

Aufsatz

Philipp S. Krüger*

„Agile Abschreckung“ gegen Bedrohungen aus dem Cyber Raum – Optionen für deutsche Politik

<https://doi.org/10.1515/sirius-2018-2003>

Kurzfassung: Wie kann effektive Deutsche Cyberabschreckung aussehen? Dieser Artikel stellt die ersten Ergebnisse eines neuen Cyberabschreckungsmodells vor, genannt „Agile Cyberabschreckung“, das auf interdisziplinärer Forschung am ISPK basiert. Danach eröffnen Cyber-Operationen einen völlig neuen Weg in der Verteilung von Macht. Grundsätzlich dafür ist der spezielle virtuelle (technologische) Charakter der operativen Domäne „Cyber“. Die beschriebene Agile Cyberabschreckung adressiert die spezifischen Cyber-Verwundbarkeiten einer „Cyber-Mittel-Macht“ wie Deutschland und schlägt vier Abschreckungsoptionen vor.

Schlüsselbegriffe: Abschreckung, Cyberspace, digitale Sicherheit

Abstract: How can an effective cyber deterrence work for Germany? This article introduces preliminary results of a new cyber deterrence model called “Agile Cyber Deterrence” based on interdisciplinary research at ISPK. It outlines a cyber deterrence strategy that (1) realizes that unlike in the terrestrial spaces where strategic effects have required territorial aggression (or the threat thereof), cyber operations have opened a new seam in the distribution of power and can impact relative national power without traditional armed aggression, (2) takes into account the inherently virtual (technological) nature of the operational domain, and (3) addresses the specific cyber vulnerabilities and deterrence options of a cyber middle power such as Germany.

Keywords: deterrence, cyberspace, digital security

1 Einleitung

„Die erhöhte globale Cyber – Gefährdungslage¹ erfordert eine Revision veralteter nationaler Cyber Strategien insbesondere hinsichtlich kontroverser Werkzeuge wie offensiven Cyberoperationen, Hack Backs und Cyber Abschreckung („Cyber Deterrence“). Während andere Nationen derzeit proaktiv neue Teilstrategien formulieren² und der Begriff „Cyber Deterrence“ fest in der strategischen Gesamtarchitektur verankert wird,³ hat Deutschland hier Nachholbedarf. Zwar prüft die Bundesregierung derzeit in Zusammenarbeit mit dem Bundesverfassungsschutz eine Gesetzesinitiative die sich mit Einzelthemen wie Hack Backs beschäftigen soll, ebenso positioniert sich das BMVg mit KdoCIR und ADIC (mehr dazu unten) als progressiver neuer Cyberakteur. Gesamtstrategisch stützt Deutschland sich jedoch auf veraltete Teilkonzepte für Cyberbedrohung und -abwehr.⁴ Zu einem Zeitpunkt, an dem sich digitale Sicherheit mehr und mehr mit persön-

¹ Laut Fitch Ratings betragen 2017 die Beitragszahlungen für US Cyberversicherungen 2.1 Milliarden US\$, 54% mehr als im Vorjahr; zu den Rekordzahlen bei DDoS und erfolgreichen Cyberangriffen: IBM X-Force Threat Intelligence Index 2017 <https://www.ibm.com/security/data-breach/threat-intelligence>

² In seiner neuen Cybersecurity Strategy (2018) spricht das U.S. Department of Homeland Security von einem „historischen Wendepunkt“ und der daraus resultierenden Notwendigkeit einer „umfassenden Cyber Strategie“, <https://www.dhs.gov/publication/dhs-cybersecurity-strategy>; Israel entwickelt seit 2017 aktiv das Konzept der „Cumulative Deterrence“ als neues Cyberabschreckungs-Paradigma, vgl. Tor, 2017.

³ Das United States Cyber Command (USCYBERCOM) hat im März 2018 eine neue Kommandostrategie freigegeben, Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command. Washington, D.C. 2018; <https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf>. Darin wird das „Deterrence“ Konzept auch auf den Cyber Raum angewendet; ebenso: Laut dem neuen Nuclear Posture Review 2018 (NPR 18) des U.S. Department of Defence können neuerdings auch Cyberangriffe strategische Dimensionen annehmen und unter die erweiterte nukleare Abschreckung fallen, https://www.defense.gov/News/Special-Reports/0218_npr/NPR18.

