29 NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), p. 31.

30 Russian Petroleum Investor 14: 5 (May 2005), p. 53; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15.

31 Russian Petroleum Investor 14: 5 (May 2005), p. 54.

(CEO),[32] and François Lamoureux, Director-General of the European Commission Directorate-General for Transport and Energy (DG TREN). As a result, DG TREN again recognized the pipeline project as a priority project within the framework of the energy dialogue between Russia and the EU. On 18 November, the Gazprom board decided to begin execution of the pipeline construction project.[33] On 21 November, Miller met Leningrad Region governor Valery Serdyukov. The sides agreed to set up a joint working group consisting of authorized representatives of the Leningrad regional administration and two Gazprom subsidiaries, OOO Lentransgaz and OAO Giprospetsgaz, to coordinate the pipeline project on the territory of the Leningrad region. Then Miller travelled abroad. On 25 November, Miller met with Finnish Prime Minister Paavo Lipponen and Fortum chairman Matti Vuoria in Helsinki. On 26 November, Miller met with Dutch Prime Minister Jan Peter Balkenende and George Verberg, CEO of national gas company Nederlandse Gasunie, in The Hague. On 28-29 November 2002, Miller made an official visit to London at the invitation of the British government. He met with the British Minister for Energy, Brian Wilson, as well as the heads of British Petroleum, Royal Dutch/Shell, Centrica, and Goldman Sachs. In all these meetings, the pipeline project was one of the projects under discussion.[34]

Miller also attempted to sell the idea of the pipeline project in Sweden. On 28 March 2003, Miller met Swedish Minister for Industry (Enterprise), Employment and Communications Leif Pagrotsky in Stockholm, discussing the possibility of supplying Russian natural gas to Sweden.[35]

On 30 June 2003, in the presence of Russian President Vladimir Putin and British Prime Minister Tony Blair, a memorandum on cooperation with regard to the pipeline project was signed with Britain.[36] And late in 2003, Gazprom established a foothold in the British gas market when Wingas (a joint venture of

---

32 Miller's formal title was chairman of the management committee of Gazprom.

33 Northwest Russia Commercial News Update. December 2002, p. 1ff. <www.bisnis.doc.gov>; Russian Petroleum Investor 13: 4 (April 2004), p. 31f.

34 Russian Petroleum Investor 13: 4 (April 2004), p. 32.

35 Interfax, 31.03.2003.

36 NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), 32.

Gazprom and Germany's Wintershall) created a joint venture on a parity basis, HydroWingas Ltd., to market natural gas in Britain.[37]

Having gained international support, Gazprom and key Russian ministries involved in the project then prepared a new feasibility study on the construction of the pipeline. The resulting proposal of the Russian Energy Ministry and Gazprom was examined by the Russian government. On 16 January 2004, Russian Prime Minister Mikhail Kasyanov signed decree No. 64-r of the Russian government to approve the proposal to build what was now referred to as the North European Gas Pipeline (NEGP). The Russian government charged the Energy Ministry with the preparation, with Gazprom's direct participation, of the necessary documentation for the construction of the pipeline. The Russian government assigned to the Russian Federation State Committee for Construction and the Housing and Utilities Sector (Gosstroy) and Russian Ministry of Natural Resources the task of ensuring, jointly with interested federal bodies of executive authority, the state expert examination of this documentation, and the environmental impact upon the regions that would be traversed by the pipeline.[38]

It was thus clear from the outset that the northern gas export pipeline project was a Russian government initiative. There were commercial incentives as well, and foreign participation, but as envisioned in the recently adopted energy strategy, it was the Russian state which took the initiative, not the private sector. It was also representatives of the Russian state who henceforth began to promote the project, among them notables such as Viktor Kalyuzhny, Deputy Minister of Foreign Affairs of the Russian Federation and Special Presidential Envoy for the Caspian Sea (and before that Minister of Fuel and Energy from 1999 to 2000), who declared that the NEGP would dramatically increase Russia's gas export potential.[39]

Even at this moment of perceived success, storm clouds were gathering over the project. On 4 February 2004, a Gazprom board meeting addressed the strategic

---

37 Russian Petroleum Investor 13: 4 (April 2004), 32f.

38 Ibid., p. 30f.

39 Kalyuzhny, Viktor, Deputy Minister of Foreign Affairs of the Russian Federation and Russian Special Presidential Envoy for the Caspian Sea, Statement at the Caspian & Black Sea Oil & Gas Conference 2004, Istanbul, 26.02.2004.

issue of how to build an export policy in the face of the new conditions imposed by the EU, which simultaneously aimed to protect the energy security and labour markets of the member states and split up the major energy companies in order to liberalize the market. The EU accordingly demanded that companies such as Gazprom too would adhere to the new policies, which conflicted with Gazprom's monopoly position. At issue were both the new policies for the EU internal market and concerns that Gazprom's dominant position would make EU member states dependent on Russia. The Gazprom board of directors reportedly concluded that the solution would be for Gazprom, jointly with the Russian government, to "persuade" the EU to cooperate and not to reduce Russian gas imports.[40] It would soon become clear that the Gazprom board and indeed the Russian government in its enthusiasm and belief in its influence with EU leaders underestimated the problem.[41]

On 11 February 2004, Gazprom CEO Miller held a Gazprom conference in Moscow on the implementation of the NEGP construction project. It was decided to go ahead and draft a detailed feasibility study. It was also decided to retain Dresdner Bank (Germany) and ABN Amro (Netherlands) as financial consultants to work on the NEGP project and the British law firm Linklaters as a legal consultant. It was also decided to conduct a tender to select an engineering consultant for the project.[42]

---

40 Russian Petroleum Investor 13: 4 (April 2004), p. 35f. The board also decided to develop a strategy for the expansion of the EU and Russia's entry into the World Trade Organization.

41 The Russian side was enthusiastic and on 05.02.2004 addressed the NEGP project issues at a meeting with François Lamoureux, DG TREN, according to Viktor Khristenko, then Russia's deputy prime minister and subsequently minister of industry and energy. Russian Petroleum Investor 13: 4 (April 2004), 37. On 06.02.2004, Khristenko gave a briefing in Moscow that the first-phase feasibility study on the NEGP would be completed before year-end 2004. He also said that a consortium of Gazprom and Finland's Fortum soon would sign a contract with the European Commission to develop a feasibility study on the pipeline. Ibid., p. 36.

42 Ibid., p. 33 and 36. The deal with Dresdner Bank had been finalized on the day before, on 10.02.2004, when Miller met in Moscow with Herbert Walter, chairman of the Dresdner Bank board of managing directors, the two agreeing that the bank would act as a financial consultant on the project. Reuters, 10.02.2004. Finally, having carried out this preparatory work, an investment decision on the NEGP would be made in the fourth quarter of 2004. This date was later postponed, however. In the fall of 2004,

Gazprom planned to launch construction work in 2005, estimated that the NEGP would be commissioned in 2007-2008, and would be able to supply 20 to 30 billion cubic meters (bcm) of gas per year.[43] There was a considerable demand for these supplies in Germany and Britain, both of which needed additional gas imports. Several international energy companies, including Ruhrgas and Wintershall (both of Germany), Gasunie (The Netherlands), Royal Dutch/Shell (Britain/Netherlands), Total (France), and British Petroleum and Centrica (both of Britain), displayed an interest in the NEGP project.[44] But Gazprom wanted more than investments and had additional criteria when it came to the selection of project participants. Gazprom wanted partners which could facilitate gas sales in new markets and closure of long-term contracts for gas purchase at fixed prices.[45] What Gazprom wanted was security of supply, which indeed is the goal of most energy producers. Gazprom defined this as (1) physical security (reliable infrastructure, sufficient resource base); (2) economic security (stability); (3) legal security, and (4) secure demand (long-term projects and contracts).[46] The need for a secure demand derived from the very substantial investment costs required for construction of new energy infrastructure.

Vladimir Putin's Views on Russian Energy Policy

As had become clear from the conclusion by the Gazprom board of directors that Gazprom, jointly with the Russian government, had to "persuade" the EU to cooperate, the project was to a considerable extent not only initiated by but also dependent on the Russian state. This was no coincidence. It also conformed to the views expressed by Russia's President Putin.

Gazprom announced that it would decide whether to invest in the construction of the NEGP in the first quarter of 2005. Russian Petroleum Investor 14: 4 (April 2005), p. 42.

43 Russian Petroleum Investor 13: 4 (April 2004), p. 30 and 35.

44 NEGP web site <www.negp.info>, last accessed in February 2006; Russian Petroleum Investor 13: 4 (April 2004), 32 and 34.

45 Russian Petroleum Investor 13: 4 (April 2004), 34.

46 Tsygankov, Stanislav (Head of the Department for Foreign Economic Activities, Gazprom), "Export Strategy for Russian Gas: Securing a Reliable Supply," 7th Russian Petroleum & Gas Congress, Moscow, 25.06.2009.

Until mid-2003, Russian energy policy remained the composite product of many disparate actors, both within the state structures and the Russian private sector. Until the spring of 2003, energy company executives even took part in the decision-making process at government level.[47] Unlike Boris Yeltsin before him, Putin attempted to limit the opportunities for the business oligarchs to enjoy direct presidential access. He preferred that a redefined version of the Russian Union of Industrialists and Entrepreneurs function as business advisory board for the Presidency.[48] Policy was soon settled in favour of state control, as described in the 2003 energy strategy.[49] This certainly included major export pipelines. Vladimir Putin stated, on 29 April 2004, that he did not intend to end state control over pipeline transportation, the key factor in Russian oil and natural gas transportation. "At the moment I consider that there are no grounds for the state to give up its control over pipeline transportation. But this does not hinder private investment, which will be welcomed." Putin continued that "private investment is possible with continued state control and state ownership of pipeline transport".[50]

---

47 See, e.g., Interfax, 20.12.2002, on the Russian president's regular contacts with top Russian businessmen. An earlier example is provided by the 1995 energy strategy, which was drafted by a number of commissions that included, in addition to various government appointees, A. F. Dyakov, president of UES, V. D. Chernyayev, president of Transneft, V. I. Ott, vice-president of Rosneft, R. I. Vyakhirev, president of Gazprom, V. Yu. Alekperov, president of LUKoil, and V. A. Fedorchenko, president of the East-Siberian Oil and Gas Company. For further information, see Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

48 Shevtsova, Lilia: Putin's Russia. Washington, DC 2003, p. 180.

49 For further information, see Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005; Fredholm, Michael: Gazprom in Crisis: Putin's Quest for State Planning and Russia's Growing Natural Gas Deficit. In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 06/48, London 2006.

50 Interfax, 29.04.2004.

Putin's opinion on this matter was well known, as was the fact that he considered natural gas a key strategic commodity. Already in October 2003, Putin reportedly told visiting German Chancellor Gerhard Schröder in Yekaterinburg:

> "The gas pipeline system is the creation of the Soviet Union. We intend to retain state control over the gas transportation system and over Gazprom. We will not divide Gazprom. And the European Commission should not have any illusions. In the gas sector, they will have to deal with the [Russian] state."[51]

Putin's views on state planning and the importance of the energy policy for Russia's foreign relations went years back, to the time before he became president of Russia. Indeed, these views formed the key part of the candidate of sciences dissertation in economics that Putin defended in June 1997 when he was still a senior official. The dissertation was written on the topic of "strategic planning of the reproduction of the mineral raw materials base of the region under conditions of the formation of market relationships" at St. Petersburg's well-known State Mining Institute.[52] What seems to have been either an abstract or a further development of the dissertation was published in January 1999 as an article on "mineral raw materials in the strategy for development of the Russian economy" in the journal of the institute, his being the lead article in an issue devoted to the fuel and energy complex.[53]

In his dissertation, Putin outlined his belief that state planning must be the key to the management of Russia's natural resources:

---

51 Felgengauer, Pavel: Oborona neftegazovoy truby. In: Novaya Gazeta 76.

52 Putin, Vladimir: Strategicheskoye planirovaniye vosproizvodstva mineral'no-syr'yevoy bazy regiona v usloviyakh formirovaniya rynochnykh otnosheniy (Sankt-Peterburg i Leningradskaya oblast'). St. Petersburg 1997. On the State Mining Institute, see its web site, <www.spmi.ru>.

53 Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 3ff. The article has since been translated into English and re-published in Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 48ff. See also Balzer, Harley: The Putin Thesis and Russian Energy Policy. In: Post-Soviet Affairs 21:3 (2005), 210ff. Putin's dissertation and journal paper were first brought to public light in Olcott, Martha Brill: The Energy Dimension in Russian Global Strategy. Vladimir Putin and the Geopolitics of Oil (Houston, Texas 2004), p. 16. Olcott doubted whether Putin wrote the dissertation himself or relied on a ghost writer, but she did not doubt that he stood for the views presented therein.

> "The main result of the dissertational work is that normative methodological recommendations on the creation of a system of strategic planning can be developed, corresponding to and based on the received scientific results. These recommendations will arm the state organs at all levels with an instrument with which to realize the strategic goals in developing the mineral raw materials complex."[54]

"Sustainable development of Russia's economy in the near term must be based on systematic growth in her developed sectors, and, most of all, on her mineral resource potential," Putin noted. He continued: "The main reserve to, in the near future, make Russia a great economic power with a high living standard for the majority of the population is maximum support for the fatherland's processing industry based on the extractive complex."[55] Putin also concluded that the strategic goal of state policy with regard to decisions about domestic and foreign economic policy must be "aimed at furthering the geopolitical interests and maintaining the national security of Russia."[56] Putin did not believe in globalization or global market forces, at least not at this particular stage in Russia's economic development. State planning must be at the core of Russia's resource management, he concluded. Russia's mineral resources would serve as the basis for Russia's economic development and as a guarantee for the country's economic security. This demanded what Putin described as the "creation, with full support from the state, of large financial-industrial groups-corporations with an interbranch profile that will be able to compete with Western transnational corporations."[57] State-sponsored foreign investment in Russia's extractive industries would also be needed, Putin noted, but the Russian state must under no circumstances lose control of the country's resources. A key demand, in Putin's

---

54 Putin, Vladimir: Strategicheskoye planirovaniye vosproizvodstva mineral'no-syr'yevoy bazy regiona v usloviyakh formirovaniya rynochnykh otnosheniy (Sankt-Peterburg i Leningradskaya oblast'). St. Petersburg 1997, p.175.

55 Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 3; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 49.

56 Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 7; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 53.

57 Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 6; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 51.

words, was to "ensure that national interests are maintained when attracting foreign investment."[58]

Incidentally, Putin's views on Russian energy security would seem to correspond to his thoughts on global energy security. In February 2006, when Russia had assumed the presidency of the Group of Eight (G8, consisting of Britain, the United States, Russia, France, Germany, Japan, Italy, and Canada), Putin concluded that "all it takes is for mankind to create a balanced [energy security] potential in order to provide every state with sustainable energy supply, and international cooperation opens all avenues for that."[59] In other words, energy security was the business of states and the appropriate state organs, not privately owned corporations.

As president, Putin began to realize his vision for Russia. The natural monopolies including the energy sector, of which Gazprom was a key component, were being put under the personal authority of representatives of the Russian state in the form of members or chairmen appointed to the boards of directors. Since these representatives were generally regarded as Putin's men and came from Putin's own staff, the Presidential Administration, it was clear that not only was Putin strengthening state control over the natural monopolies, he was also strengthening direct presidential control.[60] Examples of his appointees included both Alexei Miller, a friend of Putin from St. Petersburg, who was appointed CEO of Gazprom in May 2001,[61] and Dmitry Medvedev, the Head of the Presidential Administration, who was appointed Chairman of Gazprom in June 2002.[62] Among other Gazprom board members with direct links to the Russian

---

58 Putin, Vladimir: Mineral'no-syr'yevyye resursy v strategii razvitiya Rossiyskoy ekonomiki. Zapiski Gornogo Instituta 144 (1999), p. 8; translation from Balzer, Harley: Vladimir Putin's Academic Writings and Russian Natural Resource Policy. Problems of Post-Communism 53:1 (January/February 2006), p. 54.

59 Putin, Vladimir: 'Energy Egotism Is a Road to Nowhere'. In: Wall Street Journal, 29.02.2006.

60 Fredholm, Michael: The Russian Energy Strategy & Energy Policy: Pipeline Diplomacy or Mutual Dependence? In: Conflict Studies Research Centre, UK Defence Academy, Russian Series 05/41, London 2005 Policy.

61 Upstream, 17.06.2005, p. 32.

62 Gazprom web site, <www.gazprom.ru>. Medvedev was chairman of the board of directors of Gazprom also in 2000-2001, as well as deputy chairman of the board of

top leadership were, by 2004, German Gref, Minister for Economic Development and Trade of the Russian Federation; Viktor Khristenko, Minister of Industry and Energy of the Russian Federation; Farit Gazizullin, Minister for Property Relations of the Russian Federation; Igor Yusufov, Special Representative of the President of the Russian Federation for International Energy Cooperation, Ambassador-at-large of the Ministry of Foreign Affairs of the Russian Federation; and (until 25 June 2004) Alexandra Levitskaya, First Deputy Head of the Secretariat of the Presidential Administration.[63]

The Putin-Schröder Concord

On 8 July 2004, during German Chancellor Gerhard Schröder's visit to Moscow, Germany's largest electricity and gas concern, E.ON AG, and Gazprom signed a memorandum of understanding with regard to a variety of areas of energy sector cooperation including the construction of the NEGP. This strategic alliance was hardly surprising. E.ON was now Gazprom's largest foreign investor, having in February 2003 acquired Ruhrgas AG (and had on 1 July 2004 changed the firm's name to E.ON Ruhrgas AG; E.ON Ruhrgas thus controlled directly and through Gerosgaz, a joint venture with Gazprom subsidiary Gazexport, 6.43 per cent of Gazprom's shares).[64] The foundation for cooperation between Gazprom and E.ON thus became Ruhrgas, which had worked with Gazprom since 1970.[65]

Yet negotiations continued with Wintershall as well. Wintershall AG was a fully owned energy sector subsidiary of the chemical concern BASF AG. On 11 April 2005, at the Hannover International Trade Fair, Gazprom CEO Alexei Miller and BASF Chairman of the Board Jürgen Hambrecht signed a memorandum of

---

directors of Gazprom from 2001 to June 2002. Russian President's official website, <www.kremlin.ru>, last accessed in September 2008.

63 Gazprom Annual Report 2004, dated 17.05.2005. Inside observers concluded that even though the election of Gazprom's new board of directors was scheduled for 25.06.2004, it virtually took place at the 04.02.2004 Gazprom board meeting, with the main proposed candidates from the government already selected to the 2004 board of directors. Russian Petroleum Investor 13: 4 (April 2004), p. 36.

64 Russian Petroleum Investor 13: 9 (October 2004), p. 26ff, on 26.

65 Russian Petroleum Investor 14: 5 (May 2005), p. 53.

understanding with regard to natural gas production in Russia and elsewhere. As part of the agreement, Wintershall AG would receive a 49 per cent interest in a joint venture to construct the first phase of the NEGP.[66] On the same day in Hannover, Miller also met with the CEOs of E.ON and E.ON Ruhrgas, Wulf Bernotat and Burckhard Bergmann. The three company heads continued work on details of the memorandum of understanding signed in the summer of 2004. It had become apparent that the deal was a complex one that also included investments in the Russian gas industry. It was clear that BASF had reached an agreement first, but E.ON was still interested in the project. At the Hannover press conference Miller noted: "Now E.ON knows that it has a serious foreign competitor".[67]

On 15 February 2005, after a meeting with German Chancellor Schröder, Miller had announced that the NEGP would be in operation by 2010.[68] Finland and Fortum were now out of the picture, and so was the Finnish vision of turning Finland into a transit state. On 17 May 2005, the Gazprom board of directors approved the acquisition of the remaining 50 per cent interest in the joint venture North Transgas Oy, owned by Fortum Heat and Gas Oy. Fortum explained its withdrawal from North Transgas Oy as part of a "restructuring of its gas assets".[69] In reality, Fortum had lost interest in the project. As the hope for Finland to become a transit country had evaporated, Fortum had acquired new priorities. Besides, the German firms had taken a firm lead as foreign partners in the fundamentally Russian project.

On 8 September 2005, Russian President Vladimir Putin and German Chancellor Gerhard Schröder met in Berlin. During the meeting, Alexei Miller, Gazprom CEO, Jürgen Hambrecht, chairman of the board of BASF AG, and Wulf Bernotat, chairman of the board of E.ON AG, signed an agreement in principle to construct the NEGP. The parties would create a Russian-German joint venture, the North European Gas Pipeline Company (NEGPC) as the operator of the project. Gazprom would hold 51 per cent interest in the joint venture, and the German companies would each hold 24.5 per cent (through

---

66 Ibid., p. 49 and 54.
67 Ibid., p. 50.
68 Ibid., p. 55.
69 Fortum Corporation Interim Report, January-June 2005. Russian Petroleum Investor 14: 10 (November/December 2005), p. 48.

E.ON Ruhrgas AG and Wintershall Holding GmbH, respectively). It was now confirmed that the pipeline would allow Russia direct access to western EU markets, bypassing existing transit countries. Both the Russian and German sides regarded as a key prerequisite of the project that natural gas delivery through NEGP to the consumer would not be contingent on the political will of the transit countries, Poland, Ukraine, and Belarus. There would also be no transit fees as were paid when moving natural gas through other countries.[70] On 16 September 2005, Gazprom CEO Miller signed an order for the investment phase of the NEGP project.[71] Preparations for construction began, in particular in the Vologda and Leningrad Regions which in any case needed further natural gas infrastructure for their own use.[72]

Now Britain, then already a net importer of natural gas, felt left out. Two years had passed since the Putin-Blair meeting when a memorandum of cooperation had been signed. On 13 September 2005, the British Minister for Energy, Malcolm Wicks, speaking at a meeting of the Association of European Businesses in Moscow confirmed that Britain remained interested in Russian natural gas supplied via the NEGP. He also argued for British companies to participate in the project.[73]

It was really only from the September 2005 Schröder-Putin summit that the neighbouring countries began to comment on the project. Having been quite deliberately shut out of the project and at risk of losing both transit fees and political influence over the Russian gas trade with Western Europe, Poland and Ukraine opposed the construction of the NEGP. So did the Baltic states. Political leaders from the Baltic states and Poland, including Latvian Prime Minister Aigars Kalvītis, made attempts to persuade the EU that the decision by Russia and Germany to build the NEGP across the Baltic Sea was "ill-conceived" and that the project should not be implemented. Polish President Aleksander Kwaśniewski had by then already opposed the project, claiming that he was bewildered that Russia and Germany would carry out such a large-scale project while ignoring the economic interests of other EU member states. Kwaśniewski also argued that the NEGP project was environmentally disruptive, as well as "inef-

---

70 Russian Petroleum Investor 14: 10 (November/December 2005), p. 46 and 51.
71 Ibid., p. 46.
72 Ibid., p. 49.
73 Ibid., p. 52.

fectual from economic and political perspectives" and "a bad project". Others including Lithuania's Prime Minister Algirdas Brazauskas argued that construction of the NEGP would turn into an environmental catastrophe for the Baltic Sea and that Second World War-era chemical weapon caches on the Baltic seabed would be disturbed by the construction work and cause an ecological disaster.[74] In a controversial statement at a conference in Brussels on 30 April 2006, Polish Minister of National Defence Radosław Sikorski said the oil pipeline deal was in the Molotov-Ribbentrop tradition, in comparison to the 1939 Molotov-Ribbentrop non-aggression pact between the Soviet and Nazi German foreign ministers dividing Poland between the two countries.[75] Some even began to refer to the project as the Putin-Schröder pact.[76]

However, in Finland comments were muted. Since neither Sweden's government nor industry had yet been formally invited to participate, there were few immediate comments there either.

On 9 December 2005, construction work on the project began in the form of the welding of the first joint of NEGP, in the area of the Babayevo village in the Vologda Region. Among those attending the ceremony were Russian Prime Minister Mikhail Fradkov, Minister of Industry and Energy Viktor Khristenko, German Minister for Economy and Technology Michael Glos, Gazprom CEO Miller, and the chief executives of the German firms E.ON AG and BASF AG, Wulf Bernotat and Jürgen Hambrecht. The new German Chancellor Angela Merkel declined to participate.[77]

After the ceremony, it was announced that German ex-Chancellor Gerhard Schröder would become the future chair of the North European Gas Pipeline Company (NEGPC) shareholders' committee (board of directors). It also became know that Matthias Warnig, chairman of the Board of Directors of Dresdner Bank ZAO in the Russian Federation, had been proposed as mana-

---

74 Ibid., p. 51.

75 BBC News, 30.04. 2006; Der Spiegel Online, 01.05.2006.

76 Sinijärv, Riivo: The NEGP. Estonian Perspective. In: Baltic Mosaic. St. Petersburg Winter-Spring 2006), p. 7.

77 NEGP Press Release, 09.12.2005; Russian Petroleum Investor 15: 2 (February 2006), p. 12.

ging director of the NEGPC.[78] Neither appointment was totally unexpected, and the choice of Schröder had been preceded by rumours to that effect since 10 October.[79]

The appointment of Schröder caused a heated debate in Germany. While the energy industry generally considered the appointment a boon which would guarantee good relations with Gazprom and Russia, much of the media regarded the appointment as a disgrace or worse.[80]

As agreed, the joint Russian-German venture NEGPC was established in Zug, Switzerland, on 5 December 2005. Gazprom held 51 per cent in the joint venture and BASF and E.ON each had a 24.5 per cent stake. Zug was reportedly chosen because of its favourable taxation legislation.[81] Since Gazprom remained controlled by the Russian state, the project thus retained its character of a Russian state project although with, in the words of Putin, foreign investment. On 30 March 2006, the first official meeting of the shareholders' committee of the NEGPC was held at the Gazprom headquarters in Moscow. Gazprom proposed, and the committee elected, Gerhard Schröder as chairman.[82]

As managing director of the NEGPC, the Shareholders' Committee, as expected, appointed Matthias Warnig.[83] During the last decade of the Cold War, Warnig had been a Ministry for State Security (Ministerium für Staatssicherheit, MfS, since commonly known as the Stasi) officer in Dresden, at the same time when Vladimir Putin served there as a representative of the Soviet security service, the Committee for State Security (KGB). Putin served in East Germany with the

---

78 Russian Petroleum Investor 15: 2 (February 2006), p. 10; Russian Petroleum Investor 15: 6 (June/July 2006), p. 26.

79 Roth, Jürgen: Der Deutschland-Clan: Das skrupellose Netzwerk aus Politikern, Top-Managern und Justiz. Frankfurt am Main 2006, ch.7.