⁴ Vgl. Bundesinnenministerium (2016): Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin; https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf; Bundesverteidi-

*Kontakt: Philipp S. Krüger, Fraunhofer Institut für Sicherheit in der Informationstechnologie (SIT) sowie non-resident Fellow des ISPK; E-Mail: philipp.krueger@sit.fraunhofer.de

licher und physischer Sicherheit überschneidet und an dem nichtstaatliche Akteure über Cyberfähigkeiten verfügen die bisher Nationalstaaten vorbehalten waren, müssen wir über das veraltete Konzept der isolierten kritischen Infrastrukturen hinausdenken und Cybersicherheit als systemisches Risiko konfrontieren, das jeden Akteur, vom Militär über Firmen bis hin zur Privatperson, betrifft. Um dieser neuen ressortübergreifenden Cyber Herausforderung gerecht zu werden, ist neues Denken gefragt. Cyberabwehr und -verteidigung sowie Cybersicherheitsinnen- und -außenpolitik müssen innerhalb eines emergenten gesamtstrategischen Rahmenkonzeptes sinnvoll aufeinander abgestimmt werden um systemische Schocks zu verhindern. Dieser Artikel stellt dazu das neue Modell der „agilen Cyberabschreckung“ vor, welches defensive und offensive Werkzeuge (in-domain und out-domain) kombiniert, um in Zukunft sowohl Cyberrisiken als auch -schäden zu minimieren.

2 Globales Cybersäbelrasseln

Seit Jahren setzt sich John Bolton für eine Verstärkung US-amerikanischer Cyberwaffen ein und dafür, digital zurückzuschlagen. Jetzt, wo Präsident Trump den umstrittenen Botschafter zum nationalen Sicherheitsberater ernannt hat (und nachdem der angesehene Homeland- und Cybersecurity-Berater Tom Bossert seinen Rücktritt erklärt hat), sorgen sich die Experten der digitalen Kriegsführung über die möglichen Implikationen seines zunehmenden Einflusses auf die sowieso schon explosive globale Cybersicherheitsumgebung. „So wie wir dies bei Nuklearwaffen getan haben, sollten wir auch im Cyberspace Abschreckungsstrukturen erschaffen, um künftig zu verhindern, dass wir von russischer oder anderer Seite angegriffen und unsere Interessen bedroht werden“ schrieb er im Februar in einem Gastkommentar in *The Hill*. „Eine Möglichkeit wäre, eine Cyber-Vergeltungsmaßnahme gegen Russland zu führen.“⁵ Und letztes Jahr auf Fox Business: „Amerikanische Experten in Cyberkriegsführung sollten WikiLeaks zum Üben der Treffsicherheit verwenden.“⁶

Aufgrund des geheimen Charakters von Cyberoperationen und der gemischten Ergebnisse,⁷ ganz abgesehen

von Donald Trumps Annäherungsversuchen gegenüber Russland, bleibt es abzuwarten, wie Boltons Aussagen die offizielle US Cyberdoktrin künftig prägen werden. Hinter dieser hauptsächlich politisch motivierten Debatte steckt jedoch ein tiefergehendes Sicherheitsproblem das auch für eine Cyber Mittelmacht wie Deutschland wichtige Konsequenzen hat. Eine höhere globale Cyberunsicherheit⁸ führt derzeit zu „Sicherheitsdilemma“-Dynamiken, wo Maßnahmen eines Akteurs zur Verstärkung der eigenen Sicherheit zu Gegenmaßnahmen seitens anderer Akteure führen, welche wiederum die Schwächung und nicht eine Stärkung des ersten Akteurs zur Konsequenz haben. Sie können auch zu gefährlichen „Nebel des Cyber-Konflikts“ Situationen führen (in Anlehnung an Clausewitz Formel vom Nebel des Krieges) bei denen Unsicherheiten im Situationsbewusstsein und operative Unklarheit aufkommen.

Die Aussagen von Bolton sind insofern irreführend, dass sie Cyberoperationen bzw. Hack Backs eine strategische Wirksamkeit unterstellen, die (bisher) umstritten ist. Außerdem sind sie von einer Logik der Nuklearabschreckung durchdrungen, welche den Realitäten von Cyber Konflikten nicht gerecht wird. Drittens beschäftigen sie sich exklusiv mit (überproportionalen) Offensivmaßnahmen, wohingegen sich erfolgreiche Abschreckung seit jeher auf mindestens zwei Pfeiler stützt: Vereitelung („Denial“) und Kostenauflegung („Cost Imposition). Dabei sollte jedoch nicht übersehen werden, dass sich Boltons Kommentare mit zwei wichtigen Punkten auseinandersetzen: Erstens, dass eine wie auch immer geartete Cyberabschreckungstheorie und -praxis – unter Einbeziehung proportionaler offensiver Cyberoperationen – zweifellos bei zukünftigen Cyber-bezogenen Konflikten eine wichtige Rolle spielen wird.⁹ Und zweitens, dass Boltons Bemerkungen sowie andere wichtige Entwicklungen in der jüngsten Vergangenheit ein neues Kapitel der globa-

gungsministerium (2015): Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg 2015. Berlin.

⁵ John Bolton, 'Russian assault on 'American idea' enables Trump to take tough action', *The Hill*, 19.2.2018.

⁶ John Bolton, Fox Business, 8.3.2017.

⁷ Vergleiche zum geheimen Charakter Poznansky/ Perkoski 2016; auch die Aussagen des damaligen CIA Direktors Mike Pompeo anläss-

lich des Senate Intelligence Committee Hearings zur weltweiten Bedrohungslage im Februar 2018 deuteten darauf hin, dass die USA im Geheimen bereits Vergeltung an Russland wegen der Einmischung in den US Wahlen von 2016 verübt haben (zusätzlich zu den veröffentlichten Maßnahmen). Experten haben diese geheimen Maßnahmen als zu wenig und zu spät kritisiert. Zu den ernüchternden Ergebnissen vgl. Carter 2017, der sagte: I was largely disappointed in Cyber Command's effectiveness against ISIS. It never really produced any effective cyber weapons or techniques. When CYBERCOM did produce something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection."

⁸ Vergleiche: PWC Survey 2018.

⁹ Vergleiche: das Konzept einer breiten, inklusiven Abschreckung als ein sich entwickelnder, integrierter Mix aus Strategien, der sich von der klassischen nuklearen Abschreckung unterscheidet in Valeriano/ Maness 2015

len Cyberabschreckung einleiten: die öffentliche Artikulierung und damit Signalisierung („Signalling“) der staatlichen Fähigkeit zur offensiven Cyberabschreckung sowie die Erkenntnis, dass Cybersicherheit und nationale Macht direkt miteinander verbunden sind.¹⁰

Dieser Artikel stellt die ersten Ergebnisse eines neuen Cyber-Abschreckungsmodells vor, genannt „Agile Cyberabschreckung“, das auf interdisziplinärer Forschung am ISPK basiert. Er umreißt eine Cyberabschreckungsstrategie, die (1) „realisiert, dass entgegen terrestrischen Räumen, wo strategische Effekte territoriale Aggression (oder die Androhung solcher) voraussetzen, Cyber-Einsätze einen völlig neuen Weg in der Verteilung von Macht eröffnen“.¹¹ Er berücksichtigt (2) den grundsätzlich virtuellen (technologischen) Charakter der operativen Domäne, und (3) geht besonders auf die spezifischen Cyber-Verwundbarkeiten und Abschreckungsoptionen einer „Cyber-Mittel-Macht“ wie Deutschland ein. Er definiert (4) Cyber Abschreckung als einen Mix aus defensiven und offensiven Fähigkeiten und Maßnahmen sowohl In-Domain (Cyber) als auch Out-Domain (z.B. wirtschaftliche Sanktionen), (5) nicht mit dem Ziel der (unrealistischen) absoluten Abschreckung, sondern der Schadensminimierung.