80 Russian Petroleum Investor 15: 2 (February 2006), p. 10.

81 Saar-Echo (Germany), 14.12.2005. Zug was already the home of another Gazprom joint venture, RosUkrEnergo. Fredholm, Michael: Natural-Gas Trade between Russia, Turkmenistan, and Ukraine: Agreements and Disputes. Asian Cultures and Modernity Research Report 15. Stockholm University 2008.

82 Russian Petroleum Investor 15: 6 (June/July 2006), 26; Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006).

83 Russian Petroleum Investor 15: 6 (June/July 2006), p. 26.

KGB from 1985 to 1990.[84] Warnig served with the Stasi from 1975 but was on duty in West Germany from 1986 to August 1989. Although Warnig and Putin claimed not to have met before St. Petersburg in October 1991, they had certainly been good friends for more than a decade.[85] Warnig's background too was duly noted by foreign observers, in Sweden and elsewhere.[86]

Moreover, although an office opened in Zug on 4 October 2006, the shareholders' committee decided to open a NEGPC branch office in Moscow as well.[87] It later became clear that important activities took place in Moscow, not Zug. Yet the consortium claimed that more than three quarters of the total staff of about 70 would work in Zug.[88] The same importance to the Moscow link seems to have applied to the appointment of Warnig, who in a meeting with the U.S. Ambassador in Moscow reportedly described himself as a "de facto employee of Gazprom."[89]

---

84 The Telegraph (UK), 27.02.2005; St. Petersburg Times (Russia), 01.03.2005; Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 145.

85 Die Welt (Germany), 03.08.2014; Der Spiegel (Germany) 35, 2008, p. 81. However, Roth refers to a former Stasi officer who claimed that Putin and Warnig met already in East Germany. Roth, Jürgen: Der Deutschland-Clan: Das skrupellose Netzwerk aus Politikern, Top-Managern und Justiz. Frankfurt am Main 2006, ch.7.

86 Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 21. According to one of the U.S. State Department cables exposed by Wikileaks, Ambassador John R. Beyrle at the U.S. Embassy in Moscow in 2009 apparently advised that "given Warnig's reportedly close friendship with Prime Minister Putin, we recommend the Department facilitate Mr. Warnig's meeting requests." Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

87 Russian Petroleum Investor 16: 1 (January 2007), p. 31; Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006). Apparently "a handful of employees" had met in Zug to establish a headquarters already in August 2006. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 4 and 21. They included Matthias Warnig and other senior managers. Kommersant (Russia), 30.08.2006.

88 Nord Stream: Nord Stream. The New Gas Supply Route to Europe (Nord Stream Press Information, 22.11.2006), p. 5.

89 According to one of the U.S. State Department cables exposed by Wikileaks. Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

5.1.2 Part 2: The Pipeline Project as a Hybrid Threat

The Swedish Government's Reaction

As noted, the Swedish government perceived the proposed NEGP as a threat to several Swedish core interests: the desire to gradually end European reliance on hydrocarbons as a key source of energy; the ambition to protect the Baltic Sea environment; and the desire to minimize naval activities in the Baltic. In addition to these laudable goals, there was the military dimension, the hard security threat, which in effect would overshadow the others.

It was known that a pipeline such as the NEGP might be used as a sensor platform for Russian military intelligence collection against Swedish targets. This was not a mere hypothetical scenario, nor was the installation of sensors only a precaution against terrorism, as the Russian side from time to time claimed.[90] As early as 2004, the Russian Baltic Fleet had implemented plans to install a radar station on an oil platform at the Kravtsovskoye deposit (known as D-6), located 22 km from the shore of Kaliningrad, to which the platform was connected with a pipeline, on the Baltic shelf and owned by the Russian oil company LUKoil-Kaliningradmorneft. This facility had been announced as the Baltic Fleet's first sea-based radar station and, due to the platform's position in the Baltic Sea, was described as a significant addition to the Baltic Fleet's surveillance capability.[91] Plans for integrated systems for monitoring air, surface, and underwater movements had already been announced in 1999, with the stated intention of guarding and defending littoral territories and sea zones against intrusion by submarines and surface ships as well as against saboteurs and terrorists from "groups of people or enemy states" through the use of a variety of sensor systems including over-the-horizon target acquisition radar, optronic surveillance systems, electronic reconnaissance systems, and sonar and electromagnetic surface and

---

90 Hinted at by Russian defense minister Sergei Ivanov already on 15.05.2006 in his comment that the Northern Fleet would be vested with the task of anti-terrorist defense and of providing security for the routes of transportation of Russian hydrocarbon resources to world markets. ITAR-TASS, 16.05.2006.

91 ITAR-TASS, 12.06.2004.

underwater target acquisition systems.[92] Besides, using underwater sensor chains as tripwires for monitoring submarines was not a new idea. During the Cold War, the United States and NATO had relied on its Sound Surveillance System (SOSUS), which consisted of seabed-mounted hydrophone arrays connected by underwater cables to facilities ashore, to detect Soviet ballistic missile submarines, in particular those which from bases in the Barents and White Seas aimed to gain access to the North Atlantic by rounding northern Norway and steering south through the Greenland-Iceland-United Kingdom (GIUK) gap.[93]

But cooperation between Russian military and energy sector actors went far beyond sensor platforms. On 27 September 2004, LUKoil and the Russian Ministry of Defence had signed a broad cooperation agreement on the provision of technical and financial assistance to a range of defence establishments, including the Rear Services and Transport Military Academy in St. Petersburg, the military hospital in Khimki outside Moscow, and the main personnel department of the Ministry of Defence. LUKoil would, in addition to continuing to supply the armed forces with fuel and lubricants, also attempt to find employment for those who were discharged from military service.[94] Meanwhile, Gazprom was developing a cooperation program with the Russian Navy, in

---

92 Baranenko, Anatoly/Belyayev, Vladimir/Klimov, Sergei/Kuzmenko, Anatoly/Sokolov, Sergei and Shcherbakov, Nikolai: Protection of 200-Mile Zone, a Priority Task of Coastal States. In: Military Parade: The Magazine of the Military Industrial Complex 31, January-February 1999, p. 48ff. The authors were distinguished, with Rear Admiral Baranenko the head of the Radio-electronic Warfare Center at the Naval Academy, Kuzmenko the Chief Expert of the Navy Directorate of the Rosvooruzhenie state enterprise, and the others affiliated to the Altair state research and production association. Additional information on the technology was published by Rear Admiral Baranenko in Soloviev, Igor/ Korol'kov, Grigoriy and Anatoly, Baranenko: Morskaya radioelektronika: Spravochnik. Politekhnika, 2003, ch. 2. See also Baranenko, A./Karpov, M./Demidovich, A. and Makarov Yu: BSN kak element boyevogo obespecheniya VMF (Shore observance system as an element of the Navy's combat support). In: Morskoy Sbornik: Zhurnal Boyenno-Morskogo Flota 1836 (November 1999), p. 58f. Written by a group of naval officers including Rear Admiral Baranenko, this article provides additional historical and technical information.

93 Whitman, Edward C.: SOSUS: The 'Secret Weapon' of Undersea Surveillance. In: Undersea Warfare: The Official Magazine of the U.S. Submarine Force 7: 2 (Winter 2005).

94 ITAR-TASS, 27.09.2004.

which naval vessels and infrastructure would be used in the development and transportation of liquefied natural gas (LNG) in the Barents Sea, and naval cooperation would be sought in the preparations for the construction of the NEGP. Gazprom had already begun its naval cooperation program on 19 October 2002, when Gazprom and the Russian Navy signed a protocol on intentions to promote interaction and long-term cooperation in Russian oil and natural gas offshore exploration and development. During 27-30 September 2004, Gazprom experts and Navy officers had jointly visited the Northern Fleet facilities, inspecting potential building sites for a gas liquefaction plant, and in January 2005, possible building sites had been examined by OAO Giprospetsgaz, the Gazprom subsidiary which also appeared in relation to the NEGP project in the Baltic. Gazprom announced its intention to cooperate with the Navy in the construction of the NEGP in March 2005.[95]

The dilemma for the Swedish government was how to act on the information that the pipeline project had the potential to be used as a sensor platform. Several powerful neighbours, including Russia and Germany, were determined to carry out the pipeline project. Another powerful European state, Britain, supported the project. And despite the military dimension, the pipeline was in its setup a commercial project.

Because of this dilemma, the Swedish government had to handle the situation in multiple dimensions. First, after the September 2005 agreement to build the NEGP, the Swedish Ministry of Defence sponsored the first of several studies on the project. These were prepared by the FOI, an assignment-based authority under the Ministry of Defence. This meant that the FOI conducted research on a fee basis, on topics chosen by whichever branch of government had sponsored the assignment. The FOI conducted research independently and it would be both incorrect and unfair to suggest that the FOI produced research results merely to satisfy the sponsor's preconceptions. Yet, since the sponsor initiated and paid for the assignment, it was only natural that the sponsor also suggested avenues of research. The FOI categorized the project as "Policy support to the Government (Defence)" and described it as a security, safety and vulnerability analysis.[96] In addition, the aforementioned inter-ministerial working group from

---

95 Gazprom press release, 18.03.2005; Gazprom 4 (April 2005), p. 5.

96 Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 2.

the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment was set up in the first half of 2006.[97] This resulted in a memorandum on the pipeline project, dated 15 March 2006.[98]

The Ministry of Defence took the lead in coordinating defences. In late 2006, after several months of deliberation, the Ministry of Defence requested seven agencies under its authority to investigate and assess the security, defence, and environmental implications of the pipeline project, including the possible implications of Russian naval vessels in the area and the potential to use the pipeline and its offshore platform for intelligence collection. The seven, which included the Armed Forces (which incorporated the Military Intelligence and Security Service, MUST), the national signals intelligence agency (FRA), the Emergency Management Agency (KBM), the Rescue Services Agency (SRV), the Coast Guard (KBV), the National Defence College (FHS), and the Defence Research Agency (FOI), were asked to provide written responses by 9 February 2007 and were also invited to a first hearing on 6 December 2006.[99]

By then, the pipeline issue was also being debated in the media. A key role came to be played by the FOI. The FOI studies were highly critical of the pipeline project. Even in the first FOI study of the NEGP, it was noted that the construction of the NEGP was assessed as increasing Russian leverage on the neighbouring states. The bypassed states (Poland, the Baltic states, Belarus, and Ukraine) would become more vulnerable to Russia if Russia chose to act coercively. In addition, the study concluded, the states which supported the project and would benefit from it (primarily Germany, Denmark, the Netherlands, and Bri-

---

97 Sveriges Television (SVT), Nyheter, 07.12.2006. The internal document, published by Swedish state television, was a Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006.

98 Näringsdepartementet (Ministry of Industry (Enterprise)), Naturgasledning i Östersjön - North European Gas Pipeline, Memorandum, 15.03.2006.

99 Försvarsdepartementet (Ministry of Defense): Inbjudan till hearing samt anmodan att lämna upplysningar m.a.a. den föreslagna rysk-tyska gasledningen Nord Stream, reference FÖ2006/2715/MIL, dated 17.11.2006. Released by the Ministry of Defense on 12.07.2014. The Swedish names of the latter agencies were Krisberedskapsmyndigheten (KBM), Statens räddningsverk (SRV), Kustbevakningen (KBV), Försvarshögskolan (FHS), and Totalförsvarets forskningsinstitut (FOI). The initiative was also announced in Riksdag & Departement 34, 2006, p. 7.

tain) were at risk of becoming more sensitive to Russian pressure, if Russia chose to apply it. The FOI was concerned that the NEGP would become a tool for Russia to impose its will on its near neighbours, which would affect Swedish national security.[100] These concerns were duly noted by the Swedish Ministry of Defence. In effect, Sweden worried that its neighbours would fall prey to appeasement politics in the event of future Russian aggression.

And then there was the sensor issue. The first FOI study in June 2006 raised the alarm in public for a direct Russian threat emanating from the proposed pipeline. The study noted that "[i]t can also be assumed that the NEGP have a military dimension, e.g. concerning military protection of the pipeline and usage of the infrastructure for military or intelligence purposes."[101] The second FOI study, published in early 2007, was yet more outspoken. The study concluded that the prospects for using the offshore compressor platform then planned for the pipeline as well as the pipeline itself "as platforms for active and passive sensors are rather good" and that "Russia would get a competitive intelligence edge concerning all subsurface, surface and aerial monitoring in the Baltic Sea."[102]

This issue was also raised in one of Sweden's leading dailies, *Svenska Dagbladet*. In November 2006, three days before the Ministry of Defence requested its ancillary agencies to investigate and assess the pipeline issue, the newspaper referred to an anonymous source with inside knowledge of the Swedish government's work with regard to the project. This source volunteered information that the pipeline and platform could be used as a structure on which to mount underwater sensors. The pipeline, which would traverse the entire Baltic Sea, would then become a tripwire which would register the movements of all vessels in its vicinity. It would in effect be impossible for Swedish or other military vessels, even submarines, to move without the Russian military registering each and every movement near or across the pipeline. The Russian capacity for early warning would be tremendous, and the capability of the Swedish navy to move undetected in times of crisis would in effect evaporate. Whether this leak from inside

---

100 Larsson, Robert L.: Sweden and the NEGP. A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. Stockholm 2006, p. 30ff.

101 Ibid., p. 32.

102 Larsson, Robert L.: Nord Stream, Sweden and Baltic Sea Security. Stockholm: FOI, March 2007, p. 37 and 49.

the Swedish government was intentional or not, the technical feasibility of using the pipeline as a sensor mount was confirmed by Rear Admiral Emil Svensson, head of underwater systems at the Swedish Defence Materiel Administration (FMV).[103] In light of this, the appointment of Warnig as managing director of the NEGPC appeared ominous. Even though by then he had long experience as a businessman, his Stasi background and known friendship with President Putin suggested that he might not be averse to letting intelligence sensor operators into the project.

Besides, Russian President Vladimir Putin had unexpectedly spoken out in terms that seemingly supported the Swedish concern over national security issues. On 25 October 2006, Putin said in a TV interview that the Russian navy would have to protect Russia's economic interests in the Baltic. Like in many other countries, including Britain, he noted, the navy would have to carry out purely economic tasks in addition to military ones. In this context, Putin specifically mentioned the pipeline project as "one or our most important priorities" and also spoke about involving the Russian Baltic Fleet in efforts to tackle a series of tasks in building the pipeline, since nobody knew the conditions of the Baltic better than the naval personnel.[104] These remarks were widely reported by the Swedish media.[105]

In fact, the Russian president echoed earlier comments by the Russian defence minister, Sergei Ivanov. In October 2005, he had concluded that military security was needed to protect offshore rigs, offshore operators, and for "supplying special services during the development and operation of offshore shelf depo-

---

103 Svenska Dagbladet (Sweden), 14.11.2006.

104 Pryamaya liniya s Prezidentom Rossii Vladimirom Putinym, 25.10.2006, TV transcript <www.liniya2006.ru>. The TV interview covered a large variety of topics and the pipeline issue was only one among many; yet it was only the pipeline-related comment which was noted in the Swedish press. Eventually, from December 2008 to February 2009 and from May 2009 to January 2010, the Baltic Fleet indeed cleared munitions identified in Russian waters in support of the pipeline project. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 45.

105 See, e.g. Svenska Dagbladet (Sweden), 14.11.2006.

sits."[106] On 15 May 2006, speaking about the Northern Fleet, Ivanov had concluded that

> "the state already has serious plans to develop large oil and gas fields in the Barents Sea. The Northern Fleet has a detailed knowledge of these plans because the fleet will definitely be vested with the task of anti-terrorist defence and of providing security for the routes of transportation of Russian hydrocarbon resources to world markets."[107]

Then, on 30 July 2006, Ivanov stated that Russia's national interests could not be protected without a naval component and also spoke specifically about the Baltic Fleet: "Its existence makes it possible to seriously influence military and political processes taking place on Russia's western frontiers."[108]

The Swedish Government's Position

Despite the comments by Putin and Ivanov, a difficulty for the Swedish government was that it had little freedom of action. Neither Sweden nor the other Baltic states could formally stop pipeline construction but they were involved in consultations which gave them the power to affect how quickly the project moved forward. In effect, they could obstruct and delay the project but not prevent it. According to international legislation, all states are entitled to lay submarine cables and pipelines on the continental shelf.[109] There was therefore no real way to refuse the project, even though the pipeline would pass through the Swedish exclusive economic zone. However, under the Espoo Convention of 1991, the state or enterprise which intended to lay such a pipeline first had to prepare an environmental impact assessment (EIA).[110] A pipeline project could, as a result, be refused upon environmental grounds, until such a time that an acceptable EIA had been prepared. Even so, this meant that it was only strictly environmental considerations associated with the construction or use of the proposed

---

106 ITAR-TASS, 28.10.2005.
107 ITAR-TASS, 16.05.2006.
108 RIA-Novosti, 30.07.2006.
109 United Nations Convention on the Law of the Sea of 10 December 1982, Article 79.
110 Convention on Environmental Impact Assessment in a Transboundary Context, signed at Espoo, Finland, on 25 February 1991.

pipeline which might be used to delay the project, and only until such harmful effects upon the environment had been neutralized.

The Swedish government was therefore bound to approve the pipeline project, as long as the consortium submitted a substantive EIA. The closed debate within the Swedish government on what means might be available to stop or at least delay the project until it became unfeasible for economic or practical reasons is evident from the aforementioned internal Swedish government document from August 2006 on the proposed pipeline produced by an inter-ministerial working group from the ministries for foreign affairs, industry (enterprise), defence, agriculture, and the environment, exposed by Swedish state television. The document concluded that the project was not in Sweden's interest, that Sweden would not benefit from it, and that its many disadvantages would have a considerable negative impact on Sweden. The document listed several areas of negative impact: environmental risks especially with regard to the huge volumes of unexploded munitions (regular munitions, chemical warfare munitions, and mines) known to have been dumped in the Baltic Sea; reasons of national security including the issue of underwater sensors, the potential of Russian signals intelligence collection from the offshore platform, and the risk of an increased Russian military presence in the Swedish exclusive economic zone tasked with protecting the pipeline and offshore installation; the impact on the fishery industry; and the resulting loss of freedom of action within the exclusive economic zone. The document also suggested strategies to contain the threat. The options were quite limited. It might be possible to rely on an exemption within the United Nations Convention on the Law of the Sea by referring to the serious environmental implications of the project. In the event the consortium's EIA discussed other routes with less environmental impact or alternatives which simply were cheaper to build, the government would have cause to refuse the project (Article 5 in the Espoo Convention noted that the EIA might allow for consultation on possible alternatives to the proposed activity, including the no-action alternative and possible measures to mitigate significant adverse transboundary impact). With regard to the potential for Russian intelligence collection, the document concluded that even if the Swedish government accepted the EIA and gave the necessary permits to build the pipeline, the permit would then only cover the commercial activities of the consortium, never any intelligence use of the infrastructure by state actors. Besides, the document duly noted that according to Article 60 in the United Nations Convention on the Law of the Sea, the coastal State shall have the exclusive right to construct and to authorize

and regulate the construction, operation, and use of offshore platforms such as the compressor platform planned by the consortium in the exclusive economic zone. The authors of the document consequently noted that if the government refused the construction of the offshore platform, the entire project might become so expensive or possibly even technically unfeasible that the consortium might give up. However, they also concluded that political pressure, from the consortium as well as other states such as Russia or Germany, with the aim of making Sweden issue the required permits for the project would have to be expected.[111]

In other words, the environmental impact was important, but it was the proposed offshore platform which was the key. Not only did it pose a threat to national security, it was also the one component of the project which the Swedish government could legally refuse.

An analysis of the Swedish media shows that it was indeed the military dimension of the pipeline project which came to dominate the public Swedish debate, which can be said to have been opened in July 2006 by retired Ambassador Krister Wahlbäck, an academic who had retained contacts within the Foreign Ministry, in an opinion article in the influential daily *Dagens Nyheter*.[112] Wahlbäck claimed that, earlier in the summer, he had met officials from the German Foreign Ministry who had then said that they expected Sweden to approve the pipeline project. There is little reason to believe that Wahlbäck was unaware of the ongoing internal debate within the Swedish government when he published his article. The first FOI study had been published the previous month. Besides, the key arguments raised in the internal document (dated a week later but surely then already in the making) were also raised by Wahlbäck, including the possibility that the pipeline facilities would be used for Russian intelligence collection. In addition, the same evening following its publication, Wahlbäck appeared on national television together with Minister of Education and

---

[111] Sveriges Television (SVT), Nyheter, 07.12.2006, which exposed and published the aforementioned Policy Memorandum from the Ministry of the Environment, dated 8 August 2006.

[112] Wahlbäck, Krister: Stoppa ryska gasledningen som hotar Östersjöns hälsa ("Stop the Russian gas pipeline which threatens the health of the Baltic Sea"). Dagens Nyheter (Sweden), 31.07.2006.

Culture Leif Pagrotsky, who commented on the pipeline project in a semi-private capacity.[113]

Wahlbäck began his article by arguing for environmental concerns, yet he focused on economic and national security issues. This became the pattern of the public debate. While many newspaper articles on the projected pipeline predictably mentioned the environmental concerns raised by the project, they often did so only in passing, without giving any substantial information. This was in contrast to newspaper articles on the economic and security aspects of the project. The press treated the environmental effects as self-evident or merely used the environment as a dramatic enhancer. A study on how the Swedish press reported the pipeline issue determined that the information category most frequently covered by the press was the economy, which appeared in 71 per cent of the articles in which the pipeline appeared in the influential daily *Dagens Nyheter* from March 2002 to May 2008. The second most important information category was national security, which appeared in 62 per cent of the articles. In comparison, environmental aspects of the project were mentioned in only 39 per cent of the articles. When passing mentions were excluded, the pattern became yet clearer: 68 per cent of the articles included substantial information on the project's economic aspects, 59 per cent provided the same on national security aspects, and only 25 per cent did the same with regard to the project's environmental aspects. And of the articles which dealt with the environmental implications, 11 per cent in fact downplayed environmental concerns.[114]

Even so, this focus on economics versus national security was not acknowledged by the press itself. In fact, in November 2006, the national daily *Svenska Dagbladet* noted in the aforementioned major article on the national security implications of the pipeline project that "so far, the Swedish debate has been on the environmental risks"—but went on to describe

---

113 Roos, Lars André: Politiska nätverk och Nord Stream. En möjlighet att vara med och påverka. Report, Karlstads universitet 2007, p. 8.

114 Fransson, Anna-Lisa Sayuli/Elander, Ingemar and Lidskog, Rolf: Framing Issues and Forming Opinions: The Baltic Sea Pipeline in the Swedish Media. In: European Spatial Research and Policy 18: 2 (2011), p. 102, 103 and 104.

the entire pipeline project as a potential national security problem.[115] On the very same morning, the leading daily *Dagens Nyheter* published a substantial opinion article on the national security aspects of the project by the opposition Social Democratic party's national security spokesperson, Ulrica Messing. This article too began by concluding that "the perhaps most obvious threat – the environmental threat – has received considerable and deserved attention, whereas another at least equally important factor so far has been ignored"—which was the national security implication.[116] Yet, an examination of the contents of the newspaper articles devoted to the project shows that as of this particular date, only 6 out of 28 articles in *Dagens Nyheter* had dealt with environmental issues.[117] Sweden's official core interests focused on the environment but they took little space in either the public or internal government debate.

The two leading Swedish dailies raised the national security aspects of the pipeline project on the very same day that the Nord Stream consortium submitted its formal notification of intent. On the same day, Sweden's Defence Minister Mikael Odenberg made common cause with his opposition counterpart, Messing, explaining in a national public radio interview that "[t]his kind of pipeline can be used as a platform for intelligence collection. This naturally causes concerns. It brings security and defence repercussions for us."[118] On the following day, a printed interview with Defence Minister Odenberg was even more outspoken, as Odenberg was cited as explaining that "[w]e get a gas pipeline which motivates a Russian naval presence in our economic zone and which the Russians, if they wish, can exploit for intelligence collection. This is obviously a problem."[119]

Sweden, by the way, was not the only country which by then had noted the national security aspects of major energy sector projects. For several years, the German intelligence service, the Bundesnachrichtendienst (BND), had

---

115 Svenska Dagbladet (Sweden), 14.11.2006.

116 Dagens Nyheter (Sweden), 14.11.2006. Messing subsequently published, alone or with party colleagues, a number of identical or almost identical articles in various Swedish provincial newspapers. See, e.g. Blekinge Läns Tidning, 17.11.2006; Gotlands Allehanda, 17.11.2006; Barometern Oskarshamns-Tidningen, 20.11.2006; Ljusdals-Posten, 24.11.2006.