3 Die vierte Welle der Abschreckungstheorie

Seit der russischen hybriden Kriegsführung gegen Estland im Jahr 2007 lassen sich eskalierende, cyber-bezogene in-domain und out-domain Angriffe und Gegenangriffe, Signalling und Tit-for Tat Dynamiken beobachten.¹² In den

¹⁰ Vgl. Max Smeets: „The Netherlands just revealed its cybercapacity. So what does that mean?“, *Washington Post*, 8.2.2018. USCYBERCOMs neuer strategischer Ansatz – in Übereinstimmung mit der neuen Nationalen Sicherheitsstrategie (NSS) von 2017 – stellt eine entscheidende neue These zum Cyberspace als Domäne auf: antagonistisches Verhalten, das absichtlich unterhalb der Schwelle von bewaffneter Aggression ansetzt, kann bereits eine strategische Wirkung entfalten.

¹¹ Vgl. Harknett 2018.

¹² Der Shamoon Angriff (inoffiziell Iran zugeordnet) auf Saudi Aramco im August 2012 wird als ein in-domain Gegenangriff als Antwort auf (und Copycat) der Stuxnet, Flame, Duqu und Wiper Angriffe angesehen (inoffiziell den USA und Israel zugeordnet). Die weltweit steigende Zahl an neuen nationalen Cyber-Kommandos mit Teilstreitkraftcharakter (z. B. in den USA und Deutschland) kann als ein Signal für größere Entschlossenheit und Fähigkeiten interpretiert werden. Neue Entwürfe von Doktrinen und deklaratorischer Politik zu Cyberbedrohungen basieren eindeutig auf Abschreckungstheorien. Das US Verteidigungsministerium bringt dementsprechend in seiner *Nuclear Posture Review* vom Februar 2018 erstmals die Anwendung von nuklearen Waffen als Vergeltungsmaßnahme auch gegen

Worten des ehemaligen estnischen Präsidenten Toomas Ilves, „das größte Problem in Cyber bleibt die Abschreckung. Wir reden jetzt seit Jahren in der NATO darüber, dass wir uns damit auseinandersetzen müssen.“¹³ Was notwendig ist, ist keine Cyberkanonenbootpolitik, sondern eine ernsthafte interdisziplinäre Untersuchung der Cybereskationsdynamiken und die darauf aufbauende Entwicklung von innovativen und effektiven Abschreckungsmechanismen (inklusive proportionaler offensiver Maßnahmen), die es einem Land wie Deutschland ermöglicht, Cyberkonflikte besser zu kontrollieren, zu de-eskalieren oder zu beenden. Dies muss zu einem Zeitpunkt erfolgen, an dem sich die rapide beschleunigende Digitalisierung, Konnektivität, und Cyber-Verwundbarkeit zu einem perfekten Sturm an Cyberunsicherheit zusammengebraut haben.

Inzwischen arbeiten Wissenschaftler derzeit weltweit an neuen Modellen, welche traditionale Abschreckungstheorien an die sich schnell entwickelnde Sicherheitsumwelt anpassen sollen. Nach zwei Jahrzehnten der Vernachlässigung seit dem Ende des Kalten Krieges spricht Alex Wilner von einer „Renaissance“ und „vierten Welle“ der Abschreckungstheorie.¹⁴ Zahlreiche Veröffentlichungen und empirische Studien aus der jüngeren Zeit haben ein breites Spektrum an sub-staatlichen und nichtstaatlichen Sicherheitsproblemen wie Terrorismus, Piraterie, und organisierte transnationale Kriminalität untersucht. Seit 2009, insbesondere nach der Veröffentlichung von Martin Libickis *Cyber deterrence and Cyber War*,¹⁵ haben Forscher verstärkt die Anwendbarkeit von Cyber-Abschreckungsmodellen analysiert. Leider werden Cyberkonflikte – die jüngsten und komplexesten dieser „vierte Welle Sicherheitsprobleme“ – immer noch schlecht verstanden, da bisher wenige empirische Daten gesammelt, klassifiziert und analysiert wurden.¹⁶ Neueste Analysen haben diesem wachsenden Feld jedoch frische, über die klassische Theorie der nuklearen Abschreckung hinausgehende Erkenntnisse geliefert.¹⁷ Die agile Cyberabschreckung baut auf diese Forschung auf und ergänzt sie mit empirischen sogenannten „Cyber Threat Intelligence“ Daten, Prinzipien aus der agilen Softwareentwicklung sowie dem datenzentrischen Cybersicherheitsparadigma.

nichtnukleare Bedrohungen ins Spiel, dabei werden auch „Cyberbedrohungen“ erwähnt.