117 Fransson, Elander, and Lidskog, "Framing Issues and Forming Opinions," p. 105.

118 Sveriges Radio (Sweden), 14.11.2006.

119 Dagens Nyheter (Sweden), 15.11.2006.

organized public seminars on important issues. On 12 October 2006, the BND held its "BND Symposium 2006" in Berlin. The topic was "Energie - Quelle von Konflikt und Kooperation/Energy - Source of Conflict and Cooperation" which in light of the pipeline debate was highly topical. During the Symposium, Germany's chief of the Chancellor's office and federal minister of special affairs as well as Federal Government Commissioner for the Intelligence Services (*Kanzleramtsminister*) under Chancellor Merkel, Thomas de Maizière, noted that Germany's and Europe's energy supply by no means was secure. Cooperation with Russia was necessary, or the Russian natural gas risked being diverted to China, de Maizière warned, in the same way that other energy streams risked being diverted to the United States. The intelligence service would have to pay particular attention to the strategic developments within the energy sector, and would have to contribute to the nation's energy supply, he concluded.[120] There was little doubt during the Symposium that the German side considered the pipeline project across the Baltic a key priority, although the Germans too were suspicious of Russia's ultimate intentions. Germany's diplomatic lobbying in favour of the project would continue. When Günter Gloser, German Minister of State for Europe, visited Sweden in April 2008, he concluded that Nord Stream was "essential" to meet European demand for gas.[121] And when in June 2009 the U.S. Ambassador in Moscow asked whether

---

[120] de Maizière, Thomas: Unsere Energieversorgung ist keineswegs gesichert. Speech at the BND Symposium 2006: Energie - Quelle von Konflikt und Kooperation/Energy - Source of Conflict and Cooperation, Berlin 12.10.2006, subsequently published in the German Federal Government web site, www.bundesregierung.de. His exact words were: "Unsere Energieversorgung ist keineswegs gesichert. [...]Auch die Energieversorgung Europas kann keineswegs als gesichert angesehen werden. [...] Selbst das Gas aus Nordwestsibirien, das seit langem mehr als ein Drittel unserer Erdgasimporte sichert und damit unverzichtbar ist, könnte zu einem Teil nach China abfließen. Entsprechende Äußerungen russischer Verantwortlicher haben in den letzten Monaten in Europa beträchtliche Unruhe verursacht. [...] Diese Entwicklungen zu beobachten und zu analysieren ist eine wichtige Aufgabe auch und vor allem für Nachrichtendienste. [...] Eine verlässliche und wirtschaftliche Versorgung mit Energie ist keine Selbstverständlichkeit. Sie ist eine zentrale Aufgabe, dazu können auch die Nachrichtendienste beitragen."

[121] Gloser, Günter, Minister of State for Europe: The European Partnership with Russia, speech at the Swedish Institute of International Affairs, Stockholm 01.04.2008, transcript.

the Nord Stream project had the full support of the German government, the managing director of Nord Stream, Matthias Warnig, reportedly

> "said yes, noting that he has regular, direct access to Chancellor Merkel's office and that Nord Stream Chairman Gerhard Schroeder also meets frequently with Merkel. However, Warnig lamented that Russian diplomacy is sometimes heavy-handed and counterproductive."[122]

Whether Russia's intelligence services took active part in support of the Nord Stream project remains unknown to outside observers, even though rumours to this effect were in sway.[123] Indeed, the Russian media noted that in Germany accusations were directed against Gerhard Schröder who some claimed had already fallen into the hands of Russian intelligence during his term as Chancellor.[124]

The Seabed Surveys

It was not only the initiative to build the pipeline which came from the Russian state. So did the decision to launch the first seabed surveys in anticipation of constructing the pipeline. In addition, they were carried out in part by Russian naval personnel.

---

122 According to one of the U.S. State Department cables exposed by Wikileaks. Reference ID #09MOSCOW1530, dated 11.06.2009. <http://wikileaks.org>.

123 According to one of the U.S. State Department cables exposed by Wikileaks, an American diplomat on 03.11.2009 met with Estonian Member of Parliament Marko Mihkelson, Chair of Parliament's European Affairs Committee. Mihkelson reportedly claimed that "Russian foreign intelligence officers (SVR) have been active in Estonia investigating opposition to the pipeline. This he saw as clear evidence Nord Stream is a political, not economic project." Mihkelson also reportedly noted that militarily, Russia had used the defense of Nord Stream as an element of its September 2009 Ladoga and Zapad military exercises, during which Russia and Belarus had practiced fending off an attack from the direction of the Baltic States. Reference ID #09TALLINN325, dated 06.11.2009. <http://wikileaks.org>. While the exposed cable was cited widely, it in no way proves that the SVR operated in support of the Nord Stream project. At most, the cable suggests that there was a belief among some policy makers that the SVR was so engaged.

124 Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 141.

The first seabed survey was commissioned in 1998 by the company North Transgas as part of the first feasibility study.[125] The consortium later claimed to have asked the Swedish firm Marin Mätteknik AB (MMT) and Geoconsult in July-September 1998 to carry out the work.[126] Yet the study was carried out by AO PeterGaz, a Gazprom subsidiary. PeterGaz subsequently claimed that permits had been issued by the national authorities of the countries involved; presumably the firm considered the aforementioned protocol signed on 3 December 1997 by Russian First Deputy Prime Minister Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Sundström equal to a permit.[127]

PeterGaz also carried out the first surveys for NEGP. The first was initiated in 2004, conducted in October 2005 and consisted of a geophysical survey of the seabed in a corridor two kilometres wide along the proposed route. Two potential routes were chosen. In 2006, yet another survey took place. This was more detailed, along a corridor 180 meters wide.[128] The Swedish government in fact issued a permit in 2005 which was renewed and applied also for 2007.[129] At a minimum, the 2005 and 2006 surveys involved Russian naval personnel onboard the research ships, R/V *Professor Shtokman* and R/V *Akademik Golitsyn*, for instance when the latter carried out survey work "on behalf of Gazprom" in the Gulf of Finland and around the Danish island of Bornholm. Nord Stream AG later claimed that Russian naval personnel only participated when in Russian waters, but this was clearly incorrect with regard to the survey work around Bornholm.[130]

---

125 Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>.

126 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 41.

127 Nord Stream: Nord Streams kartläggningsaktiviteter i överensstämmelse med internationella och nationella rättsliga krav. Press release. 30.08.2007. On PeterGaz, see company web site, <www.petergaz.com>.

128 Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>; Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 4; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 15 and 41.

129 Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), dated 08.08.2006; Dagens Nyheter (Sweden), 02.02.2007.

130 Krasnaya zvezda (Russia), 25.07.2007; citing Fleet Admiral Vladimir Masorin, commander of the Russian Navy; Nord Stream: Nord Streams kartläggningsaktiviteter i

Whether Russian naval personnel in fact participated along the entire route remains unknown to outside observers. At any rate, their participation was hardly surprising since President Putin had suggested that the Russian Baltic Fleet would be involved in the construction work and Dmitry Shilyayev, head of the PeterGaz research department, later reportedly acknowledged that the Baltic Fleet would use modern deepwater unmanned devices for the control both of the route and the quality of laying the pipeline.[131] The two research vessels, R/V *Professor Shtokman* and R/V *Akademik Golitsyn*, had formerly been registered as state-owned, belonging to the Soviet Academy of Sciences, but had since been re-registered as belonging to Gazflot, a Gazprom-affiliated company. They were advanced research vessels of the types which were repeatedly suspected of involvement in intelligence collection during the last years of the Cold War, owing to their advanced communications and survey equipment and often unusual sailing patterns.[132] As research vessels, they were eminently suitable for survey missions. In September-December 2006, for instance, the *Akademik Golitsyn* surveyed the entire sea route of the proposed gas pipeline utilizing video camera equipped underwater apparatus, with experts from PeterGaz alongside the naval personnel.[133] Other research vessels which participated included the *Akademik Mstislav Keldysh* and *AtlantNIRO*, operated by the Russian Academy of Sciences and AtlantNIRO, a research institute subordinated to the Russian Federal Agency for Fisheries, respectively. The vessels and institutes involved in the surveys thus show a clear pattern of Russian state control. However, from 2007, when the NEGPC had become Nord Stream AG, non-Russian survey ships were chartered as well. The consortium, for instance, employed a Swedish company, Marin Mätteknik AB (MMT), which specialized in sea measurements and geology, for the con-

---

överensstämmelse med internationella och nationella rättsliga krav. Press release. 30.08.2007.

131 Putin in Pryamaya liniya s Prezidentom Rossii Vladimirom Putinym, 25.10.2006, TV transcript <www.liniya2006.ru>; Russian Petroleum Investor 16: 10 (November/December 2007), p. 30. Shilyayev presumably referred to a remotely operated vehicle (ROV).

132 See, e.g, Agrell, Wilhelm: Bakom ubåtskrisen: Militär verksamhet, krigsplanläggning och diplomati i Östersjöområdet. Stockholm 1986, p. 176f.

133 Russian Petroleum Investor 16: 10 (November/December 2007), p. 30; citing Dmitry Shilyayev, head of the Petergaz research department.

tinued environmental studies and seabed survey. MMT began with a survey of construction routes in the area of Bornholm Island in May 2007.[134] The firm used a multipurpose offshore support vessel named *Pollux*.[135]

By then, Nord Stream AG was in the process of contracting with a large number of international companies and institutions. Quite a few were Swedish, including some which were state-owned. In addition to MMT, the consortium hired, among others, SSPA (formerly *Statens Skeppsprovningsanstalt*, Sweden); Geological Survey of Sweden (*Sveriges geologiska undersökning*, SGU, Sweden); Stockholm University; IVL *Svenska Miljöinstitutet* (Sweden); Environmental Resources Management (ERM);[136] DOF Subsea (Norway) and continued to rely on PeterGaz (Russia) for the seabed survey and technical engineering for the Russian section. In addition, Nord Stream AG hired the Danish consultancy company Rambøll[137] to prepare the EIA; Institut für Angewandte Ökologie (Institute for Applied Ecology, Germany) to conduct additional Baltic Sea environmental studies; and the company Det Norske Veritas (DNV, Norway) for controlling and certification. Saipem Energy Services (formerly Snamprogetti, Italy) would have the lead for the technical engineering process, while Saipem (Italy) would be responsible for pipe laying. EUPEC (France) would be responsible for logistics (concrete coating, pipe storage, transport), while EUROPIPE (Germany) would manufacture the majority (75 per cent) of the pipes

---

134 Russian Petroleum Investor 16: 10 (November/December 2007), p. 30; citing MMT founder and managing director Ola Oskarsson and others. On the AtlantNIRO, see the institute web site, <www.atlantniro.ru>. On MMT, see company web site, <www.mmt.se>.

135 Grigory Pasko: The Nord Stream Chronicles, 20.06.2008; see <www.robertamsterdam.com>. MMT among other systems employed a remotely operated vehicle (ROV).

136 Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 28 and 93.

137 On this company, see Rambøll web site, <www.ramboll.com>. Rambøll had carried out the first feasibility studies for the pipeline project already at the time of North Transgas Oy. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 26.

needed for the first line, and OMK (Russia) the remaining 25 per cent of pipes. PetrolValves (Italy) would supply the necessary valves.[138]

NEGP Becomes Nord Stream, and the EIA Approval Process Begins

On 4 October 2006, coincidentally a week before the BND Symposium, the North European Gas Pipeline Company (NEGPC) changed its name to Nord Stream AG and opened its head office in Zug, Switzerland.[139] On the following day, 5 October 2006, the Dutch gas firm N.V. Nederlandse Gasunie became the fourth member to join the pipeline consortium. Gasunie CEO Marcel Kramer and Gazprom CEO Alexei Miller signed a Memorandum of Understanding in Moscow, with Dutch Minister of Economic Affairs Joannes Gerardus (Joop) Wijn attending the meeting. Gasunie would eventually acquire 9 per cent of Nord Stream equity out of the German-held shares.[140]

As noted, the Swedish counterstrategy relied on the legal requirement that the pipeline construction project would have to undergo an EIA in line with the Espoo Convention and national legislation of the concerned countries. The EIA authorities in Germany, Denmark, Sweden, Finland, and Russia had already agreed, in a meeting on 19 April 2006, that the pipeline project would be handled under the Espoo Convention. The Espoo Convention called for submitting a notification of intent about the project to responsible authorities in those countries (Russia, Finland, Sweden, Denmark, and Germany), the exclusive economic zones of which would be crossed by the pipeline, as well as in neighbouring states such as Poland, Latvia, Lithuania, and Estonia. The consortium submitted the notification documentation to the littoral states of the Baltic Sea on 14 November 2006.[141] In the 80-page Project Information Document, the

---

138 Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG. See also Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 95.

139 Russian Petroleum Investor 16: 1 (January 2007), p. 31; Nord Stream: The New Gas Supply Route to Europe. Press release. 22.11.2006.

140 Russian Petroleum Investor 16: 1 (January 2007), p. 31.

141 Nord Stream: Project Information Document – Swedish Version (November 2006), dated 24.10.2006. This was the document submitted with the notification to the littoral states of the Baltic Sea on 14.11.2006. On the 19.04.2006 meeting, see p. 32.

venture was described as an offshore natural gas transmission system consisting of two separate pipelines crossing the Baltic Sea between Russia and Germany. The second line would be built after the first one. Consultations with competent bodies and the public at large were also planned, along with the preparation of a program and EIA report. The EIA report was then expected to be finalized in the fall of 2007, and Nord Stream hoped to have the EIA approved in early 2008.[142] In fact, Nord Stream optimistically planned that the materials acquisition would already begin in April 2007 and that the first line would be laid by December 2009.[143]

Nord Stream submitted different EIA reports to each country, since each was responsible for its exclusive economic zone.[144] In Sweden, the Environmental Protection Agency administered the EIA approval process. After Nord Stream AG had submitted its notification of intent, Sweden followed protocol, publis-

---

142 Sveriges Radio (Sweden), 14.11.2006; Nord Stream: Nord Stream. The New Gas Supply Route to Europe. Press release. 2211.2006; Russian Petroleum Investor 16: 1 (January 2007), p. 34f.

143 Followed by the second line from November 2011 to October 2013. Nord Stream, Nordeuropeiska gasledningen (NEGP) (Sjödel): Bilaga till anmälan till utsatta parter enligt artikel 3 i Esbokonventionen. Zug 2006, p. 3. The document, which accompanied the notification to the littoral states of the Baltic Sea on 14.11.2006, was marked as a preliminary version, yet was the one submitted.

144 See, e.g. Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 121. In Denmark, the approval process was administered by the Forest and Nature Agency, Ministry of the Environment; in Estonia, by the Ministry of Environment; in Finland, by the Ministry of the Environment; in Germany, by the Federal Maritime and Hydrographic Agency (Bundesamt für Seeschifffahrt und Hydrographie); in Latvia, by the Ministry of Environmental Protection and Regional Development of Latvia; in Lithuania, by the Ministry of Environment; in Poland, by the Ministry of Environment; and in Russia, by the Department of International Cooperation in the Field of Environmental Protection and Nature Use of the Ministry of Natural Resources of the Russian Federation. Swedish Environmental Protection Agency (Naturvårdsverket), Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference Dnr 121-7846-06 Rv, dated 14.11.2006, p.4; Federal Maritime and Hydrographic Agency, Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, n.d. (November 2006).

hing the notification with a request that all relevant agencies and authorities would comment by 26 January 2007.[145] A number of comments came in, and on 16 February 2007, the compiled comments were sent to Nord Stream AG.[146] In Sweden, two permits were needed. The part of the pipeline located in the Swedish exclusive economic zone would require a permit under the Act of the Continental Shelf. The permitting authority was the Government (Ministry of Industry (Enterprise), Employment and Communications). As for the offshore service platform, it would require a permit under the Act of the Swedish Economic Zone. The permitting authority was again the Government (Ministry of Sustainable Development, that is, the Environment).[147]

Meanwhile the Nord Stream consortium continued to promote the project. Problems soon appeared. In early 2007, the government of Finland recommended Nord Stream AG move the projected route in the Gulf of Finland further south, into the exclusive economic zone of Estonia. On 31 May 2007, Nord Stream AG turned to Estonia with a request to survey the possibilities for a change of route. However, by then relations between Estonia and Russia had grown increasingly tense, in particular because of the controversy of the Bronze Soldier, a Soviet Second World War memorial which had recently been moved out of the city centre of the Estonian capital. In September 2007 the Estonian parliament refused Nord Stream's request.[148]

---

145 Naturvårdsverket, Synpunkter på underlag för miljökonsekvensbeskrivning för Nord Stream Gas Pipeline, reference Dnr 121-7846-06, dated 17.11.2006.

146 Naturvårdsverket, Synpunkter på Nord Stream AG:s planerade gasledning genom Östersjön öster om Gotland (Naturvårdsverket, press release, 17.11.2006); Naturvårdsverket, Synpunkter inför utarbetandet av miljökonsekvensbeskrivning (MKB) för den planerade nordeuropeiska gasledningen Nord Stream och prövningarna enligt kontinentalsockellagen och lagen om Sveriges ekonomiska zon: Yttrande, reference Dnr 382-216-07, dated 15.02.2007; Larsson, Nord Stream, Sweden and Baltic Sea Security, 25.

147 Swedish Environmental Protection Agency (Naturvårdsverket), Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference Dnr 121-7846-06 Rv, dated 14.11.2006, p. 2.

148 See, e.g. BBC News, 28.04.2007; Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 116ff; Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 72.

Poland too attempted to thwart the project, among other concerns arguing that the pipeline would hinder future dredging of the seabed to accommodate a route for tankers to reach Poland.[149] This objection was eventually overcome as well.[150]

So far, no EIA had yet been submitted. However, by the end of 2007, Nord Stream AG noted that Denmark and Germany were in agreement with the Russian position, while negotiations with Sweden were still ongoing. Nord Stream hoped for a constructive position by Sweden, claiming that the Swedish authorities had already agreed to a route within Sweden's economic zone. Presumably Nord Stream meant the aforementioned protocol signed on 3 December 1997 by Russian First Deputy Prime Minister Nemtsov and Swedish Industry (Enterprise) and Commerce Minister Sundström and the undisputed, by Sweden, TEN-E status of the project.[151]

On 21 December 2007, Nord Stream AG submitted the EIA to the Swedish government and applied to lay a pipeline in the Swedish exclusive economic zone.[152]

The Nord Stream project was by no means an issue only between Sweden and the consortium. The pipeline had been debated in the European Parliament as

---

149 Letter from Minister of the Environment Jan Szyszko to the Swedish Environmental Protection Agency, reference DOOS-082/ /2007/AK, sent as part of the notification process.

150 But not until February 2010 when a route change was approved in German waters. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 72 and 75.

151 Russian Petroleum Investor 16: 10 (November/December 2007), p. 30. On 06.09.2006, the European Commission confirmed the project's status within the Trans-European Network (TEN-E). Decision No 1364/2006/EC of the European Parliament and of the Council of 06.09.2006 laying down guidelines for trans-European energy networks. The project was mentioned in an appendix among many others. Although the decision on TEN-E status was formalized only in 2006, the actual deliberation on TEN-E projects took place already on 17.06.2005, before the September 2005 Schröder-Putin summit which alerted the neighbouring countries to the immediate realization of the pipeline project. It is highly unlikely that either EU or national political decision-makers took notice of the implications of each and every project listed in the appendix when the list was compiled.

152 Ministry of the Environment, press release, 21.12.2007.

well, and the Directorate-General for Internal Policies had scrutinized the project.[153] On 29 January 2008, a public hearing on the Nord Stream project was organized by the Committee of Petitions, in association with the Committee on Foreign Affairs and the Committee on Industry, Research and Energy of the European Parliament. A number of critical voices were raised, particularly by members of parliament from Britain, Poland, Lithuania, and Estonia, as well as by a representative of Sweden's FOI.[154]

On 12 February 2008, the Swedish government rejected the application as incomplete, claiming the need for a more complete EIA.[155] Nord Stream had to begin work on a second EIA. A period of intensive Nord Stream lobbying then began (see below), to secure the approval of the second application, when it finally would be ready. However, various Swedish interest groups continued to express negative views on the project. So did the German media. On the day following Sweden's rejection of the application, the German weekly *Stern* argued that serious questions remained with regard to the sensors issue, and also the fibre optic communications cable which would accompany the pipeline. *Stern* had noted that the sensor monitoring data would end up in Moscow in addition to Zug. Besides, *Stern* observed, in a previous pipeline project built through Poland (the Yamal pipeline), Gazprom had installed its own telecommunications system without first informing the Polish authorities. As it turned out, the main source

---

153 See, e.g. European Parliament, Directorate-General for Internal Policies: The Nord Stream Gas Pipeline Project and its Strategic Implications: Note. Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Petitions, PE 393.274, 2007.

154 Nord Stream: Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008. Nord Stream AG produced the document immediately following the 29.01.2008 hearing. Among the participants were Robert Larsson of the Swedish FOI and Andrew Riley of City University, London.

155 Miljödepartementet and Näringsdepartementet: Begäran om komplettering av ansökan om tillstånd till utläggande av rörledningssystem enligt lagen (1966:314) om kontinentalsockeln och ansökan om tillstånd till uppförande och användning av en serviceplattform enligt lagen (1992: 1140) om Sveriges ekonomiska zon.. 12.022008. Reference M2007/5568/F/M, N2008/147/FIN; Andreas Carlgren: Miljödepartementet, Regeringens prövning av gasledning i Östersjön. Press meeting. 12.02.2008.

for the *Stern* article was the Swedish FOI.[156] The German media apparently found the FOI conclusions more persuasive, or at least better copy, than those of the German government, which remained in favour of the project, as was evident from the aforementioned remarks by Günter Gloser, Minister of State for Europe, in April 2008.[157]

The Modified EIA

On 1 October 2008, the Nord Stream consortium updated and modified its application, that is, in effect submitted a second one. The application to build an offshore service platform, the one feature of the project which the Swedish government could legally refuse, was thereby formally withdrawn.[158]

Would the Swedes accept the updated EIA? On 12 November 2008, Putin himself joined the fray. In a meeting in Moscow with Finland's Prime Minister Matti Vanhanen. Putin suddenly declared that if Europe was unwilling to accept the pipeline, then Russia would instead build LNG plants and ship the LNG in a fleet of tankers.[159] The option of using LNG tankers was again raised in Sep-

---

156 Larsson, Robert L.: Security Implications of the Nord Stream Project (FOI Memo, 12.02.2008, reference FOI-R-2336-SE), p. 15; Stern (Germany), 13.02.2008.

157 Gloser, Günter, Minister of State for Europe: The European Partnership with Russia, speech at the Swedish Institute of International Affairs, Stockholm 01.04.2008, transcript.

158 Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6; Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009. Nord Stream had already in early 2008 admitted that no offshore platform was necessary. Nord Stream: Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea", European Parliament, Brussels. 29.01.2008, p. 11. Nord Stream AG produced the document immediately following the 29.01.2008 hearing. Realizing that Sweden would not grant a permit for the offshore platform, Nord Stream abandoned this part of the project. Nord Stream claimed to have withdrawn the application to build an offshore platform on 08.04.2008. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 69.

159 Reuters, 12.11.2008; Dagens Nyheter (Sweden), 13.11.2008.

tember 2009.[160] The threat of using tankers rather than a pipeline was bound to make an environmental impact.[161] Moving the gas as LNG in tankers would be more expensive, and Putin no doubt knew that the environmental impact of increased shipping in the Baltic would worry Sweden and other Baltic powers more than that of the pipeline. According to some calculations, transporting the same annual amount of natural gas through the Baltic Sea by ship would demand from five hundred to six hundred LNG tankers, and tanker collision would be a real danger.[162] In early 2008, Nord Stream AG had indeed argued that more than six hundred tankers per year would be needed in the Baltic.[163]

Other European countries proved more amenable to the Nord Stream project than Sweden. In June 2009, Russia's Ministry of Natural Resources and Ecology (MNRE) noted that Russia, Denmark, and Germany, following the latest round of consultations in Germany, had concluded that the project did not entail material environmental risks.[164] On 30 June 2009, Russia's Regional Water Administration issued a water permit for construction in Russian waters.[165] Soon after, in July 2009, positive news came from Finland as well. The Finnish environmental regulator concluded that construction of Nord Stream did not represent a seri-

---

160 Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 101.

161 The environmental implication of LNG tankers in the Baltic had been raised by the FOI already in early 2007. FOI, Yttrande till Försvarsdepartementet rörande Nord Stream och gasledningen genom Östersjön, 06-1964:3, dated 07.02.2007. Written response to Ministry of Defense request for information FÖ2006/2715/MIL, dated 17.11.2006. By 2009 (if not before), it was also known that the Swedish Coast Guard opposed the idea to bring more tankers into the Baltic Sea. Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 22.

162 European Parliament, Directorate-General for Internal Policies: The Nord Stream Gas Pipeline Project and its Strategic Implications: Note. Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Petitions, PE 393.274, 2007, p. 2. The document carries no exact date but was produced after 14.11.2007.

163 Nord Stream, Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008, p. 5. Nord Stream AG produced the document immediately following the 29.01.2008 hearing.

164 Russian Petroleum Investor 18: 8 (September 2009), p. 22.

165 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73.

ous environmental threat for Helsinki. While the Russian side took this as an approval, the conclusion did not represent a final assessment so more would be needed. However, the project could move to the next approval stage, according to the Finnish environmental preservation agencies. This was the Uusimaa Regional Environment Centre which, although it considered Nord Stream AG's environmental impact assessment to be sufficient in its fundamental aspects, required further investigations, including that of the spread of nutrients and harmful substances during the project; ensuring maritime safety during construction; restricted zones for fishing and trawling; continuous monitoring of environmental impacts; and the effects of eventual pipeline decommissioning. More research was also needed on the impact on fishing, and the plan for the follow-up monitoring of the project's environmental impact was poorly laid out, the Finns concluded.[166] In a separate development, on 2 October 2009, a munitions clearance permit was granted by the Finnish authorities.[167]

The Swedish position by then remained unchanged. Formally Sweden stuck to a legalistic approach, had not yet taken an official position, and awaited additional environmental impact studies.[168] In January and February 2009, the Nord Stream consortium responded to the comments received with regard to the second application.[169] Between 9 March and 21 August 2009, another period of

---

166 Russian Petroleum Investor 18: 8 (September 2009), p. 26.

167 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 47 and 73. In November-December 2009 and April-June 2010, the munitions in Finnish waters were cleared by BACTEC International Ltd., which in March-April 2010 also cleared the munitions found in Swedish waters.