¹³ Zitiert nach David E. Sanger: „As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy“, *New York Times*, 16.6.2016.

¹⁴ Wilner 2015.

¹⁵ Libicki 2009.

¹⁶ Vgl. Lupovici 2011 und Harknett/Callaghan/Kauffman 2010.

¹⁷ Vgl. Tor 2017, Mandel 2017, Nye 2016, Poznansky/Perkoski 2016, Valeriano/Maness 2015, Lin 2012 und Hodges/Creese 2015; siehe auch NATO CCD COE 2017.

3.1 Keine Regeln für den Cyberraum

Während einer Rede an der Lissaboner Universität im Februar hat UN Generalsekretär António Guterres zum globalen Handeln aufgerufen, um die Risiken einer elektronischen Kriegsführung für die Zivilbevölkerung zu minimieren. Guterres warnte, dass „es keine Regulierungsrahmen für diese Art der Kriegsführung gebe“, und dass „es nicht klar ist, wie die Genfer Konvention oder das internationale humanitäre Völkerrecht darauf zutrifft“. Das Versagen der UN Expertengruppe für Regierungsangelegenheiten (United Nations Group of Governmental Experts – UN GGE) sich 2017 auf einen zweiten Bericht zu einigen, betont den Umstand, dass es mit der Ausnahme von einigen wenigen, inhaltlich eng begrenzten und schwachen bilateralen Vereinbarungen,¹⁸ derzeit keine effektiven multilateralen Regeln für den Cyberraum gibt.¹⁹ Es wird sie auch in naher Zukunft nicht geben. USCYBERCOMs neue Kommandostrategie geht noch einen Schritt weiter und behauptet, dass der Status Quo im Cyberspace sich derart verschlechtert, dass strategische Gegner die Normen festlegen. Ein Trend, der nicht nur die westlichen Interessen herausfordert, sondern den gesamten Cyberraum in eine chaotische Zukunft führe.

Tatsache ist, dass die globale Anzahl von Cyberattacken stetig steigt, und die Angriffsvektoren sich kontinuierlich fortentwickeln in einem Medium welches mehr und mehr „User“ als „the Wild Wild West (oder www) of Cyberspace“ bezeichnen.²⁰ Ein Beispiel: 60% der Teilnehmer der letzten BlackHat Cybersicherheitskonferenz in Las Vegas erwarten, dass die USA innerhalb der kommenden zwei Jahre einen erfolgreichen Angriff auf ihre kritischen Infrastrukturen erleiden wird.²¹ Und die Angriffsfläche wird immer größer: Big Data, Machine Learning, autonomes Fahren, IoT erhöhen weiter die Anzahl an potentiellen Angriffszielen.²²

¹⁸ Der ehemalige White House Homeland Security und Cybersecurity Berater Tom Bossert hat erklärt, dass die amerikanische Herangehensweise an Cyber Normen unter der Trump Administration sich von multilateralen auf bilaterale Initiativen verschieben wird. Die Bilanz bilateraler Abkommen der USA war bislang ernüchternd, vgl. das weitgehend wirkungslose Abkommen zwischen den USA und China vom September 2015 hinsichtlich „cyber-enabled theft of intellectual property.“

¹⁹ Nye 2018.

²⁰ Laut dem niederländischen General Intelligence and Security Service (AIVD) bewegen sich traditionelle Bedrohungen wie Spionage, verdeckte politische Beeinflussung, Terrorismus und Sabotage immer weiter in die digitale Domäne, vgl. AIVD 2017.

²¹ Blackhat 2017.

²² Laut Chris Doran von ARM Holdings, der Firma welche die Chips in fast allen Smartphones auf dem Planeten design hat, könnte die

Sputnik-Momente²³ wie die oben erwähnten Hybridkampagnen gegen Estland (2007) und Georgien (2008), die kritische Infrastruktur APT Stuxnet (zuerst 2010 entdeckt), die Edward Snowden Leaks (2013), und die jüngeren Cyber-Infowar-Operationen gegen die US (2016) und französischen (2017) Präsidentschaftswahlen sowie der WannaCry Ransomwareangriff (2017) und die zerstörerische NotPetya Malware (gefälschte Ransomware) Kampagne²⁴ unterstreichen drei Faktoren, die diese sich rasant entwickelnde Cybersicherheitsumgebung besonders komplex und instabil machen:

1. Der Cyberspace erlebt einen beschleunigten Prozess der Politisierung, Nationalisierung, Kriminalisierung, Militarisierung und Automatisierung.
2. Ein „Levelling“ des Cyber Playing Fields (sogenannte „Peer Competition“) zwischen etablierten Cyberakteuren wie den „Echelon“ oder „Five Eyes“ Nationen (US, VK, Kanada, Australien, Neuseeland) und deren Partnern sowie ambitionierten Nachzüglern (sogenannte „second movers“) wie den 4 + 1 (China, Russland, Iran, Nordkorea, plus transnationaler, gewalttätiger Extremismus wie ISIS).²⁵
3. Nichtstaatliche Cyberakteure verfügen über Cyberfähigkeiten die zuvor ausschließlich Nationalstaaten vorbehalten waren.²⁶

Zahl von Geräten die online sind (und damit von Internet-Verbindungen) bis 2035 auf eine Billion steigen, vgl. Jamie Condliffe: How to get one Trillion Devices Online, Technology Review vom 20.9.2017; <https://www.technologyreview.com/s/608878/how-to-get-one-trillion-devices-online/>.

²³ In Referenz zum Launch des ersten künstlichen Satelliten Sputnik 1 im Jahr 1957 durch die UdSSR. Der Launch überraschte die USA und führte zur Erschaffung von ARPA (später DARPA) und gab den Startschuß für das sogenannte „Space Race“.

²⁴ Zu Stuxnet vgl. Farwell/Rohozinski 2011; Dunn Caveltly 2011, Porche/Sollinger/McKay 2011, Falliere/Murchu/Chien 2011. Im Februar 2018 beschuldigte das White House öffentlich Russland für die Verbreitung von NotPetya and nannte die Malware „the most destructive and costly cyberattack in history. It inflicted serious damage on the Ukrainian government and later caused billions in damage for corporations such as U.S. pharmaceutical company Merck Sharp & Dohme, Danish shipping firm Maersk and FedEx subsidiary TNT“; vgl. <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/>.

²⁵ Während einer Diskussion im Februar 2017 am Brookings Institute beschrieb der Chairman of the US Joint Chiefs of Staff, General Joseph Dunford, das „4 + 1 framework“ als prioritär.

²⁶ „Laut der neuen U.S. Department of Homeland Security Cybersecurity Strategy (2018) „wird die Trennlinie zwischen staatlichen und nicht-staatlichen Cyber Aktivitäten unscharf“.

3.2 Deutschlands spezifische Cyber-Verwundbarkeit

Diese Entwicklung hat weitreichende Konsequenzen nicht nur für die USA als (ehemalige) alleinige Cybersupermacht, sondern auch für Cyber-Mittelmächte wie Deutschland. Der Deutsche Bundestag, das deutsche Außenministerium, die Bundeswehr, ein Stahlwerk, die meisten Dax gelisteten Unternehmen wie z. B. Siemens, Daimler oder Telekom, sie alle waren das Ziel erfolgreicher, zunehmend komplexer Cyberangriffe. Einige Experten behaupten, dass es im Schnitt täglich 6.500 Angriffe allein auf Netzwerke der deutschen Regierung gebe. Die Angriffsoberfläche ist riesig und dehnt sich weiter aus (die Bundeswehr z. B. beschäftigt ca. 280.000 Personen und damit IT-Benutzer, mit über 55.000 SAP Nutzern).²⁷ Deutschlands traditionell exportorientierte und industrielle Wertentstehungsketten sowie der relativ starke soziale „Kitt“ bzw. Zusammenhalt ist zunehmend abhängig von einem funktionierenden und vertrauenswürdigen globalen digitalen Rückgrat, dem sogenannten „digital Backbone“ (Chips, Servern, „Machine Scaled Computing“, Lichtfaserkabeln, Routern) und dem digitalen Nervensystem – „digital Nervous System“ (Sensoren, IoT, Soziale Plattformen, Datensammlung, -verarbeitung, und -analyse, maschinelles Lernen, „Human Scaled Computing“).²⁸ Diese grundsätzliche Cyber-Verletzbarkeit wird noch weiter verstärkt durch die extreme deutsche (und europäische) Abhängigkeit von fremder Software und Hardware. Es gibt derzeit außer SAP nur wenige deutsche Digitalfirmen von internationalem Rang.