168 This was also the position usually adopted in discussions with representatives of other countries. According to one of the U.S. State Department cables exposed by Wikileaks, a Swedish diplomat reportedly said that "the Swedish government was not opposed to the project, as long as it passed strict Swedish environmental review. 'The environment is important to Swedes; there will [be] no special deals and no political intervention.'" Reference ID #07MOSCOW5585, dated 29.11.2007. <http://wikileaks.org>. According to another cable, a Swedish official reportedly said that "all public signs from Sweden's political leadership support Nordstream, for 'greater diversity leads to decreased dependency.' However, he added, 'remember that the bridge to Denmark took 8-10 years to approve' because of challenges and appeals based on environmental concerns. Approvals for the Nordstream pipeline to cross Sweden's EEZ would take at least as long," the official reportedly concluded "with a grin." Reference ID #08STOCKHOLM792, dated 28.11.2008. <http://wikileaks.org>.

169 Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6.

consultation took place during which all relevant agencies and authorities were requested to comment on the Nord Stream project, and Nord Stream AG took the opportunity to present its view to those who commented. On 5 June and again on 30 September 2009, Nord Stream AG supplied additional data on the alternative routes which had been suggested.[170] Still Sweden made no commitments. Furthermore, Sweden would assume EU presidency during the second half of 2009. This period would prove crucial for the project, and the trade press glumly argued that the Swedish presidency might cause difficulties for Russian projects.[171]

On 16 July 2009, as soon as Sweden had assumed the EU presidency, Russian President Dmitry Medvedev held a press conference with German Chancellor Angela Merkel during an official visit to Germany. Medvedev first thanked Finland for its positive decision on the EIA (although in fact no final decision had been made), then expressed his hope that this example would inspire the other states involved in the process. Medvedev noted:

> "With regard to the position of Sweden, we know what their position is and we have to treat it with respect. At the same time, we believe that there are additional explanations that can make a difference, and given the fact that Sweden currently holds the presidency of the EU, it has a great opportunity to contribute to the energy security of Europe."

Speaking in support of the Russian view, Merkel added,

> "I am one of those who don't spend a lot of time worrying about the controversy surrounding pipelines. [...] And if you look at the demand for gas in Europe over the next decade, there are many opportunities for trade between Russia and Europe, Russia and Germany."

There was thus little doubt that Germany still lobbied for the pipeline project.[172]

---

170 Letter from Matthias Warnig, Nord Stream, to the Ministry of Industry (Enterprise), Energy and Communications (Näringsdepartementet), dated 29.09.2009; Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6; Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009.

171 Russian Petroleum Investor 18: 8 (September 2009), p. 26f.

172 Ibid., p. 27.

On 2 October 2009, the French firm GDF SUEZ announced that its intention to acquire 9 per cent of the shares in Nord Stream AG would be negotiated shortly.[173] This meant that France too wished to see the pipeline built.[174] A number of West European countries by then supported the pipeline project, as can be seen by a brief survey of the annual contracts for gas delivery up to 2035 which had already been signed. Wingas (Germany) had contracted up to 9 bcm of natural gas, followed by E.ON Ruhrgas (Germany), with up to 4 bcm. Gazprom Marketing & Trading (Britain) had contracted up to 4 bcm. Britain had visibly supported the project during the early years (although interest later faded because of political changes in its relationship with Russia which went beyond the purpose of this study[175]). GDF SUEZ (France) contracted up to 2.5

---

[173] Russian Petroleum Investor 18: 10 (November/December 2009), p. 9. In June 2008, Gaz de France and Suez had merged and named itself GDF SUEZ.

[174] Russian Petroleum Investor 19: 3 (March 2010), p. 14. Indeed, a memorandum to this intent was eventually signed on 01.03.2010, during an official visit to France by President Dmitry Medvedev, with GDF SUEZ SA on 20.06.2010 acquiring 9 per cent of the equity from the German shares. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 23.

[175] The reason was chiefly connected to energy policy and state control. Gazprom had in 1999 established a subsidiary in Britain named Gazprom UK Trading, which in 2004 was replaced by Gazprom Marketing & Trading Ltd. Its purpose was to sell natural gas to the U.S. market, among others, but also eventually to gain a 10 per cent share of the British market. In 2006, Gazprom negotiated to purchase a 20 per cent share of Britain's largest energy utility firm, Centrica, a bid ultimately not found acceptable by the British authorities, likely upon political grounds. See, e.g., RIA-Novosti (Russia), 17.11.2004; BBC News, 02.02.2006, 03.02.2006. In summer 2006, Vitaly Vasiliev, head of Gazprom Marketing & Trading, still worked to receive 3-7 bcm through Interconnector and BBL to gain 10-15 per cent of the British market. Grib, Nataliya: Gazovyy imperator: Rossiya i novyy miroporyadok.. Moscow 2009, p. 121. However, other political tensions were building up as well, with Britain hosting a cluster of high-profile Russian exiles unanimously opposed to President Putin including the Chechen leader Akhmed Zakayev, wanted for charges of terrorism, the controversial Russian businessman Boris Berezovsky, wanted for charges of, among others, corruption, and former Russian agent Alexander Litvinenko, who died on 23.11.2006 in London and who in a posthumously public letter accused Putin of his death. In 2007, Zakayev and others repeated Litvinenko's accusations. The tensions grew, and in early 2008 the British Council offices in Yekaterinburg and St. Petersburg were ordered closed. See, e.g. Reuters, 18.01.2008.

bcm, while Dong Energy (Denmark) had contracted up to 1 bcm.[176] The Netherlands too had an interest in the project, as was clear from Gasunie joining the consortium in 2006.[177]

On 20 October 2009, Denmark granted a construction permit for Nord Stream through Danish waters.[178]

Finally, on 5 November 2009, Sweden and, a few hours later, Finland approved Nord Stream construction through their exclusive economic zones. Sweden added a number of conditions for its approval so as to ensure some degree of control over the pipeline project.[179] Sweden's approval came two weeks before an EU-Russia summit in Sweden's capital Stockholm scheduled to take place on 18 November.[180] Holding the EU chairmanship, there had apparently been no way for Sweden to postpone the decision further. Even so, the process had taken almost three years since notification and 23 months since Sweden received the original EIA application.

Yet the Swedish government stuck to its official legalistic line and noted that the environmental provisions had been satisfied. "No serious Swedish government would so blatantly break international law that it would say no to the pipeline," clarified the Minister of the Environment, Andreas Carlgren, in an interview.[181] On a personal level or in a semi-private capacity, comments were often less neutral. Indeed, the personal views of Swedish government members remained

---

176 Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG. Dong expected to sell on some 0.6 bcm of its share to Gazprom Marketing & Trading Ltd for sale in Britain. Western Europe Oil and Gas Insight 4 (Business Monitor International, August 2006), p. 8.

177 An historian cannot fail to note that Sweden had not faced such an alliance since the days of the Great Northern War (1700-1721).

178 Russian Petroleum Investor 18: 10 (November/December 2009), p. 9 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73.

179 Miljödepartementet: PM Tillståndsprövning av Nord Streams gasledning i Östersjön. Memorandum. 05.11.2009; Russian Petroleum Investor 18: 10 (November/December 2009), p. 9f.

180 Russian Petroleum Investor 18: 10 (November/December 2009), p. 10.

181 Dagens Nyheter (Sweden), 05.11.2009.

mostly identical regardless of political party affiliation.[182] With regard to Russian natural gas, the opinion of a majority of Swedish politicians could seemingly be summarized in the words of the Minister of Education, Jan Björklund, a few months prior to the decision: "There are only two problems with Russian gas. First, it is gas. Second, it is Russian."[183] The view of the Swedish government was that any increased use of hydrocarbons was detrimental to its ambition to reduce the global emission of greenhouse gases. No matter that other European countries needed the natural gas; this was a matter of faith for Swedish governments regardless of political colour, as Björklund's comments showed.

When the Swedish approval came, few bothered about the fact that Russia and Germany had not yet approved the project. The Russian and German approvals were by then rightly assumed to be a formality.[184] Russia granted the permit to construct the offshore section on 18 December 2009, and Germany followed on 21 and 28 December.[185] Finland had granted an exclusive economic zone usage license on 5 November 2009, in accordance with the Act on the Finnish Exclusive Economic Zone, but had not yet granted a construction permit. The latter would be provided by the Western Finland Environmental Permit Authority which decides whether to approve a construction permit under Finland's

---

182 Göran Persson, Prime Minister of the Social Democratic government until 06.10.2006, was a noted opponent of both Russian natural gas and the pipeline project, and this was well known in Russia. On 13.06.2006, he in Parliament noted that he had never hidden the fact that he did not wish to introduce Russian natural gas in the Swedish energy supply system (in Swedish: "Jag har heller aldrig dolt att jag inte vill introducera rysk gas i det svenska energisystemet"). EU-nämndens stenografiska uppteckningar 2005/06:42 13.06.2006. A month later, Prime Minister Persson in an interview with a leading Swedish financial news weekly said that Sweden was ready to stop the pipeline project. Veckans affärer (Sweden), 09.08.2006 (print issue dated 17.08.2006). On 18.08.2006, he in Visby described the pipeline project as an environmental threat since it could stir up munitions and chemical substances from the Second World War. Vedomosti (Russia), 21.08.2006.

183 Jan Björklund. Speech in Marstrand, 20.08.2009. In Swedish: "Det finns bara två fel på rysk gas. Det ena är det är gas. Det andra är att den är rysk."

184 Russian Petroleum Investor 18: 10 (November/December 2009), p. 9.

185 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 73 and 75.

Water Act. Finland provided its second and final approval on 12 February 2010.[186]

Nord Stream AG was finally cleared to begin construction. On 6 April 2010, the first seabed pipe was laid. Three days later, a ceremony to celebrate the event was held, attended by Russian President Dmitry Medvedev, Dutch Prime Minister Jan Peter Balkenende, ex-Chancellor of Germany and chairman of the Nord Stream board Gerhard Schröder, Gazprom CEO Alexei Miller, Nord Stream AG managing director Matthias Warnig, and the new Commissioner for Energy in the European Commission, Günther Oettinger.[187]

Nord Stream Lobbying

"Nord Stream was possibly the most unpopular infrastructure project in Europe," Nord Stream later admitted.[188] During the entire EIA process, Nord Stream AG therefore spent considerable efforts on lobbying and the recruitment of lobbyists. Already from the outset, when ex-Chancellor Schröder was appointed chairman of the consortium, the venture had been keen to recruit influential lobbyists. Yet more were to follow, on national as well as local levels in the countries in which the EIA process and pipeline construction would take place. In August 2008, for instance, Finland's former Prime Minister Paavo Lipponen was employed as a consultant for Nord Stream AG, with the task of assisting in the application to Finland.[189]

But most lobbying activities took place in Sweden. When the commercial Swedish television station TV 4 investigated the lobbying activities of Nord Stream AG in its investigative television show *Kalla fakta* ("Cold facts"), it noted that many of these activities took place on the local level of government, in towns and local academic institutions. For instance, the television

---

186 Ministry of the Environment (Finland): Notification in accordance with Article 3 of the Convention on Environmental Impact Assessment in a Transboundary Context (Espoo Convention) for the Nord Stream Gas Pipeline, reference YM5/5521/2006. 14.11.2006; Russian Petroleum Investor 19: 3 (March 2010), p. 14.

187 Russian Petroleum Investor 19: 5 (May 2010), p. 41.

188 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 75.

189 Helsingin Sanomat (Finland), 15.08.2008.

reporters alleged that a professor at Gotland University College who had criticized the pipeline project had changed his assessment after having been offered, and receiving, a research grant of SEK 5 million from Nord Stream AG in June 2007. The reporters also alleged that politicians on Gotland who had criticized the pipeline had ceased their criticisms when it was decided that Nord Stream AG would renovate the local port town of Slite.[190] In August 2007, months before the consortium even approached the Swedish government with its EIA, the Gotland port town of Slite had accepted that the Nord Stream consortium would use its facilities for logistics during the pipeline project construction, in exchange for the consortium providing approximately SEK 70 million to renovate the harbour.[191] A new quay was eventually constructed, since the old quay was too small, with work starting in December 2008, before the consultation period relating to the amended EIA was over.[192] In total, Gotland benefited from SEK 100 million which was spent on Slite port and various cultural research projects.[193] Slite henceforth became an important logistics site and storage depot for the Nord Stream project, together with the port town of Karlskrona—which in addition to becoming one of the Nord Stream project's two Swedish warehouse terminals also hosted one of Sweden's most important naval bases. But Sweden was not the only country in which local politics, the project's need for logistics, and lobbying activities took place. In Finland, the consortium employed the port of Hanko (which after the Second World War had been the site of a Soviet naval base) as a warehouse terminal and the port of Kotka as a pipe coating yard. In Germany, the port of Sassnitz/Mukran was used both as a warehouse terminal and for pipe coating.[194]

On the national level in Sweden, following Sweden's rejection of the first EIA application in spring 2008, Nord Stream AG, hired Dan Svanell, who had been

---

190 Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009.

191 Ibid. See also Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 129.

192 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 121.

193 Nord Stream: Bemötande av synpunkter m.m. från den publika remissrundan. Virum: Ramboll Oil & Gas, on behalf of Nord Stream, September 2009, p. 121.

194 Russian Petroleum Investor 18: 8 (September 2009), p. 23, citing Nord Stream AG.

press secretary to seven Social Democratic ministers, including Leif Pagrotsky who had met Gazprom CEO Miller for discussions on the pipeline project in 2003 and been one of those who initiated the public debate in 2006 (the Social Democratic party had since lost an election), and knew the Swedish government structure well.[195] Then Nord Stream hired Tora Leifland Holmström, a close advisor of Minister of Agriculture Eskil Erlandsson, as communications project manager.[196] Finally, Nord Stream hired former State Secretary Ulrica Schenström, who had been described as the right hand of Prime Minister Fredrik Reinfeldt and reportedly had enjoyed access to classified information about Swedish strategies with regard to the Nord Stream project.[197] With these recruitments, Nord Stream AG successfully hired key people from both the government and the leading opposition party who were well versed in how the Swedish government functioned and, at least in some cases, no doubt had insider knowledge of the government's views on the Nord Stream project.

In addition, Nord Stream AG spent considerable efforts and funds on public hearings in Stockholm and other Swedish cities and the distribution of information on the pipeline project. Between 2006 and 2008 the Nord Stream consortium claimed to have arranged or participated in more than a hundred public meetings and conferences in the countries around the Baltic Sea.[198] As lobbying intensified, this number rose to more than two hundred by late 2009.[199] Of these, a large share took place in Sweden. Nord Stream AG even sponsored a number of academic research projects, including marine archaeology research carried out off Gotland in 2007 and a book in Swedish on sixteenth-century naval warfare written by a Russian journalist.[200] The book described the Northern Seven Years' War (1563-1570), which was chiefly fought between Sweden and Denmark. It was presumably a coincidence that the book described a war

---

195 Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009.

196 Ibid.; Morén, Kristoffer. In Baltic Worlds 4, 2010, p. 15.

197 Resumé, 09.07.2008; Swedish television station TV4 investigative news program Kalla fakta, 15.02.2009; Nyhetskanalen (Sweden), 15.02.2009; Dagens Nyheter (Sweden), 15.02.2009.

198 Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 5.

199 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 71.

200 Smirnov, Alexej: Det första stora kriget. Stockholm 2009.

between Sweden, the government of which was against the Nord Stream project, and Denmark, which was in favour of it.

Nord Stream AG also employed the renowned British public relations agency Hill and Knowlton to polish the image of the project. Hill and Knowlton described the firm's participation in the following terms: "H+K Strategies' corporate communications and public affairs activities have helped enable Nord Stream maintain open dialogue with regulatory decision-makers and enhance information flow at an international level."[201] In other words, Hill and Knowlton assisted Nord Stream AG with the EIA application process (while Ramsbøll produced the actual EIA). The Hill and Knowlton agency was quite successful, and indeed won several awards in 2009 for its public relations activities on behalf of Nord Stream AG.[202]

5.1.3 Outcome

The first line of the pipeline was eventually constructed according to plan, as adjusted for the delays in the EIA process, with work beginning in 2010 and coming on line on 8 November 2011, at a ceremony attended by French Prime Minister François Fillon, German Chancellor Angela Merkel (who six years earlier had declined to attend the welding of the first joint of the pipeline), Dutch Prime Minister Mark Rutte, Russian President Dmitry Medvedev, EU Energy Commissioner Günther Oettinger, and Erwin Sellering, Minister President of Mecklenburg-Western Pomerania. The second line came on line on 8 October 2012, with less pageantry and official representation.[203] Transport capacity would be 55 bcm per year.[204] Yet, no offshore platform was ever built, nor were any military sensors installed, as far as is known.

---

201 Hill and Knowlton web site, <www.hillandknowlton.co.uk>. The web site mentions the firm's successful work for Nord Stream but does not offer access to details with regard to the project.

202 AMEC Communication Effectiveness Awards. Web site, <http://amecorg.com/wp-content/uploads/2011/08/amec_awards_2010_winners.pdf>.

203 Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 76, 133, 141 and 240. By late May 2012, Nord Stream announced plans for a third and fourth line. Ibid., p. 75.

204 Ibid., p. 284.

There is the distinct possibility that the Swedes were right in suspecting the Russian Navy or intelligence services of plans to use the offshore platform for military intelligence collection. As noted, the offshore platform was the only part of the project which Sweden actually could veto, according to the United Nations Convention on the Law of the Sea. Yet on 13 February 2007, before Sweden had even responded to the submitted notification of intent, the Russian Ambassador to Sweden, Alexander Kadakin stated, in a controversial interview on national public radio, that "it is even imaginable that the platform will not be built. It is technically possible to have a pipeline without such a platform, as a worst-case scenario."[205] This was not, at the time, the official position of the Nord Stream consortium, which had made elaborate plans for the offshore platform and claimed that it was really necessary for the viability of the entire project.[206] As late as on 14 September 2007, Nord Stream explained in Stockholm that the platform was an integral part of the pipeline system.[207] Even so, the possibility of building the pipeline without an offshore platform had already been raised by an anonymous source reportedly "close to" the pipeline project in an interview with the Russian newspaper *Vremya Novostey* in August 2006.[208] And in early 2008, Nord Stream AG confirmed that it could build the pipeline without the offshore platform.[209] In other words, Ambassador Kadakin

---

[205] Sveriges Radio (Sweden), 13.02.2007. In the same interview, Kadakin concluded that he could not understand "what kind of an idiot" had been able to argue to his superiors that the offshore platform could be used for intelligence collection aimed at Sweden (in Swedish: "Jag fattar inte vad det är för en slags idiot som har kunnat hävda detta i sina rapporter till sina svenska överordnade.") However, even as the Ambassador referred to the project's individual detractors as idiots, he stressed that relations with the Swedish government remained friendly and concluded that there had been no official Swedish criticism aimed at the Nord Stream project, thus maintaining the illusion of smooth and disinterested government-to-government relations.

[206] Dirk von Ameln, Deputy Technical Director, Nord Stream AG: Hearing in Swedish Parliament. Stockholm 12.12.2006, Hearing in Visby 22.01.2007. Noted in Carl B. Hamilton: Naturgasledning på Östersjöns botten: Lägesrapport 23 februari 2007 (Folkpartiet, 23 February 2007), p. 19f.

[207] Nord Stream, The Service Platform: An Intergral *(sic)* Part of a Safe System. Nord Stream Forum. Stockholm, 14.09.2007.

[208] Vremya Novostey 149, 21.08.2006.

[209] Nord Stream, Response to Questions Asked, and Inaccurate Statements Made, during the Public Hearing of the Committee on Petitions, "The Nord Stream Pipeline and Its Impact on the Baltic Sea," European Parliament, Brussels, 29.01.2008, p. 11. Nord

and *Vremya Novostey*'s anonymous source seemed to have access to more information, and at an earlier stage, than the authorized representatives of Nord Stream AG. This indeed fuels suspicions that the offshore platform's primary purpose indeed may have been intelligence collection, but that Russia scrapped these plans when confronted with the Swedish resolve to stop the entire project, if possible, by refusing permission to build the platform. Because for Russia, the export pipeline was the greater good, due to the need to bring in revenues from the export of natural gas to Western Europe. Intelligence collection would no doubt have been an added benefit but was not the primary driver behind the project. The other possible explanation is that the platform all along was regarded as a negotiable concession, which would be a benefit if permitted but was not really necessary for the project.

Further support for the suspicion that there had indeed been Russian plans to use the offshore platform, and likely the entire pipeline, for military intelligence collection came in 2008, after the Nord Stream consortium had already confirmed that no offshore platform would be built. A Russian paper was then published in a scientific journal about the sensor systems to be used to protect the Nord Stream pipeline from terrorism. The article was written jointly by two lieutenant colonels and two scientists and concluded that the pipeline might be under threat not only from terrorists but also from saboteurs from companies and countries opposed to its construction. In response to this threat, the pipeline would be protected by a composite sensor system consisting of surface and underwater components, including sensors mounted on the pipeline itself. Based on the information received from the sensor systems, suitable measures, including the firing of missiles against hostile surface vessels or aircraft, could be initiated in real time to destroy the threat, the authors argued. The paper quaintly referred to the pipeline under its old name NEGP and the accompanying map still included the offshore platform, although the text mainly referred to non-stationary surveillance means such as satellites, unmanned aerial vehicles (UAV), and autonomous underwater vehicles (AUV). It thus gave the distinct impression of being an old paper dusted off and updated for publication despite, to some extent, being out of date. But the affiliation of the writers left little room for

---

Stream AG produced the document immediately following the 29 January 2008 hearing.

doubt. The two scientists were affiliated with the State Research Navigation-Hydrographic Institute (GNINGI), a state institute under the Russian Ministry of Defence, whereas the two military officers were listed as serving officers of military unit number 54023, which elsewhere has been identified as a formation within the Russian military intelligence service Main Intelligence Directorate (GRU) believed to be involved in satellite imagery intelligence collection. The authors ended the paper by suggesting that the several countries with an interest in the pipeline could work together to protect it, by integrating some of their respective surveillance systems.[210]

As far as is known, no military sensors were installed in conjunction with the pipeline. Simply by advertising its concern widely and vociferously, Sweden ensured that it would be difficult for the Russian side to use the pipeline for military intelligence purposes. The Policy Memorandum exposed by Swedish national television made it abundantly clear that even if the Swedish government eventually accepted the EIA and gave the necessary permits to build the pipeline, then this permit would only cover the commercial activities of the consortium, never any intelligence use of the infrastructure by state actors.[211] The condition that would adhere to the eventual permit was duly noted by the Nord Stream consortium, and when Nord Stream AG arranged a public hearing in Stockholm on 29 November 2006, about four months after the document was written (but about a week before it was leaked to the press, posing questions on

---

[210] Katenin, V. A./ Surzhikov, I. M. and Makarov, A. M: Vozmozhnyy oblik sistemy osveshcheniya nadvodnoy i podvodnoy obstanovki v interesakh obespecheniya deystviy antiterroristicheskikh sil i sredstv zashchity podvodnykh truboprovodnykh sistem (Possible Look of a Surveillance and Warning System Aimed for Provision [of] Effective Actions of Anti-terror Forces and Security Protection of Underwater Pipeline Systems). In: Morskaya radioelektronika 24, No. 2, June 2008, p. 12ff. On GNINGI, see its web site, <http://gningi.ru/>. For the identification of military unit number 54023 as the 162nd Military-Technical Center, based on Volokolamskoye Shosse 56/2 in Moscow, a formation within the GRU which engaged in satellite reconnaissance, see commonly available web sites, e.g. <http://wikimapia.org>; <http://agenturaforum.com>; <www.evasiljeva.ru/2014/04/blog-post_30.html>. This identification is supported by official tenders for satellite equipment, as published in the Russian government web site, <www.zakupki.gov.ru>.

[211] Policy Memorandum from the Ministry of the Environment, then usually translated into English as the Ministry of Sustainable Development (Miljö- och samhällsbyggnadsdepartementet), 08.08.2006.

whether the Russian side had already learnt of the Swedish assessment), its materials included an addendum which acknowledged that the permit would only apply to natural gas deliveries, and that any "incorrect usage" might result in a halt in the pipeline's operation.[212] The addendum was duly noted by the Swedish side.[213] It is for this reason that Russia, faced with Swedish opposition and known determination to treat any installation of military sensors as grounds for refusing the project, would be unlikely to take the risk of installing any such sensors later. If military sensors were eventually discovered in conjunction with the pipeline, Sweden could retroactively recall its permit. One could of course argue that if the Russians really wanted to install military sensors, they might be able to install the appropriate sensors anyway, by clandestine means after the pipeline was put in operation. However, since the primary purpose of the project was always to guarantee the export of natural gas, the risk of installing such sensors for the secondary purpose of military intelligence collection would no doubt be assessed as too great. Besides, in a real crisis, such sensors would be of little use – since the pipeline had a known, fixed location and despite the assurances of the two GRU officers would be easy to breach, if this was ever deemed necessary, thus at the same time destroying the integrity of the sensor chain. Needless to say, this would also halt any natural gas exports, which would affect Russia more than its Western customers who were not fully dependent on Russian supplies.

The Russian side thus attained its primary objective of building natural gas export infrastructure which bypassed the transit countries. However, when the necessary permits to build the Nord Stream pipeline were finally granted, in November 2009, the world was suffering from a global financial crisis.

The 2003 energy strategy had been afflicted with several problems. In addition to alarming consumer and transit countries, it also consisted of detailed objectives that, in some cases, soon no longer corresponded to market realities. In late 2006, Russia accordingly commenced work on an updated energy strategy.[214] The new Russian energy strategy was approved in late 2009, eight days after

---

212 Nord Stream: Säker gasförsörjning för Europa. Presentation, 29-30.11.2006.

213 Larsson, Robert: Nord Stream presentation . FOI Memo 1905, 30.11.2006.

214 Ministry of Industry and Energy: On a refinement of the Energy Strategy of Russia for the period up to 2020 and its prolongation up to 2030. Decree of the Ministry of Industry and Energy No. 413, 21.12.2006.

Sweden's approval of the Nord Stream project.[215] The new strategy was in many ways a response to the then ongoing financial crisis. Gone were the phrases that suggested military strategy. Instead the new strategy repeatedly emphasized the need to create a favourable economic environment.[216] Of the statements in the 2003 strategy that the energy factor would be a fundamental element within Russian diplomacy, nothing remained but the hardly unusual, in international commerce, conclusion that the strategic objective of the foreign energy policy was the Russian energy sector's full-scale integration into the world energy market, the enhancement of its positions thereon, and gaining the highest possible profit for the national economy.[217] The leading Russian energy companies would receive diplomatic support abroad.[218] Russia had national interests in the operation of the global energy market, but in the roadmap of state policy measures attached to the strategy there were no alarming statements beyond that of promoting Russian energy companies abroad and offering them "information, political, and economic support."[219] In fact, the energy strategy candidly admitted problems in Russia's foreign energy policy, including the financial crisis but also the continuing export dependence on transit countries and the politicization in the energy relationships between Russia and foreign countries.[220] And politicization was indeed what had characterized the struggle to build the Nord Stream pipeline.

5.1.4 Concluding Remarks

The Nord Stream pipeline was successfully completed as a commercial project, but Sweden made certain that no offshore platform was built and worked to ensure that no military sensors were installed. The Swedish opposition and

---

215 Government of the Russian Federation: Energeticheskaya strategiya Rossii na period do 2030 goda ("Energy Strategy of Russia to the Year 2030"), Government of the Russian Federation Decree No. 1715-r, 13.11.2009.

216 See, e.g. Government of the Russian Federation: Energeticheskaya strategiya Rossii na period do 2030 goda ("Energy Strategy of Russia to the Year 2030"), Government of the Russian Federation Decree No. 1715-r, 13.11.2009, p. 16, 18 and 19.

217 Ibid., p. 34.

218 Ibid., p. 35, app. 5, p. 23f.

219 Ibid., p. 89, app. 5, p. 18ff.

220 Ibid., p. 35.

strong resolution with regard to the minutiae of the EIA may also have pushed the consortium into taking the environmental aspects very seriously, something for which Nord Stream AG eventually received considerable and deserved recognition. In effect, both sides achieved some of their goals. Russia succeeded in building a natural gas export pipeline with direct access to Germany, thus bypassing those transit states with which Russia had frequently encountered political problems. Sweden, as far as is known, prevented Russia from laying an underwater sensor chain across the Baltic Sea and obstructed the project by legalistic means to the extent that Russia would find it difficult to justify an increased naval presence in the Swedish exclusive economic zone based on the existence of the pipeline alone (although there was, as before, nothing to prevent a naval presence as such). Sweden did not succeed in its lofty but futile attempt to save the EU from importing more Russian natural gas, nor save the Baltic Sea from the environmental impact of the pipeline, if there was one (an issue to which everybody had paid lip service but which was quickly forgotten by the media and the public after construction began).

The Nord Stream consortium claimed that Sweden's obstruction cost more than EUR 100 million in expenses related to the EIA process and associated lobbying activities, not counting almost two years of added time spent on the EIA process.[221] These costs would initially have to be borne by the corporations which owned Nord Stream AG but in the end were likely to be recouped from the European consumers. Sweden devoted considerable resources to monitoring and delaying the pipeline project, but these costs were taken from the regular operational funds of the government ministries and agencies involved, which ultimately came from the Swedish taxpayers. In return, the taxpayers and European consumers could enjoy the media show of the Nord Stream controversy, which ran for several years and provided entertainment to all and lucrative careers to some.

There was certainly a Swedish *long-term strategy*, on political and environmental grounds, to oppose further imports of Russian natural gas. When

---

[221] Nord Stream: Sammanfattning av projektet. Stockholm 30.09.2009, p. 6. In fact, this was the total cost of the environmental studies, route surveys, and technical planning and many of these would in any case have been necessary for the project. Nord Stream: Nord Stream. Secure Energy for Europe: The Nord Stream Pipeline Project 2005-2012. Zug 2013, p. 43, 58 and 72.

faced with the perceived threat of the pipeline as a sensor platform for Russian military intelligence, the long-term strategy hardened into an *intention* to oppose the pipeline project. Did this also lead to a Swedish *master plan* on how to thwart the project? If so, it was the one formulated by the inter-ministerial working group set up in 2006. The actual details – the *operations plan* – were then worked out in the winter of 2006/2007, coordinated by the Ministry of Defence. However, because of the decentralized administrative system there was probably never any formal operations plan, only a general agreement on what could be done to oppose the pipeline project by the respective actors which then *executed* the informal plan independently.

The Russian *long-term strategy* was the one formulated by President Putin over a series of years, and this resulted in an *intention* to bypass the transit countries so as to avoid further political difficulties with Russia's energy exports. This led to the *master plan* which can be said to the one presented in the 2003 energy strategy, in conjunction with the presumably secret plans of the Navy and GRU to use the pipeline as a sensor platform. The Russian side seems not to have anticipated the Swedish counterstrategy against the pipeline plan. The Russian side only developed a counter-counterstrategy, an *operations plan*, in early 2007, having then realized the scale of Swedish opposition. The *execution* phase of the operations plan began with full force only from 2008, after the Swedish government had rejected the original EIA.

The conclusions presented here would likely be disputed by both the Swedish and Russian governments. The Swedish government never officially voiced its concerns over the military intelligence collection opportunities for Russia perceived to exist in the pipeline project, nor did the Russian government ever mention an intention to use the pipeline in this way. Instead the struggle was relegated to low-level civil servants, military officers, retired officials, newspaper editors, lobbyists, and businessmen, whose activities, if necessary, could be disregarded as not representative of the formal stance of their respective governments. As in the work of the intelligence services, deniability was the key. Neither government was prepared to shatter the illusion that official relations remained smooth and without mutual suspicions with regard to intentions. Minister of the Environment Carlgren approved the project by referring to international law and concluded that the environmental provisions had been satisfied. The outspoken

Ambassador Kadakin referred to the project's opponents as idiots but stressed that relations with the Swedish government remained friendly and concluded that there had been no official Swedish criticism aimed at the Nord Stream project. Such comments were unsurprising. Nor would the two governments acknowledge that their respective intelligence services might be in the process of collecting information on each other. For a state, a hybrid power projection must in its essentials remain covert. There may be overt aspects, such as through the use of diplomatic power and commercial entities, but its targeted, multi-dimensional, and coordinated features may not be acknowledged, or the hybrid power projection becomes an open act of aggression, which might escalate existing rivalry into open confrontation.

5.2 The Hybrid Threat Capability of the Afghan Taliban Movement, 2001-2014

Michael Fredholm

When the Afghan Taliban leaders withdrew into Pakistan in late 2001, they had no intention of surrendering the struggle against the U.S.-led international coalition which had forced them out of Afghanistan. Yet, with a substantial international military presence firmly entrenched in Afghanistan, there was no way that the Taliban could regain power by conventional military means. Even with Pakistani military support, the Afghan Taliban movement could not have repeated the 1994 invasion of Afghanistan in the face of such military opposition.

For this reason, soon after its forced withdrawal into Pakistan, the Afghan Taliban began to employ the means and methods of hybrid warfare and hybrid threats, in this work defined as *"a threat to a state or an alliance that emanates from the capability and intention of an actor to use its potential in a focused manner, that is coordinated in time as well as multi-dimensional (political, economic, military, social, media, etc.) in order to enforce its interests."*[1] This was a result of strategy debates within the Taliban top leadership, likely with the support of political agents and military advisors from the Pakistani Inter-services Intelligence agency (ISI). Pakistan had long considered influence in Afghanistan a vital component of national security policy and was reluctant to surrender its influence. The policy is generally regarded as having originated from two perceived strategic needs: (1) to allow Pakistan the use of Afghanistan's territory for strategic depth in a conventional war against India; and (2) to ensure friendly Pashtun hegemony in Afghanistan so that ethnic Pashtuns on either side of the Pakistan-Afghanistan border would drop any plans to unite in a single Pashtun nation, and thereby compromise Pakistani

---

1 As defined by the National Defence Academy (Landesverteidungsakademie), Vienna: "Eine hybride Bedrohung ist die Gefährdung eines Staates oder Staatenbündnisses durch das Vermögen und die Absicht eines Akteurs, sein Potential zielgerichtet, mehrdimensional (politisch, wirtschaftlich, militärisch, gesellschaftlich, medial etc.) und in einem zeitlich abgestimmten Zusammenhang zur Durchsetzung seiner Interessen einzusetzen."

territorial integrity.[2] Pakistani specialists were certainly dispatched into Afghanistan when the Taliban movement aimed to establish a new front, or when combat conditions were particularly difficult. It is likely but not conclusively proven that Pakistan modelled its support to the Taliban on that provided to favoured Afghan insurgent leaders within the mujahidin front in the 1979-1989 Soviet war in Afghanistan.[3] Even so, there is little doubt that it was the Afghan Taliban leaders, not their Pakistani advisors, who formulated policy, including hybrid warfare and hybrid threats.

The hybrid threat capability developed by the Afghan Taliban (here defined as the Afghan Taliban movement with affiliates, excluding allied but independent international terrorist groups such as Al-Qaida and foreign terrorist groups such as the Pakistani Taliban) included various tactics and strategies to be employed at home and abroad. From 2002 onwards, the Afghan Taliban movement developed a considerable capability for hybrid threat projection. Being at war, in Afghanistan the Taliban movement, unsurprisingly, engaged in hybrid warfare. Abroad, the movement utilized its capacity for hybrid threats. For this reason, the domestic threat in Afghanistan deriving from the Taliban and the international threat of the movement were quite different in character.

While the Afghan Taliban movement had no expressed policy on the concept of hybrid warfare or hybrid threats as such, the movement was obviously aware of the means and potential of the concept. So were, for instance, the entire first two sections of the Taliban *Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan* primarily focused on the effect that the means of intimidation would have to compel the population into joining the Taliban, and how ordinary people and collaborators should then be treated.[4] In addition, the *Code of Conduct* emphasized that all who worked

---

2 See, e.g. Fredholm, Michael: Afghanistan and Central Asian Security. Asian Cultures and Modernity Research Report 1, Stockholm University March 2002, p. 16.

3 Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 242ff, on p. 246, 256 and 259.

4 Sections 1 and 2, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010 (Taliban Voice of Jihad Online in Pashto, 09.08.2010). The second edition included 14 sections and 85 articles. The first edition, which used very similar language, was published in the first half of 2009 and included

for the Taliban Islamic Emirate must strive to force those who supported the infidels to acknowledge and surrender to the Taliban.[5] It was clear from the *Code* that this encompassed threats and propaganda as well as fighting. The *Code* stressed the need to win the hearts and minds of the population. Article 78 translates as "The mujahidin are duty-bound to show good character and Islamic behaviour to the nation. They should win the hearts of Muslims at large."[6] The Taliban *Code* mirrored the counterinsurgency strategies adopted by Western countries in these respects, in their emphasis on winning the hearts and minds of the contested population.[7] In this regard, there was no great difference between Western and Taliban views on warfare. Nor was there such a difference in the view on new tactics and technologies. The Taliban movement, in similarity to other military organizations, displayed a learning curve, in which new methods, tactics, and technologies were adopted to stay abreast of developments.[8]

In fact, the hybrid threat capability of the Afghan Taliban movement soon grew to encompass several distinct types of powers, in both domestic and international dimensions. Many of these powers were exercised from Afghanistan, but particularly those with an international dimension more often geographically originated in Pakistan, where the Taliban leadership enjoyed safe havens. The full hybrid warfare and hybrid threat capability of the Taliban is summarized in Table 8.

---

13 sections and 67 articles. The first edition in turn replaced the *Book of Rules for the Mujahidin*, first published in the holy month of Ramadan 2006.

5 Article 77, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010.

6 Article 78, Code of Conduct for the Mujahidin of the Islamic Emirate of Afghanistan, 2nd edn of 29 May 2010. This article was also in the 2009 edition. However, it was not in the original 2006 Book of Rules.

7 See, e.g. the emphasis on statements such as "The decisive terrain is the human terrain" and "The people are the center of gravity". In: Petraeus, David H.: Counterinsurgency Guidance. 01.08.2010, COMISAF/CDR USFOR-A.

8 Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 242ff, passim. The learning curve was also evident in the aforementioned updated and improved editions of the *Book of Rules* and *Code of Conduct*.

Domestic Threat						
Type of Threat	**Target**	**Means and Method**	**Purpose**	**Geographic Origin**	**Effect**	**Defensive Actors**
Military Power	ISAF/ ANSF	Guerrilla attacks, IEDs	Defeat or intimidate enemy	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Terror Power	ISAF/ ANSF	E.g. suicide bombers	Intimidate enemy	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Terror Power	Population	E.g. killings, mutilations	Intimidate population	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Media Power	Population	E.g. night letters, proclamations, videos	Propaganda	Afghanistan/ Pakistan	High	Armed forces, police, intelligence
Organized Crime Power	ISAF/ ANSF	Support to bandit gangs	Cause disruption	Afghanistan/ Pakistan	Medium	Armed forces, police, intelligence

International Threat						
Type of Threat	**Target**	**Means and Method**	**Purpose**	**Geo-graphic Origin**	**Effect**	**Defensive Actors**
Diplo-matic Power	ISAF member states	Negotia-tions	Negotiate withdrawal	Pakistan	Me-dium	Foreign Ministry, Interna-tional organiza-tions
Diplo-matic Power	Worldwide Muslim commu-nity	Negotia-tions	Appear as responsi-ble party	Pakistan	Me-dium	Foreign Ministry, Interna-tional organiza-tions
Media Power	ISAF member states, worldwide Muslim commu-nity	*Afghanistan In Fight*, Internet, Twitter	Propa-ganda	Pakistan	Low/ me-dium	Media houses, government institutions, think tanks, NGOs
Terror Power	ISAF soldiers' family members	Threats by telephone or SMS	Intimidate individual to resign	Afghani-stan, ISAF member state	Low/ me-dium	Security service, Intelligence service, police
Terror Power	Attacks	Not used	Intimidate enemy to withdraw	Pakistan	None	Security service, Intelligence service, police

Table 8: Afghan Taliban Movement Hybrid Threat
Michael Fredholm

5.2.1 Background

The Taliban Movement in the 1990s

To assess the Afghan Taliban movement's capability for hybrid warfare and hybrid threats, it helps to first explain the origins of the movement. The Afghan Taliban movement emerged as a military force in 1994, when it was created, in all essentials, by and for Pakistani interests even though few, if any, Taliban leaders subsequently were much concerned about following Pakistani orders.[9] The movement's leaders at the time regarded themselves as the world's perhaps only true Islamic government, on the lines of the righteous caliphate of the early years of Islam.[10] The Taliban government accordingly styled itself the Islamic Emirate of Afghanistan.[11]

The Taliban were reinforced by large numbers of Pakistanis, religious volunteers as well as regular Pakistani military units. Indeed, the very first Taliban incursion into Afghanistan in 1994 was reportedly supported by Pakistani army artillery fire and motor transportation from the Pakistani side of the border.[12] The volunteers, who were first reported by the Pakistani press in mid-June 1997,[13] were initially mostly Pashtuns of Afghan or Pakistani origin but from 1999, Pakistani Punjabis arrived in increasing numbers and eventually formed the majority of the Pakistani volunteers.[14]

---

9 Rashid, Ahmed: Taliban. Islam, Oil and the New Great Game in Central Asia. London 2000, p. 26ff and 125; Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 71 and 82.

10 Gohari, M. J.: The Taliban. Ascent to Power. Oxford 1999, p. 118.

11 Taliban web sites: <www.taleban.com>; <www.afghan-ie.com> (both now defunct).

12 Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 45f and 49f.

13 Ibid., 12 and 25.

14 Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan. 30.08.2000; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 22ff, in particular on 100; Davis, Anthony: Struggle for Recognition. In: Jane's Defence Weekly, 04.10.2000, p. 21; Davis, Anthony: Foreign Fighters Step Up Activity in Afghan Civil War. In: Jane's Intelligence Review 13: 8 (August 2001), p. 14ff.

The Pakistani military played a considerable role in the military success of the Taliban. Senior Pakistani intelligence and army officers were involved in strategic planning. Regular Pakistani soldiers served as units in combat roles, or were detached from their units for the provision of special skills such as those of tank drivers and aircraft pilots, in technical and rear support, maintenance, and administrative functions. Pakistani aircraft assisted with troop rotations for Taliban forces during combat operations in late 2000. Pakistani military officers from the ISI as well as commandos from Pakistan's Special Services Group (SSG, a special forces regiment based near Peshawar) also appeared to take considerable responsibility for the planning and execution of major operations. This was shown by the impressive use of mobility, speed, logistics support, as well as efficient contemporary command, control, communications, and intelligence procedures displayed by the Taliban, on a level hitherto never seen among Afghan troops and certainly not to be expected from such a comparatively new military formation, even considering the fact that the Taliban also recruited numerous officers and men of the pre-1992 Afghan army, many from the hardline, Pashtun nationalist Khalq ("Masses" or "People") wing of the Communist Party.[15] Pakistan-based Western diplomats knew that the ISI was instrumental in forming and supporting the Afghan Taliban movement.[16] However, following the 11 September 2001 terrorist attacks, this was seldom mentioned so as not to embarrass Pakistan and cause further tensions in an already dangerous domestic political environment.

---

15 Davis, Anthony: How the Taliban Became a Military Force. In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, in particular on 68ff; Saikal, Amin: The Rabbani Government. 1992-1996; In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 29ff, on 39; Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000; Davis, Anthony: Struggle for Recognition. In: Jane's Defence Weekly, 04.10.2000, p. 21; Davis, Anthony: Foreign Fighters Step Up Activity in Afghan Civil War. In: Jane's Intelligence Review 13: 8 (August 2001), p. 14ff; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 49; Rashid, Ahmed: Jihad: The Rise of Militant Islam in Central Asia. New Haven 2002, p. 174; Human Rights Watch (HRW): Fueling Afghanistan's War. HRW Press Backgrounder, 2001.

16 Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 45f, 49 and 91.

Weapons being abundant in Afghanistan, the Taliban did not really have a supply problem with regard to personal weapons. Fuel, heavy weapons, and ammunition were another matter. The Taliban depended on Pakistan for delivery of ammunition, particularly for tanks and artillery, some small arms, pick-up trucks, and petroleum (both motor and aviation fuel), oil, and lubricants. They also received financial payments. A significant share of the Taliban procurement of arms, munitions, and spare parts was handled by Pakistani private companies, often run by retired military officers. They bought considerable quantities from Chinese manufacturers through dealers in Hong Kong and Dubai (United Arab Emirates). The supplies were usually shipped in sealed containers to the Pakistani port of Karachi, whence they were trucked to Afghanistan without normal customs inspection, since this was not required by the two countries' trade agreement, the Afghan Transit Trade Agreement (ATTA).[17] Some were probably paid for through financial assistance to the Taliban from private or state supporters in the Arabian Peninsula through the use of Islamic charities such as the Al-Rashid Trust, which has since been accused of smuggling weapons and supplies, disguised as humanitarian aid, to the Taliban.[18] The Taliban were funded partly from contributions from supporters abroad, typically on the Arabian Peninsula, partly from taxes, in particular deriving from narcotics production in Afghanistan.[19] It was not unknown for Taliban leaders to maintain foreign bank

---

17 Support from Pakistan: Human Rights Watch (HRW): Fueling Afghanistan's War. HRW Press Backgrounder, 2001; Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 28.05.1999; 30.08.2000; 17.10.2000; Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 44f, 72 and 183f; Rashid, Ahmed: Heart of Darkness. In: Far Eastern Economic Review, 05.08.1999, p.8ff; Magnus, Ralph H./Naby, Eden: Afghanistan: Mullah, Marx, and Mujahid. Boulder, Colorado 1998, p. 190; Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 69.

18 The New York Times (USA), 25.09.2001.

19 Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 35, 120 and 123f; Rashid, Ahmed: Heart of Darkness. In: Far Eastern Economic Review, 05.08.1999, p. 8ff. The Taliban in mid-2000 banned the cultivation of opium poppy. Some Western drug law enforcement officials claimed that this was merely a public-relations exercise, and that drugs were instead stockpiled in order to push up the price. Because of the 2001 downfall of the Taliban, we may never know their ultimate intentions. The Taliban certainly made substantial profits from the narcotics trade *before* they outlawed it. See, for instance, Far Eastern Economic Review (Hongkong), 28.12.2001. They also reportedly sold large quantities of the stockpiled drugs after the 11.09.2001 terrorist attacks on the United States in order to finance the

accounts. For instance, Taliban supreme leader Mullah Muhammad Omar had accounts in the Laskari Bank in Islamabad and the National Westminster Bank in Britain. Both were allegedly opened for him by the ISI.[20] Many Pakistanis too profited from business connections with the Taliban. Taliban leaders soon developed relations with a number of Pakistani businessmen close to Asif Ali Zardari, the husband of Benazir Bhutto, Pakistan's prime minister 1993-1996, who in turn were given highly lucrative permits for fuel deliveries from Pakistan to the Taliban. Pakistan also assisted in the development of necessary infrastructure in Taliban-controlled Afghanistan. Pakistan Telecom, for example, set up a microwave telephone network in Kandahar. This became part of the Pakistani telephone grid. Kandahar received the same prefix (081) as that for Quetta, so Kandahar could be called from Pakistan as a local call.[21]

In the early years of the movement, the Taliban received considerable material and financial support also from Saudi Arabia. By then, every major Taliban offensive seemed to be preceded by a visit from Prince Turki ibn Faisal al-Saud, head of the Saudi General Intelligence Agency (*al-Istakhbarah al-Amah;* or simply *Istakhbarat*), and his staff. Earlier, Prince Turki also played a major role in organizing the mujahidin front against the Soviets during the 1979-1989 war.[22]

---

expected war. Jacquard, Roland: Les archives secrètes d'Al-Qaida. Révélations sur les héritiers de Ben Laden. Paris 2002, p. 62 n.4. According to Vladimir Fenopetov, Chief, Europe and West/Central Asia, UN Office on Drugs and Crime, the Taliban ban of opium production, which came into force in 2001, was merely a ruse to (1) make full use of an existing overproduction, and (2) increase the price of opium. Trafficking out of Afghanistan, according to United Nations statistics, in fact remained constant. Vladimir Fenopetov, "Eurasia's Narcotics Situation", conference on 'New' Security Threats in Eurasia: Implications for the Euro-Atlantic Space. Central Asia-Caucasus Institute/Silk Road Studies Program, Stockholm, 20.05.2005.

20 Jacquard, Roland: Les archives secrètes d'Al-Qaida. Révélations sur les héritiers de Ben Laden. Paris 2002, p. 24.

21 Rashid, Ahmed: Pakistan and the Taliban. In: Maley, William (ed.): Fundamentalism Reborn? Afghanistan and the Taliban. New York 1998, p. 72ff, on 84f.

22 On 19.09.1998, the uncompromising Taliban leader Mullah Omar insulted Prince Turki and the Saudi royal family. Saudi Arabia then ceased its support for the Taliban, although the diplomatic recognition pushed through by Pakistan in May 1997 was not withdrawn. Perhaps significantly, from October 1998 the Taliban, who previously had generally been able to seize the initiative in any military offensive, began to lose ground

The Taliban military chain of command was vague and ill-defined at the time. The top decision-making body was the Rahbari Shura (Leadership Council, often referred to as the Supreme Shura) in Kandahar, headed by Mullah Omar. There were also other, lower shuras that reported to the Kandahar Leadership Council, such as the Kabul Shura and the Military Shura or Military Commission. The Kabul Shura was fundamentally a cabinet of acting ministers in Kabul. They primarily dealt with day-to-day problems and local military and political activities, since all important decisions were taken in Kandahar. The Military Commission, another loose body of senior Taliban officials, was technically in authority of military affairs. However, Mullah Omar remained head of the Taliban armed forces, and the Military Commission accordingly seemed to limit itself to planning strategy and in some cases the implementation of tactical decisions. It had no strategic decision-making powers, and all decisions on military strategy, appointments of key commanders, and the allocation of funds were taken by Mullah Omar. Under Mullah Omar, there was a chief of the general staff and chiefs of staff for the army and air force, supposedly in command of ground operations and air operations, respectively.[23] Military operations were supposed to be directed by the minister of defence or the military chief of staff. However, it seems that ground operations remained in the hands of various local task force commanders, several of whom were also members of the Taliban government.[24] The Taliban ran an intelligence service, the *Istakhbarat* (named after, and no doubt at first assisted by, Saudi intelligence).[25]

Due to its foreign support, the early Taliban movement operated more as a conventional although semi-irregular military force than as an actor in hybrid warfare. For all its harsh policies, the Taliban movement never engaged in terro-

---

to a Northern Alliance offensive that managed to maintain its momentum until the summer of 1999. Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 48, 72, 131, 138f, 201f, 227ff and 264 n.16.

23 Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 95ff and 220f.

24 Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000.

25 Burke, Jason: Lies, Payoffs, Traps Are Allies' Weapons. Observer (UK), as included in Japan Times, 10.11.2001.

rist activities against neighbouring states.[26] However, at times during its offensives, the movement did indulge in what can only be called terrorist activities aimed at its Afghan enemies. Examples include the torture, castration, and killing of former President Sayyid Muhammad Najibullah in 1996, followed by the public display of his corpse, and the massacres of an estimated six to eight thousand civilians in Mazar-e Sharif, Maimana, and Shiberghan in 1998. These acts of terrorism were ordered by the Taliban leadership, and can be interpreted as an active strategy of intimidation directed against the Afghan population.[27]

The Taliban forces varied widely in training and experience. Some had considerable military experience, and many men had received military training in Pakistan, around Kabul, or in other quiet areas of Afghanistan. Others, however, especially some of the recent recruits from Pakistan, had received virtually no training and were frequently trucked straight to the front to take part in combat operations.[28] Most Taliban soldiers received regular salaries. Among those who did were the professional soldiers from the former communist armed forces, serving in the capacity of gunners, tank drivers, mechanics, and aircraft pilots. Although the majority of the professionals were Pashtuns, they were seldom as religiously motivated as other Taliban soldiers, particularly the volunteers from Pakistan.[29]

This description of the first years of the Afghan Taliban movement shows that far from being a tribal army, the early Taliban leaders and in particular their Pakistani supporters were often reasonably sophisticated fighting men, aware of the practicalities of both conventional and irregular warfare. While their military capabilities in the 1990s should not be exaggerated, the Taliban understanding of tactics and strategy was not much inferior to that of their neighbours, something which is easily forgotten in light of the speed in which their state collapsed in the

---

26 Afghanistan was not on the United States list of states sponsoring terrorism, since the United States did not recognize the Taliban government.

27 Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 49f and 73f.

28 Jane's Information Group: Jane's Sentinel Security Assessment: Afghanistan, 30.08.2000.

29 Rashid, Ahmed: The Taliban: Exporting Extremism. In: Foreign Affairs November/December 1999, p. 100.

face of the Afghan Northern Alliance campaign on the ground supported by American-led air support in late 2001.[30]

The Post-2001 Taliban Movement

With the invasion of U.S.-led forces in October 2001, the Taliban movement retreated into Pakistan. Following the withdrawal, it took some time before the Taliban movement fully reorganized and reconstituted itself as a military force. Due to the large and resilient support system the Taliban had acquired during its rule prior to 2001, the Taliban remained the largest threat to stability in Afghanistan.[31] This was facilitated by the fact that until 2005, the Taliban were not under serious military pressure.[32] In Pakistan, the Taliban movement continued to receive substantial support from Pakistani sources.[33]

From the viewpoint of the international coalition, the conflict in Afghanistan can be summarized as having consisted of four phases. In 2001-2005, the international forces followed the Light Footprint approach, which resulted in modest and insufficient foreign military and financial aid to the government of Afghanistan. The U.S.-led coalition was from 2003 onwards also distracted by the Iraq War. In the years 2005-2009, a Taliban resurgence took place, largely as a result of the Light Footprint of previous years and the existence of Taliban sanctuaries in Pakistan. By then, foreign aid was increasingly used as a tool for short-term

---

30 Hammer, Carl: Tide of Terror. America, Islamic Extremism, and the War on Terror. Boulder, Colorado 2003, p. 223ff.

31 National Counterterrorism Center (NCTC): Afghan Taliban. NCTC web site, <www.nctc.gov>, 2013.

32 Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 244.

33 See, e.g. Fredholm, Michael: The Need for New Policies in Afghanistan: A European's Perspective. Himalayan and Central Asian Studies 15: 1-2 (2011), p. 54ff, on 67. In time, the Taliban also began to receive some support from Iran. In 2010, at least three meetings between Iranian Islamic Revolutionary Guards Corps (IRGC, *Pasdaran-e Enghelab-e Islami*) officers and Taliban leaders took place. The Iranians reportedly had considerable success in offering patronage to individual Taliban commander Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 247, 257.

stabilization in response to Taliban activity, instead of for much-needed long-term developments. The years 2009-2011 saw a U.S. military and civilian surge, accompanied by a substantial increase in aid. Unfortunately, the surge did not succeed in uprooting the Taliban insurgency. The years 2011-2014, finally, were characterized by the concept of transition intended to accomplish Afghan assumption of full sovereignty. Paradoxically, transition and full sovereignty were accompanied by almost complete foreign aid dependency, since insufficient long-term developments had taken place to ensure Afghanistan's economic future.

It follows from this that the Taliban movement was granted several quiet years in which to grow in strength, without being under serious military pressure anywhere. Yet the movement was an exile organization, without the benefits of being in control anywhere outside its Pakistani sanctuaries. Consequently, the Taliban movement came to fragment into several semi-autonomous organizations, nominally united under Mullah Omar and what became known as his Quetta Shura, so named since it was for many years based in the Pakistani city of Quetta.

The Taliban was never a homogeneous movement, not even in the 1990s, and the divisions remained and to some extent deepened in exile. Mullah Omar and the Quetta Shura had one agenda, which the affiliated and allied groups only shared in part, since they had agendas of their own. In addition, even the Quetta Shura was a decentralized organization and in most cases consisted of loose units independent of each other, even though they all claimed allegiance to Mullah Omar. In fact, the Quetta Shura itself fragmented. In 2012, a power struggle emerged within the Shura, and internal rivalries sharpened in 2013.[34] By mid-2013, Mullah Omar remained the nominal head of the movement, although its members sometimes believed that he was held captive in Pakistan, or even that he was dead (he was not, as it turned out).[35] The Taliban movement was then

---

[34] Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013; Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 6.

[35] Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013; Ron Moreau: Taliban Forces Desperate to Hear from Their Absent Leader, Mullah Omar.

widely regarded by its own members as having become divided into several largely autonomous alliances. These were the original Leadership Council in Quetta,[36] Abdul Qayyum Zakir's alliance within the Quetta Shura,[37] Akhtar Mansur's alliance within the Quetta Shura,[38] the Peshawar Shura,[39] and the Miram Shah Shura, also known as the Haqqani Network.[40] However, by April 2014 some of the tensions and divisions were resolved with the removal of Abdul Qayyum Zakir from the Military Commission, ostensibly owing to illness.[41]

Daily Beast, 01.05.2013. < http://www.thedailybeast.com/articles/2013/05/01/taliban-forces-desperate-to-hear-from-their-absent-leader-mullah-omar.html>.

36 The Leadership Council (Rahbari Shura) in Quetta was the main decision-making body of the Taliban and accordingly included several old Taliban leaders. Although of diminishing importance because of a decline in revenue and power, as a collective force the Rahbari Shura still enjoyed a certain amount of prestige within the movement.

37 Abdul Qayyum Zakir's alliance within the Quetta Shura was based on Zakir's personal network but also included those of several other Taliban leaders. Zakir, a former Guantanamo detainee transferred to Afghan custody who following his 2007 release by Hamid Karzai's government returned to the insurgency and in 2009 was appointed head of the Quetta Military Commission, was supported by both the Pakistani government and the Peshawar Shura, thus enjoying his own sources of revenue. See, e.g. Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 17.

38 Akhtar Mansur's alliance within the Quetta Shura was based on Mansur's personal network, funded from sources inside Afghanistan and among the Afghan Diaspora, and also included the powerful Baradar and Dadullah networks (the latter revived in 2010-2011 after a period of disorder due to the death of its founder; Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013, p. 3) in common opposition to Abdul Qayyum Zakir. As head of the Quetta Political Commission, Mansur had considerable political influence.

39 The Peshawar Shura, which itself consisted of several smaller networks, some of which were of Pakistani jihadist origin, was reportedly more state- and university-educated than clerical as well as directly supported, and thus under a certain level of control, by the Pakistani government. See, e.g. Giustozzi, Antonio: Turmoil within the Taliban: A Crisis of Growth? Central Asia Policy Brief 7, Central Asia Program, George Washington University 2013, p. 2; Giustozzi, Antonio: The Taliban and the 2014 Elections in Afghanistan. Washington, DC 2014, p. 17.

40 Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

41 Voice of Jihad: Statement dated 25.04.2014.

Nominally, the organization known among Western analysts as the Haqqani Network but in Afghanistan more often referred to as the Miram Shah Shura formed a part of the Peshawar Shura. However, being the most formidable of the various alliances within the Taliban movement, this was a fundamentally autonomous wing of the Afghan Taliban movement based in Miram Shah in Pakistan and named after its leader, Jalaluddin Haqqani.[42] The Haqqani Network was a distinct military and political organization created by Jalaluddin Haqqani during the 1980s which, after the war against the Soviet Union, remained a source of power in the borderlands shared by Afghanistan and Pakistan. The Haqqani leaders were experienced; having survived three decades of warfare, educated in theology, and with a sophisticated understanding of international trade and politics. Their patriarch, Jalaluddin Haqqani, had earned the name Haqqani as an honorific title as a result of his studies at the prestigious Dar ul-Ulum Haqqaniyyah *madrasah*. He spoke excellent Arabic, as did his son Sirajuddin, and both had first-rate connections in the Arab world. The Haqqanis could discuss the intricacies of Islamic theology in the language of the Prophet, and kept a low profile by avoiding Western journalists, thereby also avoiding the taint of international terrorism for decades, despite close links to Al-Qaida.[43]

Affiliated to the Taliban movement but even older than the Haqqani Network was the Hezb-e Islami of Gulbuddin Hekmatyar (HIG), popularly named for its leader Gulbuddin Hekmatyar, a former Afghan warlord and prime minister and one time ally of the United States. Originally a political party in the 1980s involved in the war against the Soviet Union, the HIG had political allies in the Afghan parliament, may have supported its own candidate in the 2014 presidential election (possibly Qutbuddin Hilal who once served under Hekmatyar[44]), and was perhaps the most politically sophisticated and well-established Afghan in-

---

42 Gopal, Anand/Mahsud, Mansur Khan and Fishman, Brian: The Battle for Pakistan. Militancy and Conflict in North Waziristan. Washington, DC 2010; Peters, Gretchen: Crime and Insurgency in the Tribal Areas of Afghanistan and Pakistan. Harmony Program, Combating Terrorism Center, West Point 2010; Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

43 Rassler, Don/Brown, Vahid: The Haqqani Nexus and the Evolution of Al-Qaida. Harmony Program, Combating Terrorism Center, West Point 2011.

44 Institute for War and Peace Reporting, 27.03.2014.

surgent group. Most Hezb-e Islami members were then detribalized Pashtuns from the state-educated state intelligentsia. The leaders were primarily intellectual Islamists from an urban background, so the party lacked a firm tribal base. This was in fact an advantage, as the party tended to recruit where tribal structures had broken down, which made it highly popular in Pakistani refugee camps. The party, radical Islamist in world view, was regarded as the best organized and most disciplined party within the anti-Soviet resistance. However, Hekmatyar's organisation collapsed as Pakistani funds from 1994 were diverted from it to the newly created Taliban movement. Reportedly with thousands of sympathisers and fighters, HIG had strong relations with Al-Qaida and was closely linked with the Afghan Taliban. Hekmatyar and his followers were believed to have remained operating chiefly in Kunar Province, Afghanistan.[45]

Then there were several similarly autonomous groups of foreign fighters, including the remnants of the Al-Qaida core as well as groups such as the Uzbek-led Islamic Movement of Uzbekistan (IMU) and the Pakistani, ethnically Pashtun terrorist group, the Tehrik-e-Taliban Pakistan (TTP, "Movement of Pakistani Taliban"). All these groups enjoyed bases and sanctuaries in Pakistan.

It was never known how many insurgents operated in Afghanistan. Besides, many were, at any given moment, based on the Pakistani side of the border. A common estimate was up to 25.000 Quetta Shura Taliban fighters, in addition to about 3.000 Haqqani fighters and 1.000 HIG fighters. As for Al-Qaida and other foreign fighters, their total number in Afghanistan was unlikely to have exceeded a thousand and was likely far fewer, probably only numbering a few hundred.[46] Since the foreign fighters played a strictly supporting role in Afghanistan, their means and motivations will not be further covered here.[47]

The post-2001 Taliban movement was, as a military force, less conventional in outlook than the old 1990s Taliban, but no less sophisticated and not lacking connections in a large number of countries. Moreover, the existence of sanctua-

---

45 GlobalSecurity: Hizb-i-Islami. 15.08.2012.

46 Katzman, Kenneth: Afghanistan. Post-Taliban Governance, Security, and U.S. Policy, Washington, DC 2012, p. 48.

47 On that topic, see, e.g. Fredholm, Michael: Afghanistan Beyond 2014. Stockholm 2013.

ries in Pakistan enabled the movement to develop strategies based on hybrid warfare and hybrid threats.

Hybrid Warfare and Hybrid Threats

As noted, the hybrid warfare and hybrid threat capability developed by the Afghan Taliban included different tactics and strategies to be employed at home and abroad. From both an analytical and practical perspective, these two theatres of war are best described as distinct from one another.

Being at war, the Taliban movement engaged in hybrid warfare in Afghanistan. Abroad, the movement instead utilized its capacity for hybrid threats. The domestic threat in Afghanistan deriving from the Taliban and the international threat of the movement were, consequently, quite different in character.

5.2.2 The Domestic Theatre: Hybrid Warfare

Military Power Projection against the ISAF and ANSF

In Afghanistan, the Taliban soon began to carry out a hybrid warfare campaign against the international coalition (Operation Enduring Freedom and the International Security Assistance Force, ISAF) and the fledgling Afghan National Security Forces (ANSF). The purpose of the campaign was to defeat or at least intimidate the coalition. Some Taliban leaders conceived that inflicting casualties on the foreign military forces would demoralize public opinion in their country of origin, causing panic among politicians, and thereby force a withdrawal.[48]

The hybrid warfare campaign consisted of two mutually supporting activities. First, the Taliban employed military power, early on by what in effect were guerrilla-style attacks but soon thereafter they increasingly made use of Improvised

---

[48] See, e.g. Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 255.

Explosive Devices (IEDs) placed at convenient locations, in particular along roads, in vehicles, or used in suicide attacks. The IED campaigns had the dual objective of limiting the freedom of movement of the international military forces and at the same time intimidating the foreign soldiers, if they could not be defeated outright.[49]

Pakistani military support, whether official or non-official, was particularly conspicuous in the IED campaign. As late as 2011, IED specialists in southern Afghanistan were still often of Punjabi origin. Locals believed that they were Pakistani Army specialists. When killed, the IED specialist would have to be replaced, so a replacement IED specialist was sent from the Taliban leadership. As a result, there was a degree of central control over the IED effort, which again suggests Pakistani involvement.[50] The Taliban had an IED development centre in Pakistan. The Taliban confirmed that Iraqi insurgents assisted them with IEDs, but ISAF assessed that both Iranian and Pakistani support played a major role.[51]

Since the Taliban knew that ISAF's rules of engagements did not permit the killing of minors, the Taliban developed a strategy of employing children as emplacers of IEDs.[52] In effect, this was yet another form of hybrid warfare tactics, since any killings of children by ISAF could be used for propaganda purposes.

Terror Power Projection against the ISAF and ANSF

At the same time, the Taliban employed what can best be termed terror power, through the use of suicide bombers against international and Afghan military targets. Sometimes they were particularly effective, such as when on 15 January 2006 the director of the Canadian Provincial Reconstruction Team (PRT), seni-

---

49 For an example of the Taliban IED campaigns, see Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 29.

50 Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 250ff.

51 Ibid., p. 252.

52 Ibid., p. 251.

or diplomat Glynn Berry, was killed in Kandahar City.[53] Tactics developed in which one or more suicide bombers were used to spearhead an assault which then was followed up with guerilla-style forces (a tactic incidentally first development in Chechnya[54]). Results could be spectacular, such as when the Taliban attacked Sarpoza Prison on the outskirts of Kandahar City on 13 June 2008 with a vehicle borne IED (VBIED), a suicide bomber, and a rapid full scale attack by Taliban fighters on motorcycles. Some 400 imprisoned Taliban fighters were released, then removed in buses which the Taliban had waiting outside.[55]

The purpose of the terror campaign was to intimidate the ISAF coalition into withdrawing its forces. A further objective was to create success stories which could be used for propaganda purposes (see below).

Terror Power Projection against the Afghan Population

The Taliban also engaged in terror campaigns directed specifically against the Afghan population. This can be seen as a continuation of the policies used by the Taliban in the 1990s (see above). Terror power was used to intimidate the population into defecting from the government supported by international forces and the ANSF. Shadow government structures (often far better organized than the governing structures used when the Taliban in fact ruled major parts of Afghanistan pre-2001) were set up to exert control over the population. Examples of the use of terror power include the killings of collaborators (government workers and ordinary Afghans who reported the location of Taliban units or IEDs to the international military forces) and what the Taliban in religious terms labelled apostates, that is, Muslims who did not subscribe to the extreme version of Islam adopted by the Taliban. The Taliban would then execute, often by beheading, a number of locals for cooperating with foreign troops, displaying the corpses in public as a warning to others.[56] These methods had a

---

53 Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 25.

54 Fredholm, Michael: The New Face of Chechen Terrorism. Central Asia - Caucasus Analyst, September 2003, Johns Hopkins University, Georgetown.

55 For this and other examples, see, e.g. Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 40 and 46.

56 Ibid., p. 25 and 42.

major impact on the Afghan rural population. Cases were noted when Afghan National Police (ANP) units failed to engage the Taliban, since they knew that they or their families would then face the prospect of Taliban reprisals.[57]

In a similar manner, the Taliban regularly attempted to dissuade people from voting in the national elections. A common method to influence voters not to participate was to cut off the index finger of those who went to the polls, who were easily recognizable since dipping the finger in black ink was part of the election process.[58] The campaign served a dual purpose. First, it terrorized the population into adopting the extreme version of Islam which served as the Taliban movement's ideology, since the Taliban considered democratic elections an affront to Islam. Second, the mutilations eroded trust in the Afghan government.

Another example of how the Taliban imposed their will by terrorist power was the strategy to force telecom operators to close cellular telephone networks at night. The Taliban believed that the international military forces used cellular phone signals to track and launch attacks against them. This was probably a correct assessment since cell phones periodically send signals to the network even when they are not in use making calls and such signals can be monitored by signals intelligence, satellites, and other means. But the Taliban also feared that ordinary Afghans on the side of the government might observe them and wished to prevent such collaborators from privately calling in to report Taliban movements. ISAF set up a call centre for this very purpose in 2007. Since most Taliban movements took place at night for reasons of security, this was the time to shut down the telephone networks. For this reason, the Taliban began to blow up telecommunications towers following threats to telephone operators warning them to shut down the towers at night or face attack. When telephone service providers responded by following the Taliban movement's orders, the Taliban not only ensured their own security, they also made a huge impact on the Afghan population, eroding their will to resist Taliban control by showing them by example that it was the Taliban movement, not the government forces, which set the agenda.[59] This successful intimidation campaign enabled the Tali-

---

57 Ibid., p. 30.

58 See, e.g. BBC News, 15.06.2014.

59 See, e.g. the Textually.org web site <www.textually.org/textually/archives/2008/03/019260.htm>; citing AP, 01.03.2008;

ban to impose a strategic, delegitimising blow to the authority of the government.

A similar delegitimizing effect was achieved by the widespread assassinations of government leaders, high-ranking members of the clergy on the side of the government, and women in public service and girls' schools. While government leaders and women in public service were primarily targeted for political reasons and to intimidate the population, the assassination of pro-government clergy had the added effect of reducing their influence with the population. Those who were not killed had to remain in Afghan National Army (ANA) compounds from which they primarily preached by radio, not in person, which severely limited their impact and cleared the field for Taliban clergy to win the battle for souls.[60]

Media Power Projection against the Afghan Population

In the battle for souls, the Taliban also exercised its media power. This showed itself as proclamations and videos distributed online and by other means. The Taliban also used night letters, which were leaflets distributed at night, thus serving as a tangible reminder that the Taliban had a presence seemingly everywhere.[61] Due to the widespread illiteracy in Afghanistan, the night letters were often read out aloud by a mullah or an elder, which in itself increased the impact of the message. Media power fundamentally consisted of the dissemination of threats to collaborators and propaganda, which not only resulted in the winning of hearts and minds but also in the intimidation of the general public, who realized then, if not before, that when the foreigners eventually withdrew, the Taliban would remain.

Examples of intimidating propaganda included the video recording of public execution by stoning in August 2010 of a couple in Kunduz who in the eyes of

---

Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 33.

60 See, e.g. Forsberg, Carl: The Taliban's Campaign for Kandahar. Institute for the Study of War, Washington, DC 2009, p. 44ff.

61 Johnson, Thomas H.: The Taliban Insurgency and an Analysis of Shabnamah (Night Letters). In: Small Wars and Insurgencies 18: 3 (September 2007), p. 317ff.

the Taliban had committed adultery, the recording of which was subsequently distributed through the Internet.[62]

Power Projection through Organized Crime

The Taliban also enlisted, in a manner, the help of organized crime.[63] The Taliban often encouraged the activities of local bandit gangs in areas where the Taliban movement had not yet established, but was working to gain, a presence. Not only did this facilitate Taliban activities by causing confusion and presenting additional targets to the international military forces and ANSF, the activities of bandit gangs also legitimized the subsequent imposition of Taliban justice and its harsh methods. In effect, the Taliban first encouraged the growth of crime, then stepped in to suppress it. Many bandit gangs would indeed find the arguments to join the Taliban movement persuasive at this time, especially if they had already used the Taliban name to discourage police and local communities from resisting.[64]

5.2.3 The International Theatre: Hybrid Threats

Diplomatic Power Projection against the ISAF Member States

Internationally, the Taliban primarily focused on diplomatic power projection. A major aim was to negotiate the withdrawal of the international coalition, with threats if necessary, so that the Taliban could return to power. For this task, the

---

62 Reuters, 16.08.2010; The Telegraph (UK), 27.01.2011 (<www.telegraph.co.uk>, with video).

63 Here we will disregard the question of the extent to which the Taliban movement funded its activities through Afghanistan's abundant opium production. The opium trade was fundamentally a means for funding, thus providing the means to fight, and not intended as a means for hybrid threat projection as such, even though one could argue that in the long term, drugs from Afghanistan would play its role in destabilizing some of the states which provided troops to ISAF.

64 Giustozzi, Antonio: Military Adaptation by the Taliban 2002-2011. In: Farrell, Theo/Osinga, Frans and Russell, James (eds.): Military Adaptation in Afghanistan. Stanford 2013, p. 245.

Taliban relied on diplomatic power, with negotiations conducted through friendly Muslim countries such as Pakistan, Saudi Arabia, the United Arab Emirates, and Qatar. These countries were not chosen at random; only Pakistan, Saudi Arabia, and the United Arab Emirates, in this order, had recognized the Taliban Emirate of Afghanistan in May 1997.[65]

The diplomatic process against ISAF member states can be said to have begun in September 2009 in Dubai, United Arab Emirates. At the request of the Taliban, German intelligence then held a first meeting with a Taliban delegation. A further eight meetings had to take place before the Germans brought in American representatives so that real negotiations could get underway. This first U.S.-Taliban meeting took place outside Munich in Germany on 28 November 2010, with the participation of a Qatari representative whom the Taliban representatives trusted. A second meeting consequently took place in Qatar's capital Doha on 15 February 2011. The third meeting took place in Munich on 7-8 May 2011. Through this series of meetings, the Taliban aimed to persuade the United States to lift sanctions, release high-level Taliban prisoners, and to allow the opening of a Taliban representative office in a Muslim country.[66]

These meetings all took place in secret, and at the time there was little chance for the Taliban to gain a negotiated American withdrawal. However, the Taliban diplomatic campaign eventually paid off in the form of a more public, international diplomatic presence, aimed more at the worldwide Muslim community than at the West.

Diplomatic Power Projection against the Worldwide Muslim Community

Towards the worldwide Muslim community, it was important for the Taliban leadership to appear as a responsible and religiously legitimate party. The Taliban

---

65 AFP, 25.05.1997 (Pakistan, on 25.05.1997); The News International, 27.05.1997 (Saudi Arabia, on 26.05.1997); AFP, 28.05.1997 (UAE, last of the three). Incidentally, the Taliban government in turn recognized the separatist government in the Russian republic of Chechnya in January 2000, an act which caused the lasting enmity of Russia. Jane's Sentinel: Afghanistan, 01.06.2000.

66 Rashid, Ahmed: The Truth behind America's Taliban Talks. In: Financial Times, 29.06.2011.

did not mind meeting with the Kabul government, as long as they met as equals. This was accomplished when Saudi King Abdullah hosted talks with the Taliban in the holy city of Mecca from 24 to 27 September 2008.[67]

However, it took some time before suitable conditions for further meetings could be agreed, not least because of difficulties for outside observers to ascertain whether the alleged Taliban representatives who turned up from time to time really represented Mullah Omar. In June 2013, formal peace talks between the Afghan government and the Taliban were finally announced, to take place in Doha. However, the Qatari leaders were somewhat too hospitable to their Taliban guests, allowing them to open a formal representative office, and the talks were cancelled in a row over the Taliban displaying their flag and presenting themselves as the legitimate rulers of the Islamic Emirate, that is, the state of Afghanistan. The Doha office was closed within 24 hours of its opening, amid speculations that negotiations would reopen in Turkey or Saudi Arabia.[68]

Nonetheless, the Taliban had achieved their aim of appearing as a responsible and legitimate party. Besides, U.S. President Barack Obama had by then announced the planned drawdown of American military forces in Afghanistan, so for the Taliban leadership, it was only a question of time before they could make a move for real power. When in early 2014, Taliban leaders met representatives of the Afghan government in Dubai, United Arab Emirates, and in Riyadh, Saudi Arabia, they refused to negotiate a peace agreement.[69] This led to discussions on whether the Taliban representatives had been genuine emissaries of Mullah Omar or frauds; however, there was at this time no reason for the Taliban movement to negotiate further, since they had already achieved their key diplomatic aim of being seen as a legitimate party.

Media Power Projection against the ISAF Member States and the Worldwide Muslim Community

In conjunction with the application of diplomatic power, the Taliban movement also made good use of media power projection. The media campaign was aimed

---

67 CNN, 05.10.2008.
68 Reuters, 14.08.2013.
69 The New York Times (USA), 04.02.2014.

simultaneously at the ISAF member states and the worldwide Muslim community. Its purpose was to show the might of the Taliban, the hopelessness of continued war against them, and their legitimacy vis-à-vis the worldwide Muslim community.

Already in the 1990s, the Taliban had operated a series of web sites, and this practice continued from the sanctuaries in Pakistan. Taliban web sites primarily published statements of the Leadership Council of the Islamic Emirate of Afghanistan, that is, the Taliban government, but they also published articles, weekly analyses, interviews, and reports, as well as a continuing list of news from the front. For an example of the latter, see Table 9. The emphasis was on enemies killed, in particular foreigners, ANA troops, and Arbakis (self-defence militias on the side of the government), and installations attacked.

11/05 : Enemy vehicle blown up in Kunduz
11/05 : Enemy base struck with missile strikes in Logar
11/05 : Arbakis come under attack in Kunduz
11/05 : Base in Logar comes under artillery rounds
11/05 : 46 killed, many injured in Ghazni operation
11/05 : 6 killed in gunfight in Nangarhar
11/05 : 6 Arbakis killed in Wardak
11/05 : Commander along with 2 police captured in Kabul
10/05 : 5 enemy soldiers killed, 4 injured in Ghazni
10/05 : Enemy security post destroyed in Laghman
10/05 : Army installations attacked in Kabul
10/05 : Enemy check point attacked
10/05 : Mortar shells hit post; Arbaki killed
10/05 : Clash occurs as enemy attacked in Paktika

10/05 : Arbaki commander, 2 gunmen killed in Paktika
10/05 : Arbaki militias suffer deadly losses in Kunduz
10/05 : 6 killed, two armored tanks destroyed in Kunduz
10/05 : 14 killed, 22 vehicles destroyed as convoy ambushed
10/05 : Double martyrdom attack causes U.S.-nato invaders heavy losses
10/05 : 5 puppets[70] killed and wounded, vehicle and equipment seized
10/05 : Check post attacked, 3 police killed in Marjah
10/05 : 3 police and ANA trooper killed in clash
10/05 : 5 ANA and 3 Arbakis killed in Gerishk, equipment seized
10/05 : Roadside bomb rips through police truck, kills and wounds 4
10/05 : Chora firefight leaves 2 puppets wounded

Table 9: Sample text from Taliban web site *<http://shahamat-english.com/>, 11.05.2014.*

[70] Afghans who supported the international forces.

The Taliban movement also published a glossy, professionally produced electronic news magazine in English, with news from the front, lists of destroyed enemy aircraft, statistics of attacks, articles, interviews, and the like. This was *Islamic Emirate Afghanistan In Fight*, a publication with many colour photographs, including photos of killed and wounded enemy soldiers and destroyed enemy vehicles. The magazine was most likely published and distributed from Pakistan.

The Taliban also discovered, and made good use of, Twitter. As a tool for the dissemination of brief propaganda nuggets in English, Twitter eventually began to rival the Taliban web sites. The Taliban tweets focused on news from the front, with the customary emphasis on enemies killed and installations attacked. For a few examples of Taliban tweets, see Table 10.

Abdulqahar Balkhi @ABalkhi A martyrdom seeker detonated car bomb on dismounted foreign troops in front of Maiwand district HQ building (#Kandahar) 3:30pm today... Abdulqahar Balkhi @ABalkhi cont: as other troops gathered to evacuate the casualties around destroyed tank, another martyrdom seeker approached & detonated motorbike. Abdulqahar Balkhi @ABalkhi cont: blasts killed more than 15 invaders & wounded many on final day of #KbWaleed operations, area cordoned off from public #Afghanistan Abdulqahar Balkhi @ABalkhi A US terrorist along with Arbaki lapdog were killed, 3 US invaders wounded in missile strike on Shilgar district HQ (#Ghazni) 10am Wed.

Table 10: Sample Taliban tweets
<https://twitter.com/ABalkhi>, 07.05.2014

Terror Power Projection against ISAF Soldiers' Family Members

While the Taliban media campaign did have the objective of influencing the population in the ISAF member states, the Taliban no doubt realized that few ordinary Westerners would read their magazines, announcements, or tweets. Something more tangible was therefore needed to influence public opinion in the ISAF member states. For this purpose, apparent Taliban agents issued threats by telephone or Short Message Service (SMS) text messages to the family members of ISAF soldiers serving in Afghanistan on a number of occasions. Some were threats that family members would be murdered if the soldier did not leave Afghanistan, while others assured family members that it was the ISAF soldier who would be killed, if his or her family did not get their offspring back home. There was little doubt that the threats were meant to intimidate the individual into resigning from service in Afghanistan. Some calls emanated from the area of operations in Afghanistan, while others originated within the ISAF member state, likely within the Afghan refugee Diaspora. This showed the apparent worldwide reach of the Taliban movement. Less obvious but possibly equally serious, was that the telephone and SMS threats were directed to the private telephones of family members, which could only have been identified by somebody taking note of the private calls from ISAF garrisons to the place of origin of the troops. This showed that the Taliban had been able to infiltrate at least some of the Afghan telecom companies providing roaming services.[71]

Among the various types of international hybrid threat projection employed by the Taliban, this was the only one which was not exclusively directed and executed from Pakistan. Threatening telephone calls and text messages also emanated from within the ISAF member states, proving that the Taliban had supporters within the Afghan Diaspora and among other groups overseas.

Terror Power Projection in the Form of Attacks Abroad

As far as is known, none of the telephone threats resulted in an actual attack. Indeed, a conspicuous characteristic of the terror power projection

---

[71] Radio Sweden news program *Ekot*, 01.07.2010; Försvarsmakten (Armed Forces), Årsrapport Säkerhetstjänst 2011: Militära underrättelse- och säkerhetstjänsten, MUST (Försvarsmakten 2012), p. 18.

abroad of the Afghan Taliban movement was that the Taliban neither planned, nor carried out through opportunistic means, terrorist attacks *outside* Afghanistan. This did not happen during the 1990s, nor after the Taliban withdrawal into Pakistan. International terrorism would seem to have been a certain means to intimidate a foreign population into forcing a withdrawal of its military forces from Afghanistan. Yet no such attacks were carried out by the Afghan Taliban movement (although they certainly were carried out by the Taliban movement's allies among the Al-Qaida and other international terrorist groups for reasons of their own).

The reason for this curious absence of international terror power projection can presumably be seen in two characteristics of the Afghan war. First, the Afghan Taliban movement had no history of engaging in terrorism abroad and many of its leaders had little interest in events elsewhere. Second, from 18 June 2004, when the first known American drone attacks was carried out,[72] a balance of terror emerged between the United States and the Taliban movement. As long as the Afghan Taliban movement did not sponsor international terrorism, the United States did not direct any drone attacks against the senior Afghan Taliban leaders in Pakistan. Whether this was a deliberate agreement with the Americans, if so it was no doubt negotiated with the help of Pakistani mediators, or merely an assumption on the part of the Taliban leadership remains unknown. Implicit in the understanding must have been the American realization that one eventually would need to have somebody to negotiate with in the Taliban leadership. Whether this conclusion is correct remains unknown to outside observers. Yet the fact remains that the Taliban leadership did not sponsor international terrorism, and no American drone attacks were aimed against the senior Taliban leaders in their well-known and easily recognizable compounds in a suburb of the Pakistani city of Quetta.

5.2.4 Concluding Remarks

The Taliban leadership had a *long-term strategy* to gain political power and impose a strict form of Islam in Afghanistan. When faced with the inability to defeat the coalition by regular military means, the long-term strategy

---

72 The New York Times (USA), 19.06.2004.

hardened into an *intention* to fight with whatever tactics and strategies that were available. Although not conclusively proven, it seems likely that a *master plan* on how to oppose the coalition and the government of Afghanistan through a combination of military power and terror power was worked out with the assistance of former or serving ISI officers. The actual details – the *operations plan* – grew out of developments in Afghanistan and elsewhere, such as the limited number of foreign troops that were sent to Afghanistan. The Light Footprint policy, that is, the lack of boots on the ground, enabled the Taliban movement to reassert power in parts of the country. The *execution* phase of the operations plan began with full force only from 2005, since, despite incursions into Afghanistan, the Taliban were, as noted, earlier not under serious military pressure there or elsewhere.

This operations plan certainly included aspects of hybrid warfare and hybrid threats. Whether the Taliban actually used such terms is a moot point; events show that they knew about and understood the concepts of hybrid warfare and threats very well. The Afghan Taliban leaders consequently developed a hybrid threat capability, which they subsequently used as part of the tactics and strategies of the movement.

There is no denying that the Afghan Taliban movement enjoyed a certain level of success in its hybrid warfare campaigns. Most successes derived from the movement's capability to create and sustain a domestic hybrid capability. While the Taliban hybrid warfare capability was not in itself sufficient to defeat the international coalition, it certainly helped to create a sense of defeatism which ultimately led to President Obama's 22 June 2011 decision to end the American-led military presence in Afghanistan by 2014.[73] But this defeatism was not the result of the Taliban movement's attempts to intimidate the foreign militaries or their constituencies abroad. Instead, it derived directly from the Taliban ability to intimidate the Afghan population into turning away from the foreign military presence and the government of Afghanistan, an effect much facilitated by the general ineptitude and widespread corruption of the latter during these crucial years.

---

[73] The New York Times (USA), 22.06.2011.

Then why did the Afghan Taliban movement neither plan, nor carry out through opportunistic means, terrorist attacks outside Afghanistan? International terrorism would seem to have been a certain means to intimidate an enemy population into forcing a withdrawal of its military forces from Afghanistan, yet no such attacks were carried out by the Afghan Taliban movement—and the behaviour of the Taliban toward the Afghan population shows that it was not a reluctance to engage in violence that decided the issue. The reasons for this lack of foreign terrorism were no doubt twofold. First, the Afghan Taliban had no history of engaging in terrorism abroad. Second, a balance of terror emerged between the Taliban and the U.S.-led coalition. As long as the Afghan Taliban movement did not sponsor international terrorism, no drone attacks targeted senior Afghan Taliban leaders in Pakistan.

This balance of terror also illustrates the phenomenon that successful insurgencies tend to share two common features: access to sanctuaries in a neighbouring country and access to material support and financing from outside the conflict zone, either in the neighbouring country or from a Diaspora population abroad. In 1964, the experienced French counterinsurgency and counterterrorism practitioner Roger Trinquier concluded that the best strategy to confront such an insurgency was a secret war against the neighbouring country, through the creation of a clandestine guerrilla force on its territory to strike the insurgent sanctuaries and serve as leverage until the material support ceases.[74] The armed drone program, which was led by the civilian Central Intelligence Agency (CIA) and

---

[74] Trinquier, Roger: Modern Warfare: A French View of Counterinsurgency. Westport, Connecticut 2006 (first published in 1964), p. 83. Trinquier describes the enemy in both counterinsurgency and counterterrorism as an armed clandestine organization, engaged in clandestine warfare. The clandestine organization operates in one or both of two modes, that of partisan/guerrilla and terrorist, respectively. These two categories function in different ways since they operate in different types of terrain. In the partisan/guerrilla mode, an armed clandestine group will choose targets to establish a presence and gain territorial control through a display of power. The post-2001 Taliban movement operated in this mode in Afghanistan, and the same went on among jihadist insurgents in Pakistan, Yemen, Somalia, Mali, Syria, and fundamentally in any other place where armed clandestine groups operated. Having established a degree of territorial control (cf. Al-Qaida in Afghanistan prior to 2001), the group was, simultaneously with conducting local operations, free to engage, or not, in international terrorism as well. Ibid., p. 16. Yet the importance of a local base is often forgotten in terrorism studies. Trinquier's experiences could have been particularly useful in post-2001 Afghanistan but were largely forgotten when operations were initiated.

utilized a combination of military and terror power, was in effect a high-tech version of such a clandestine force, which in the context of the present paper easily qualifies as a hybrid threat response to a hybrid threat.

There could be no purely military solution to the problem of Taliban and foreign fighters as long as they retained sanctuaries in Pakistan.[75] History is rife with cases in which guerrilla groups could not be defeated as long as they were granted sanctuaries in neighbouring countries. A military solution could certainly have been found—if the coalition had been prepared to follow the enemy into their sanctuaries in Pakistan. However, the countries that constituted ISAF were unwilling to do so without Pakistani cooperation, and such was never likely to be forthcoming since Pakistan was sensitive about its territorial inviolability and integrity. The problem of the inviolability of the Pakistani sanctuaries of the Taliban became evident when U.S. conventional troops launched the only major ground offensive in the 2001-2002 war against the Taliban. This was Operation Anaconda, commanded by Major General Franklin Hagenbeck and commenced on 1 March 2002 against what was reported to be a concentration of several hundred Taliban and Al-Qaida troops south of Gardez in Paktia province.[76] This was the first time U.S. and coalition conventional forces were at the forefront of ground combat. Operation Anaconda was declared over on 18 March 2002. As before, the Taliban and Al-Qaida fighters simply dispersed and withdrew, many of them into Pakistan, when the battle turned against them. After the operation, Major General Hagenbeck indicated the need to engage in hot pursuits into Pakistan, but on 25 March he was overruled by then Secretary of Defence Donald H. Rumsfeld.[77] As a direct result of Rumsfeld's decision, the Taliban and allied non-Afghan terrorist groups established bases in Pakistan, the Taliban set up in and around Quetta and the Al-Qaida and other foreign fighters went, primarily, to Waziristan.

How could the coalition reach and neutralize these bases? By military means, it could not, since no coalition soldiers were permitted to engage in hot pursuit

---

75 Fredholm, Michael: The Need for New Policies in Afghanistan: A European's Perspective. Himalayan and Central Asian Studies 15: 1-2 (2011).

76 John Pike: Operation Anaconda. 05.07.2011. <http://www.globalsecurity.org/military/ops/oef-anaconda.htm>.

77 Hammer, Carl: Tide of Terror: America, Islamic Extremism, and the War on Terror. Boulder, Colorado 2003, p. 281.

into Pakistani territory. Drone warfare became the solution, and the CIA's clandestine Predator and Reaper armed drone program inflicted significant losses on terrorists and insurgents in Waziristan.[78]

The drone campaign had a strategic effect that went far beyond the killing of insurgent leaders and the disruption of insurgent networks and activities. First, data-driven as opposed to anecdotal research shows that drone strikes were associated with decreases in the incidence and lethality of terrorist attacks. They were also associated with decreases in particularly lethal terrorist tactics, including suicide and IED attacks.[79] A primary reason for this was the disruption mechanism of drone strikes. Strikes disrupted and reduced the ability of terrorists in the safe havens to operate in a cohesive and effective manner. The havens were simply not safe anymore, and the terrorists found it increasingly difficult to exercise sovereign control over their sanctuaries. In addition, the drone strikes resulted in the deaths of many terrorist leaders. This too reduced the ability of the terrorists to engage in violence elsewhere, since the decapitation of the terrorist leadership reduced its ability to plan and carry out acts of terrorism. In effect, drone attacks terrorized the terrorists, forcing them to change their activities so as not expose themselves needlessly to strikes. Moreover, data indicate that drone strikes seemed to reduce terrorist activity not only in their safe havens but in their immediate neighbourhoods as well.[80] It was thus hardly surprising that Pakistan's military leadership tacitly agreed to the drone campaign in Waziristan early on, a territory which by then was beyond the control of the Pakistani military, even though it resulted in political frictions.[81]

There is thus little doubt that drone strikes aimed at the Taliban Leadership Shura in Quetta would have made an impact on the Taliban movement, had such strikes taken place. However, this particular method of hybrid

---

78 Roggio, Bill/Mayer, Alexander: Charting the Data for US Airstrikes in Pakistan, 2004-2014. <www.longwarjournal.org>.

79 Johnston, Patrick B./Sarbahi, Anoop K.: The Impact of U.S. Drone Strikes on Terrorism in Pakistan and Afghanistan. Paper, RAND Corporation and Stanford University 11 February 2014.

80 Ibid., p. 25.

81 See, e.g. Reuters, 20.05.2011, based on a U.S. diplomatic cable from 11.02.2008 exposed by WikiLeaks detailing discussions between Pakistan's chief of army staff General Ashfaq Kayani and Admiral William J. Fallon, then commander of U.S. Central Command.

warfare was not used by the United States against the Taliban leaders, nor did the latter respond with terrorist attacks overseas. A hybrid threat, drone warfare, was accordingly successfully used to counter another hybrid threat, that of international terrorism.

5.3 Projektion von Soft Power über soziale Netzwerke in hybriden Konflikten

Martin Staudinger

Im März 2014 und den darauf folgenden Monaten erhielten westeuropäische Journalisten, die über den Umsturz in der Ukraine und die unmittelbar darauf folgende Annexion der Halbinsel Krim durch die Russische Föderation berichteten, ungewöhnlich heftige und zahlreiche Reaktionen: Nicht nur in Mails und Briefen, auch in Postings auf den Websites und Facebook-Accounts der Medienunternehmen sowie über andere Kanäle im Internet äußerten sich Leserinnen und Leser zur Darstellung der Ereignisse – sehr viele davon mit scharfer Kritik, Unverständnis und auch persönlichen Angriffen.

„Was bei uns gerade im Streit um Russland und die Krim passiert, habe ich in dreißig Jahren Debattenerfahrung noch nicht erlebt", schrieb Bernd Ulrich, Ressortleiter Politik der deutschen Wochenzeitung „Die Zeit" am 10. April 2014:

> „Wenn die Umfragen nicht täuschen, dann stehen zurzeit zwei Drittel der Bürger, Wähler, Leser gegen vier Fünftel der politischen Klasse, also gegen die Regierung, gegen die überwältigende Mehrheit des Parlaments und gegen die meisten Zeitungen und Sender. Aber was heißt stehen? Viele laufen geradezu Sturm." [1]

Der Versuch, dieses Phänomen zu verstehen und zu erklären, provozierte seinerseits wieder fast 750, teils wütende, Kommentare.

Ein Teil der Reaktionen, die nicht nur Ulrich verblüfften, dürfte genuiner Ausdruck eines auch in Europa weit verbreiteten Sentiments gewesen sein und wurde auch als solcher wahrgenommen. Nachträglich deutet aber viel darauf hin, dass ein beträchtlicher weiterer Teil der Reaktionen auf die Berichterstattung gesteuert war.

---

[1] Wie Putin spaltet. In: Die Zeit Online, 10.04.2014. <http://www.zeit.de/2014/16/russlanddebatte-krimkrise-putin>, abgerufen am 17.06.2015.

Die „Süddeutsche Zeitung“ sprach in ihrer Internet-Ausgabe von „Scharen bezahlter Manipulatoren“, die angewiesen seien,

> „die Meinung in den Kommentar-Bereichen großer Nachrichtenportale zu dominieren, Debatten in Sozialen Netzwerken zu stören und Communitys der Gegenseite zu zersetzen. Im Schutz der Anonymität sind sie von gewöhnlichen Diskutanten und einfachen Provokateuren - sogenannten Trollen - kaum zu unterscheiden.“[2]

Für die Annahme, dass viele Meinungsäußerungen zur Ukraine-Krise von Propagandisten stammen, gibt es nicht nur Indizien – etwa, dass sich laut Umfragen des Allensbach-Instituts zu diesem Zeitpunkt lediglich acht Prozent der Deutschen dazu bekannten, eine „gute Meinung von (Russlands Präsident Wladimir, Anm.) Putin“ zu haben und 70 Prozent kein Verständnis für den russischen Präsidenten zeigten; sie wird auch durch Rechercheergebnisse unabhängiger Medien untermauert. So hatte die oppositionelle russische Zeitung „Nowaja Gaseta“ bereits 2012 über die „Agentur zur Analyse des Internets“ berichtet, ein Unternehmen im Petersburger Vorort Olgino, in dem zuletzt bis zu 600 Mitarbeiter damit beschäftigt seien, „Meinungen im Internet im Sinne des Kreml zu manipulieren“. Im Zusammenhang mit der Ukraine-Krise wurde diese Information gegenüber der „Süddeutschen Zeitung“ von einem leitenden Mitarbeiter des Unternehmens bestätigt [3]

> „Ein Geschäftsführer der ‚Agentur zur Analyse des Internets’ hat sich unterdessen für die Flucht nach vorn entschieden. Am Telefon bestätigte Michail Burtschik der Süddeutschen Zeitung die Authentizität des Materials, wollte sich aber nicht weiter zur Tätigkeit der Agentur äußern. In seinem Blog nennt Burtschik sich nun den ‚geschäftsführenden Troll’ und erklärt, es sei doch gar nichts dabei an der Tätigkeit, Journalisten würden schließlich auch fürs Schreiben bezahlt. Einige seien als Patrioten sogar stolz darauf, ‚Trolle von Olgino’ genannt zu werden: ‚Lieber Troll sein und seine Heimat lieben, als anonym auf die Regierung schimpfen’, schreibt Burtschik [...]“[4]

---

2 Putins Trolle. In: Süddeutsche Zeitung Online, 13.06.2014. <http://www.sueddeutsche.de/politik/propaganda-aus-russland-putins-trolle-1.1997470>, abgerufen am 17.06.2015.

3 Ebd.

4 Ebd.

Umgekehrt versorgte das im Kiewer Hotel Ukraina etablierte Ukrainian Crisis Media Center Medien und Öffentlichkeit auch über Soziale Netzwerke wie Facebook und Twitter rund um die Uhr mit der ukrainischen Perspektive der Krise.[5]

Die Entstehung der Sozialen Netzwerke im Internet und ihre zunehmende Nutzung durch weite Teile der Bevölkerung hat auch den Einsatz einiger Aspekte von Soft Power in Konflikten maßgeblich verändert.

Dem trug General Valery Gerasimow, Generalstabschef der Russischen Föderation laut einem Bericht der „Huffington Post" in einem am 27. Februar 2013 in der russischen Publikation „Militärisch-industrieller Kurier" veröffentlichten Artikel Rechnung. Darin heißt es u.a.:

> „Das Internet eröffnet zahlreiche, asymmetrische Möglichkeiten, die Kampfkraft des Feindes zu schwächen. In Nordafrika konnten wir den Einsatz von Technologien zur Beeinflussung staatlicher Strukturen und der Bevölkerung mit Hilfe von Informationsnetzwerken beobachten. Es ist notwendig, die Aktivitäten im Netz einschließlich der Verteidigung unserer eigenen Objekte zu perfektionieren."[6]

Offensivakteure der Staats-, Volks- und Terrorgewalt bedienen sich gleichermaßen Sozialer Netzwerken wie Facebook, Twitter, Instagram oder YouTube, teilweise mit denselben oder ähnlichen Zielen. Diese können etwa darin bestehen, sich Interpretationshoheit zu sichern, Imagepflege zu betreiben, bereits vorhandene Anhänger zu motivieren oder neue zu rekrutieren, aber auch Gegner einzuschüchtern.

All das zählte schon bisher zum Aufgabenrepertoire von Propaganda. Dennoch ist ein Paradigmenwechsel zu konstatieren.

Zunächst macht es das Internet möglich, mit vergleichsweise geringem Aufwand und in kurzer Zeit eine große Zahl von Rezipienten zu erreichen. Mit Stand

---

5 Eigenwahrnehmung des Autors.

6 Russischer Top-General enthüllt Putins PLäne für die Ukraine. In: The Huffington Post, 03.09.2014. <http://www.huffingtonpost.de/2014/09/03/russischer-general-plaene-putin-ukraine_n_5759124.html?ncid=fcbklnkushpmg00000071>, abgerufen am 17.06.2015;
Originalquelle: <http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf>.

Ende 2013 gab es weltweit mehr als 2,8 Milliarden Internet-Nutzer. [7] Nach Angaben des auf die Hochtechnologie-Branche spezialisierten Meinungsforschungsinstituts Bitkom Research aus dem Oktober 2013 sind zwei Drittel von ihnen – also über 1,8 Milliarden – auch in Sozialen Netzwerken aktiv.[8]

Erhebungen des U.S.-Softwareunternehmens Adobe zufolge existierten Anfang 2014 bei den 21 weltweit größten Netzwerken insgesamt 5,7 Milliarden Nutzerprofile.[9] Statistisch gesehen ist also jeder Internet-Nutzer durchschnittlich in drei Netzwerken aktiv. Das ergibt einen beträchtlichen Resonanzraum.

Der eigentliche Paradigmenwechsel besteht jedoch in der Möglichkeit zur Individualisierung von Einflussnahme bei gleichzeitiger Maximierung von Öffentlichkeit und potenzieller Verschleierung der Agenda.

Nach dem Ende des Kalten Krieges war zunächst die zunehmende Einbindung von PR-Agenturen in die mediale Begleitung von Konflikten zu bemerken. Beispiele – ohne Anspruch auf Vollständigkeit – betreffen etwa die U.S.-amerikanische PR-Agentur Hill & Knowlton, die im Vorfeld des Zweiten Golfkrieges die falsche Behauptung in die Welt setzte, irakische Soldaten hätten bei der Invasion in Kuwait Frühgeborene aus den Brutkästen eines Spitals gerissen und dadurch getötet. Hill & Knowlton war von der im Exil befindlichen kuwaitischen Regierung engagiert worden, um eine Rückeroberung des Emirats durch Öffentlichkeitsarbeit zu unterstützen.[10]

---

7 Internet Usage Statistics. The Internet Big Picture. In: Internet World Stats. <http://www.internetworldstats.com/stats.htm>, abgerufen am 17.06.2015.

8 Berg, Achim: Pressekonferenz –Nutzung sozialer Netzwerke in Deutschland. Bitkom, 31.10.2013. <http://www.bitkom.org/files/documents/BITKOM-PK_Studie_Nutzung_Sozialer_Netzwerke_31_10_2013.pdf>, abgerufen am 17.06.2015.

9 Jeremy Waite: Which Social Networks Should You Care About in 2014? 03.01.2014. <https://blogs.adobe.com/digitaleurope/2014/01/03/social-networks-care-2014/?PID=6149999>, abgerufen am 17.06.2015.

10 Deception on Capitol Hill. In: The New York Times Online, 15.01.1992. <http://www.nytimes.com/1992/01/15/opinion/deception-on-capitol-hill.html>, abgerufen am 17.06.2015.

In den Balkan-Kriegen wurden die Agentur Ruder Finn damit beauftragt, die Position Serbiens zu unterminieren.[11]

Und im Georgien-Krieg 2008 „versorgte die in Brüssel angesiedelte PR-Agentur aspect communications, die seit November 2007 für die georgische Regierung tätig ist, die Medien im Minutentakt mit praktischerweise gleich auf Englisch verfassten Aussendungen“[12]

Russlands Interessen wurden währenddessen von Gplus europe, eine Tochter des New Yorker PR-Imperiums Ketchum, vertreten.[13]

Vor der Etablierung Sozialer Netzwerke waren PR-Agenturen wie alle anderen beim Einsatz offensiver Mittel wie Kampagnen (Information und Desinformation), Manipulation, Propaganda und Mobilisierung in hohem Maße auf traditionelle Medien angewiesen, die gleichzeitig wiederum eine Filterfunktion ausübten oder als parteiisch erkennbar waren.

Ein konkretes Beispiel: Leserbriefkampagnen zur Beeinflussung der veröffentlichten Meinung waren relativ einfach als solche zu erkennen. Zudem oblag es der Entscheidung der Redaktionen, Zuschriften zu veröffentlichen oder nicht beziehungsweise das Verhältnis verschiedener Standpunkte zu moderieren. Die Identitäten der Verfasser oder ihre schlichte Existenz ließen sich mit relativ geringen Mitteln überprüfen.

Im Internet ist diese Filterfunktion de facto außer Kraft gesetzt. Soziale Netzwerke erlauben es Internet-Nutzern, Inhalte zunächst mehr oder weniger ohne Einschränkung zu veröffentlichen. Postings auf Facebook können beispielsweise vom Inhaber des jeweiligen Profils nur manuell gelöscht werden. Sofern klassische Medien auf ihren Websites Kommentare zu ihrer Berichterstattung zulas-

---

11 Schmidt, Christian: Kriegs-PR und Propaganda? Zum jüngsten Jugoslawienkrieg. Hausarbeit, Institut für Kommunikations- und Medienwissenschaft, Universität Leipzig 2000.

12 Staudinger, Martin/Szyszkowitz, Tessa: Der Krieg nach dem Sieg. In: profil 37/08, 08.09.2008, S. 68. <http://www.profil.at/home/der-krieg-sieg-218312>, abgerufen am 17.06.2015.

13 Die Strategen der Wortschlacht. In: Süddeutsche Zeitung Online, 17.05.2010. <http://www.sueddeutsche.de/politik/pr-im-kaukasus-konflikt-die-strategen-der-wortschlacht-1.707833>, abgerufen am 17.06.2015.

sen, ist es nur durch den Einsatz von Moderatoren möglich, Inhalte vor Veröffentlichung auszuwählen oder danach wieder zu entfernen – ein Aufwand an Zeit und Kosten, auf den viele Medien zugunsten der Förderung von Traffic zur Generierung von Anzeigenumsatz in der Vergangenheit häufig verzichtet haben.

Das bedeutet gleichzeitig, dass Äußerungen zur Berichterstattung von Medien sofort und in aller Öffentlichkeit möglich sind – ein Umstand, der per se kein Problem darstellen sollte, aber leicht für Kampagnen, Propaganda, Manipulation oder andere offensive Methoden der Ausübung von Soft Power missbraucht werden kann und in jüngster Zeit auch wurde.

Gleichzeitig lassen sich über die Sozialen Netzwerke Adressaten individualisiert ansprechen: Etwa, um sie direkt mit Inhalten zu konfrontieren, aber auch, um sie im Bedarfsfall öffentlich an den Pranger zu stellen. Das kann Journalisten wegen ihrer Berichterstattung ebenso treffen, wie behördliche Funktionsträger oder politisch Verantwortliche.

Auf diese Art und Weise Druck aufzubauen, kann sich nicht nur aufgrund der Maximierung von Öffentlichkeit als wirksam erweisen, sondern auch aufgrund der Perzeption durch die Adressaten. Wer mit einer Vielzahl von ablehnenden, kritischen oder auch denunziatorischen Stellungnahmen konfrontiert ist, die in dem weiter oben angesprochenen Resonanzraum vorgebracht werden, kann leicht den – möglicherweise irrigen – Eindruck gewinnen, sich selbst in einer Minderheitenposition zu befinden oder dazu verleitet werden, die tatsächlichen Mehrheitsverhältnisse in der Öffentlichkeit falsch einzuschätzen. „Die Zeit" fasste vor wenigen Wochen einen weiteren Aspekt folgendermaßen zusammen.

> „Autoritär geführte Staaten [...] haben sich überdies propagandistisch weiterentwickelt. Nicht nur, dass sie ihre eigenen Medien recht effizient steuern, sie beeinflussen mit ihren Fernsehsendern, mit Bloggern und über die Sozialen Medien auch die westliche Öffentlichkeit. Das ist eine eminent wichtige Veränderung, weil die Selbstkritik zum Wesen westlicher Gesellschaften gehört, ja einen großen Teil ihrer Stärke ausmacht. Diese Selbstkritik wird nun von anderswoher bösartig verstärkt, sie bekommt dadurch leicht einen selbstzerstörerischen Zug."[14]

---

[14] Die Welt ist verrückt – und was machen wir? In: Die Zeit Online, 02.09.2014. <http://www.zeit.de/2014/36/krieg-krise-westen-russland-irak/seite-4>, abgerufen am 17.06.2015.

Zudem ist es sehr leicht möglich, eine Agenda zu verbreiten und gleichzeitig zu verschleiern. Akteure sind nicht ohne weiteres als solche erkenntlich. Sie können sich hinter vorgeblich nicht involvierten Identitäten verstecken – der besorgte Bürger z.B.

All das bedingt die Möglichkeit von Rückkoppelungen auf politische Systeme, vor allem wenn sie demokratisch strukturiert und in der Folge empfänglich für die - oft imaginierte - Reaktion des Elektorats sind.

Besonders drastisch zeigt sich das breite Spektrum der Projektion von Soft Power über die neuen Medien aber anhand der Aktivitäten des so genannten „Islamischen Staats" (IS, auf Arabisch „ad-daula al-islāmiyya", bis Mitte Juli 2014 bekannt als „ISIS" – Islamischer Staat im Irak und in (Groß-)Syrien). Die dschihadistisch-salafistische Organisation, deren Ziel die gewaltsame Errichtung eines Kalifats zunächst in Syrien und dem Irak, in der Folge aber auch in Libanon, Israel, Palästina und Jordanien ist, wird u.a. von den USA[15], dem UN-Weltsicherheitsrat[16], Australien[17] und dem Generalbundesanwalt beim Bundesgerichtshof der Bundesrepublik Deutschland[18] als terroristische Vereinigung eingestuft.

Der IS ist in den Sozialen Netzwerken hoch aktiv. So berichtete die „New York Times" am 28. Juni 2014:

> „The extremist group battling the Iraqi government, the Islamic State in Iraq and Syria, may practice a seventh-century version of fundamentalist Islam, but it has demonstrated modern sophistication when it comes to using social media,

---

15 US Department of State, Bureau of Counter Terrrorism: Foreign Terrorist Organizations. <http://www.state.gov/j/ct/rls/other/des/123085.htm>, abgerufen am 17.06.2015.

16 UN Security Council, Security Council voices great concern over reported seizure of oilfields by terrorist groups operating in Syria, Iraq. SC/11495, 28.07.2014. <https://web.archive.org/web/20140819224243/http://www.un.org/News/Press/docs//2014/sc11495.doc.htm>, bgerufen am 17.06.2015.

17 Australian Government, Australian National Security: Listed terrorist organisations. <http://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/default.aspx>, abgerufen am 17.06.2015.

18 Vgl. Bundesministerium des Innern: Verfassungsschutzbericht 2013, S. 192ff, hier vor allem 209ff. <http://www.verfassungsschutz.de/embed/vsbericht-2013.pdf>, abgerufen am 17.06.2015.

> particularly Twitter and other sites like WordPress and Tumblr. On Twitter, ISIS has hijacked World Cup hashtags, flooding unsuspecting soccer fans with its propaganda screeds. It has used Facebook as a death-threat generator; the text-sharing app JustPaste to upload book-length tirades; the app SoundCloud for jihadi music; and YouTube and Twitter for videos to terrify its enemies."[19]
>
> „ISIS, as well as its fighters and supporters, quickly adopted these tools and has been utilizing the latest Internet technologies and social media outlets to maintain massive, sophisticated online media campaigns used to promote jihad, communicate, recruit and intimidate",

wurde Rita Stern, Analystin der SITE Intelligence Group, im oben genannten Artikel zitiert.[20]

Obwohl bislang nur wenige wirklich gesicherte Zahlen vorliegen, deutet vieles darauf hin, dass der „Islamische Staat" bei der Rekrutierung und Einschüchterung mit Hilfe Sozialer Netze durchaus Wirkung erzielt. In Österreich sorgte beispielsweise im Sommer 2014 der Fall eines Dschihadisten mit tunesischen Wurzeln für Aufsehen, der sich über Facebook damit brüstete, an Hinrichtungen durch IS-Milizen beteiligt gewesen zu sein.[21]

Bemerkenswert ist in diesem Zusammenhang der Umstand, dass der IS Gewalttaten wie die Hinrichtung wehrloser Gefangener nicht wie bei den meisten anderen Kriegsparteien üblich verheimlicht, sondern ganz im Gegensatz offensiv propagiert – vermutlich auch, um sich durch die Demonstration besonderer Brutalität für neue Mitkämpfer attraktiv zu machen.

Der zweite mutmaßliche Zweck, die Einschüchterung, zielt nicht nur auf das direkt erreichbare Umfeld des Islamischen Staates ab, sondern auch auf die in-

---

19 Iraq's Sunni Militants Take to Social Media to Advance Their Cause and Intimidate. In: The New York Times Online, 28.06.2014. <http://www.nytimes.com/2014/06/29/world/middleeast/iraqs-sunni-militants-take-to-social-media-to-advance-their-cause-and-intimitdate.html?module=Search&mabReward=relbias%3Ar%2C{%221%22%3A%22RI%3A7%22}&_r=0>, abgerufen am 17.06.2015.

20 Ebd.

21 Dschihadist aus Wien mutmaßlich an Gräueltaten in Syrien beteiligt. In: profil Online, 26.08.2014. <http://www.profil.at/articles/1435/982/377621/dschihadist-wien-graeueltaten-syrien>, abgerufen am 17.06.2015.

ternationale Gemeinschaft. Den Regierungen, Behörden und der Bevölkerung anderer Staaten kann damit beispielweise suggeriert werden, dass der IS bereits jetzt über eine große Anhängerschaft im Ausland verfügt – was seine Attraktivität bei potenziellen Gefolgsleuten möglicherweise neuerlich zu steigern imstande ist.

Wieder sind es die Sozialen Netzwerke, über die Fotos, Videos, Audiodateien und andere Informationen rasch und direkt an einen großen Empfängerkreis herangetragen werden können.

Zusammenfassung

Dem Einsatz offensiver Mittel wie Kampagnen (Information und Desinformation), Manipulation, Propaganda und Mobilisierung in hybriden Konflikten stehen durch die Etablierung der Sozialen Netzwerke neue, äußerst wirkungsvolle Distributionskanäle zur Verfügung, in denen der Informationsfluss kaum zu kontrollieren, filtern oder gar verhindern lässt.

Daraus – und aus dem Umstand, dass es in den Sozialen Netzwerken möglich ist, gleichzeitig eine Agenda zu verschleiern und ihre öffentliche Wirkung zu maximieren – ergeben sich mannigfaltige Möglichkeiten der Einflussnahme auf die Bevölkerung, die Medien und somit indirekt oder direkt auf politisch Verantwortliche, die sich im Einzelfall möglicherweise schwer erkennen und bekämpfen lässt.

5.4 Abkürzungsverzeichnis

ACT	Allied Command Transformation
AG	Aktiengesellschaft
AIVD	(Dutch) General Intelligence and Security Service
ANA	Afghan National Army
ANP	Afghan National Police
ANSF	Afghan National Security Forces
AP	Associated Press
APCIP	Austrian Program for Critical Infrastructure Protection
ATTA	Afghan Transit Trade Agreement
AUV	autonomous underwater vehicles
BABS	Bundesamt für Bevölkerungsschutz
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BiH	Bosnien-Herzegowina
BMLVS	(Österreichisches) Bundesministerium für Landesverteidigung und Sport
BND	Bundesnachrichtendienst
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection

CPNI	(Dutch) Centre for Ptotection of National Infrastructure
CSCE	(American) Commission on Security and Cooperation in Europe
	Swedish Certification Body for IT-Security
CSIRT	(Dutch) Computer Security Incident Response Team
DDoS	distributed denial-of-service
DefCERT	(Dutch) Defence Computer Emergency Response Team
DG TREN	(European) Directorate-General for Transport and Energy
DNV	Det Norske Veritas
DO(o)D	Department of Defense
EBRD	European Bank for Reconstruction and Development
EC	Electronic Cash
EIA	environmental impact assessment
EMV	(Schwedische) Aufsichtsbehörde hinsichtlich der elektromagnetischen Verträglichkeit
ENISA	European Union Agency for Network and Information Security
EPCIP	European Program for Critical Infrastructure Protection
ERM	Environmental Resources Management
ESS	Europäische Sicherheitsstrategie
ESVP	Europäische SIcherheits- und Verteidigungspolitik
EU	Europäische Union

EUFOR	European Union Force
EUMM	European Union Monitoring Mission
EUR	Euro
FBI	(U.S.-amerikanisches) Federal Bureau for Investigation
FHS	Swedish National Defence College
FIOD	(Dutch) Fiscal Information and Investigation Service
FMV	Swedish Defence Materiel Administration
FOI	Swedish Defence Research Agency
FRA	Försvarets radioanstalt, schwedischer Nachrichtendienst
GAO	(U.S.) Government Accountability Office
GCHQ	Government Communications Headquarters
GIUK	Greenland-Iceland-United Kingdom
GNINGI	(Russian) State Research Navigation-Hydrographic Institute
GOVCERT	Government Computer Emergency Response Team
GPS	Global Positioning System
GRU	(Russian) Main Intelligence Directorate
HIG	Hezb-e Islami of Gulbuddin Hekmatyar
HIIK	Heidelberger Instituts für Internationale Konfliktforschung
HRW	Human Rights Watch
IB	Internationale Beziehungen
ICTY	Internationale Strafgerichtshof für das ehemalige Jugoslawien

IEA	Internationalen Energieagentur
IED	Improvised Explosive Devices
IFK	Institut für Friedenssscherung und Konfliktmanagment
IGH	Internationaler Gerichtshof
IKKM	internationales Konflikt- und Krisenmanagement
IKT	Informations- und Kommunikationstechnologie
IMU	Islamic Movement of Uzbekistan
IRB	(Dutch) IT Response Board
IS	Islamsicher Staat
ISAF	International Security Assistance Force
ISI	Pakistani Inter-services Intelligence agency
ISIS	ISlamsicher Staat im Irak und (groß-) Syrien
ISS	International Security Strategy
IT	Informations-Technologie
IVL	Swedish Environmental Research Institute
IWF	Internationaler Währungsfond
IWWN	International Watch and Warning Network
KBM	Emergency Management Agency
KBV	(Swedish) Coast Guard
KGB	(Russian) Committee for State Security
LNG	liquefied natural gas
LVAk	(österreischische) Landesverteidigungsakademie
MIVD	(Dutch) Military Intelligence and Security Service

MMT	Marin Mätteknik AB
MNRE	(Russian) Ministry of Natural Resources and Ecology
MSB	(schwedisches) Amt für Bevölkerungsschutz und Bereitschaft
MSD	(schwedische) Militärstrategische Doktrin
MUST	(Swedish) Military Intelligence and Security Service
MVW	Massenvernichtungswaffen
NATO	North Atlantic Treaty Organization
NBV	(Dutch) National Communications Security Agency
NCSC	(Dutch) National Cyber Security Centre
NCT	(Schwedisches) Nationales Zentrum für die Bewertung der Bedrohungslage im Terrorismus
NCTB	(Niederländische) Nationale Koordination für Terrorismusbekämpfung
NDS	(American) National Defense Strategy
NEGP	North European Gas Pipeline
NEGPC	North European Gas Pipeline Company
NEL	Norddeutsche Erdgas-Leitung
NG(R)O	Nicht-Regierungsorganisation
NORDEFCO	Nordic Defense Cooperation
NSA	National Security Agency
NSIT	Nationale Zusammenarbeit gegen schwere IT-Sicherheitsbedrohungen
NTSG	(Swedish) National Telecommunications Coordination Group

OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OK	organisierte Kriminalität
OPAL	Ostsee-Pipeline-Anbindungs-Leitung
OPTA	(Niderländische) Unabhängige Post- und Telekommunikationsautorität
OSC(Z)E	Organization for Security and Cooperation in Europe
OSSR	Ozbrojené sily Slovenskej republiky“
PR	Public Relations
PRT	(Canadian) Provincial Reconstruction Team
PTS	(Swedish) Post and Telecom Agency
RAF	Rote Armee Fraktion
RKP	(Swedish) Criminal Investigation Service
SAMFI	(Schwedische) Kooperationsgruppe für Informationssicherheit
Säpo	Swedish Security Service
SAS	Special Air Service
SASIB	Slovak Association for Information Security
SCADA	Supervisory Control and Data Acquisition
SEK	Schwedische Kronen
SGU	Geological Survey of Sweden
SIOD	(Dutch) Social Information and Investigation Service
SKI	Schutz Kritischer Infrastrukturen
SMS	Short Message Service
SOFÄ	(schwedishes) Kooperationsprojekt gegen gefährliche Stoffe

SOSUS	Sound Surveillance System
SR	Slowakische Republik
SRV	(Swedish) Rescue Services Agency
SSG	(Pakistani) Special Services Group
SST	state-sponsored terrorism
TEN	Trans-European Network
TTP	Tehrik-e-Taliban Pakistan, "Movement of Pakistani Taliban"
UAV	unmanned aerial vehicles
UdSSR	Union der Sozialistischen Sowjetrepubliken
UK	Vereinigtes Königreich von Großbritannien und Nordirland
ULV	Umfassenden Landesverteidigung
UN(O)	Vereinte Nationen
UNFICYP	Friedenstruppe der Vereinten Nationen in Zypern
UNTSO	United Nations Truce Supervision Organization
USA	Vereinigte Staaten von Amerika
USD	(amerikanischer) Dollar
USV	Umfassenden Sicherheitsvorsorge
VBIED	vehicle borne improvised explosive devices
VUCA	volatil, unsicher, komplex und ambivalent
WGA	Whole-of-Government-Approach
WHO	World Health Organization
WTO	World Trade Organization
ÖBH	Österreichisches Bundesheer
ÖSS	Österreichische Sicherheitsstrategie

5.5 Abbildungsverzeichnis

5.6 Tabellenverzeichnis

5.7 Autorenangaben

In alphabetischer Reihenfolge

Mag. Dr. **Rastislav BÁCHORA**, eMA, geboren 1978. Doktorat in Politikwissenschaft an der Universität Wien, postgraduales Studium an der Fakultät für Politikwissenschaften an der Universität Belgrad, seit 2010 Lehre am Institut für Europäische Studien und Internationale Beziehungen an der UNI Bratislava.

Mag. Dr. Gerald **BRETTNER-MESSLER** geboren 1969, Studium der Geschichte und einer Fächerkombination (Zeitgeschichte, Rechtsgeschichte, Osteuropäische Geschichte, Politikwissenschaft) an der Universität, seit 2003 Hauptlehroffizier und Forscher an der Landesverteidigungsakademie.

Mag.iur. **Christoph R. CEDE**, geboren 1992, Studium der Rechtswissenschaften an der Karl-Franzens Universität Graz. Derzeit weiterführendes Studium in Intelligence and Strategic Studies an der Universität Aberystwyth. Im Sommer 2014 und 2015 war er als Gastforscher am IFK tätig.

ObstdhmfD Mag. **Anton DENGG** ist seit 2004 am IFK. Studium der Politikwissenschaft an der Universität Wien. Verschiedene Vortragstätigkeiten zu den Themen Terrorismus und Terrorismusbekämpfung sowie Bedrohungs- und Konfliktbild. Mitglied in der Combating Terrorismus Working Group (CTWG) des PfP-Konsortiums. Von 2011-2013 Verwendung als Adviser on Anti-Terrorism Issues bei der Action Against Terrorism Unit (ATU) im Transnational Threat Department (TNTD) der Organization for Security and Co-operation in Europe (OSCE). Seit März 2013 wiederum Leiter des Referats Konflikt- und Bedrohungsbild am IFK.

Prof. Dr. **Michael FREDHOLM** is an historian and defence analyst who has written extensively on the history, defence strategies, security policies, and energy sector developments of Eurasia. He is currently affiliated to the Stockholm International Program for Central Asian Studies (SIPCAS), which originated at Stockholm University and since 2012 is based at the Swedish Research Institute in Istanbul. At SIPCAS, he has made a special study of Central Asian geopolitics, Afghanistan, Islamic extremism, and the causes of and defence strategies against terrorism. He has worked as an

independent academic advisor to governmental, inter-governmental, and non-governmental bodies for more than two decades, including on Foreign Ministry official reports on Eastern Europe, Russia, Central Asia, and failing states. Educated at Uppsala, Stockholm, and Lund Universities, Michael Fredholm taught at Stockholm University (South and Central Asia Programme), Uppsala University (Orientalist Programme), the Swedish Royal Military Academy and Defence Academy (various courses), and a special educational and advisory programme on East Asia for the Commander-in-Chief. He also lectured, during conferences or as visiting professor, at numerous institutions and universities in cities around the world including Ankara, Bishkek, Istanbul, Kolkata, Krynica, Madrid, New Delhi, Oslo, Shanghai, Srinagar, Stockholm, Tashkent, Tsukuba, and Vilnius.

Miliz MjrdhmtD Dipl.-Ing. **Alfred GULDER**, MBA, geboren 1967, ist als stellvertretender Leiter für Flugsicherung in der nationalen Aufsichtsbehörde / Oberste Zivilluftfahrtbehörde im Bundesministerium für Verkehr, Innovation und Technologie (bmvit) tätig. Er absolvierte ein Studium der Nachrichtentechnik auf der TU Wien und den Master of Business Administration und war in zivilen und militärischen Industrien und der österreichischen Flugsicherung beruflich tätig.

Mag. **Ramy JOUSSEF** ist seit April 2013 wissenschaftlicher Mitarbeiter der im Rahmen der Exzellenzinitiative der deutschen Bundesregierung geförderten Bielefeld Graduate School in History and Sociology (BGHS), sowie Mitglied des Instituts für Weltgesellschaft an der Universität Bielefeld. Zuvor studierte er Politikwissenschaft an der Universität Wien, war 2011 Volontär am Institut für Friedenssicherung und Konfliktmanagement (IFK) der Landesverteidigungsakademie Wien und leistete anschließend einen Auslandseinsatz im Rahmen von KFOR. Zu seinen Forschungsfeldern gehören die Soziologie der politischen Gewalt und der Weltpolitik, sowie soziologische Theorie mit Schwerpunkt auf systemtheoretischer Gesellschaftstheorie. Derzeit promoviert er über Funktion, Ausdifferenzierung und Kommunikation von Diplomatie aus systemtheoretischer Perspektive.

Mag.iur. **Reinmar NINDLER** war Universitätsassistent am Institut für Völkerrecht und Internationale Beziehungen der Universität Graz sowie am Europäischen Trainings- und Forschungszentrum für Menschenrechte

und Demokratie der Universität Graz und ist Fulbright Stipendiat an der Columbia Law School, New York.

Dr. **Thomas PANKRATZ**, geboren 1967 in Linz/OÖ. Politikwissenschafter. Forscher und Hauptlehroffizier im Fachbereich Strategie am Institut für Strategie und Sicherheitspolitik der Landesverteidigungsakademie (Wien).

Herbert SAURUGG, MSc, Major, geboren 1974, war 15 Jahre Berufsoffizier im Bereich Führungsunterstützung sowie IKT-/militärische Sicherheit und ist seit 2012 beurlaubt. Nach der berufsbegleitenden Ausbildung zum Akademischen Sicherheitsexperten für IKT absolvierte er ein Masterstudium an der Hochschule für Management Budapest. Er ist Gründungsmitglied von Cyber Security Austria - Verein zur Förderung der Sicherheit Österreichs Strategischer Infrastruktur sowie Initiator der zivilgesellschaftlichen Initiative "Plötzlich Blackout!" - Vorbereitung auf einen europaweiten Stromausfall. Er beschäftigt sich mit systemischen Betrachtungen rund um die Themen "systemische Risiken, Kritische Infrastrukturen und Krisenmanagement".

Mag.iur. Mag.phil. **Paul SCHLIEFSTEINER**, geboren 1986. Studium der Rechtswissenschaften und der Geschichte an der Karl-Franzens Universität Graz. Mitarbeiter am Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS). Derzeit Teilnahme am Masterprogramm „International Security Studies“ der Universität der Bundeswehr.

Mag.iur. **Michael N. SCHURIAN,** BSc, geboren 1986, war von 2013 bis 2014 als Verwaltungspraktikant und wissenschaftlicher Assistent am IFK tätig. Studium der Rechtswissenschaften und der Internationalen Betriebswirtschaft an der Universität Wien und der Singapore Management University. Laufendes Doktorat der Rechtswissenschaften. Diverse Fortbildungen am Peace Operations Training Institute. Forschungsbereiche: Theorie des gerechten Krieges, Militärethik, Polemologie, Konfliktnachsorge.

Mag. **Martin STAUDINGER**, geboren 1968, leitet das Auslandressort des Nachrichtenmagazins profil, für das er bereits aus Kriegs- und Krisengebieten wie Afghanistan, Kongo (Kinshasa), Mexiko, Libyen, Syrien, Tschad und der Ukraine berichtet hat.

Die Vernetzung von Gesellschaften wird durch technische Errungenschaften immer komplexer. Somit erweitern sich auch Einflussfaktoren auf die Sicherheit von Gesellschaftssystemen.

Spricht man in diesem Zusammenhang in sicherheitspolitischen Fachkreisen von hybrider Kampfführung, gehen die Autoren in diesem Buch einen Schritt weiter und beschäftigen sich mit Optionen der Machtprojektion, die über Kampfhandlungen hinausgehen. Dabei sehen sie hybride Bedrohungen als sicherheitspolitische Herausforderung der Zukunft. Beispiele dazu untermauern den im Buch vorangestellten theoretischen Teil. Mögliche Handlungsoptionen runden diese Publikation ab.

ISBN: 978-3-902944-71-9