Der deutsche Technologie-Venture Capital Investor Klaus Hommels (Facebook, King.com, Skype und Spotify) bezeichnet dies als einen Mangel an „Plattformkompetenz“.²⁹ Andere bezeichnen es als den deutschen bzw. europäischen Mangel an einem „digital-industriellen“ Komplex. Zusätzlich problematisch ist die Tatsache, dass in der digitalen Wirtschaft eine derartige mangelhafte Ausgangssituation sich verstetigen kann: mangelnde digitale „Plattformkompetenz“ führt oftmals zu mangelhafter „Cross-Plattformkompetenz“, d. h. die Fähigkeit, neue digitale Produkte, Dienstleistungen und Geschäftsmodelle zu kreieren, die auf bestehenden Plattformen und dem dazugehörigen Know-How aufbauen. Die US „Unicorns“ Uber und AirBnB bauen z. B. auf bereits existierende Geo-

location-Systeme, sozialen Netzwerken, Matchmaking und Datenanalyseplattformen auf, die in den USA entwickelt wurden.

Die Antwort der deutschen Wirtschaft auf die raue Wirklichkeit dieser spezifisch deutschen Cyber-Verwundbarkeit besteht aus einem Mix an Regulierungen, stark geförderten staatlichen FuE-Aktivitäten und cybersicherheitsbezogenen Investitionen der deutschen Privatwirtschaft im Ausland. Die Antwort der deutschen Sicherheitsaußen- und -innenpolitik ist ein Gemenge aus Verschlüsselung, hoher Abhängigkeit bei nachrichtendienstlichen Cyber-Erkenntnissen, z. B. von den Five-Eyes Ländern, hohe Abhängigkeit von ausländischen militärischen Cyberoperationskomponenten (Hardware und Software) und verschiedenen, vom Auswärtigen Amt getriebenen diplomatischen Cyber-Initiativen, die bisher aber ohne wesentlichen bilateralen oder multilateralen Erfolg geblieben sind. Wenig überraschend hat dies dazu geführt, dass deutsche Beiträge zur Cyberabschreckungsforschung bisher kaum zu finden sind.

4 Abschreckungsmissverständnisse aus den Zeiten des Kalten Kriegs

Abschreckung bedeutet, jemanden von etwas abzubringen, indem man ihn glauben lässt, dass die Kosten seines Handelns den zu erwartenden Gewinn übersteigen. Cyberabschreckung unterscheidet sich von dem damit verwandten und manchmal sich überschneidenden Bereich der Cyberabwehr: Cyberabschreckung beschäftigt sich hauptsächlich mit der Manipulation des Verhaltens des Gegners; Cyberabwehr soll dagegen eher die Auswirkungen eines Angriffs abschwächen als die Entscheidung des Gegners beeinflussen, einen Angriff überhaupt zu starten.

In Erinnerung an den Kalten Krieg befürchtet die deutsche Führungselite (und die anderer Nationen), dass der Einsatz von nationalen Cyberabschreckungsmechanismen zu einer Situation führen könnte, in der Deutschland in eine schwer vorhersagbare und unkontrollierbare Eskalationsleiter einsteigt und so möglicherweise an relativer Macht in den aktuellen Ost-West Cyberkonfrontationen verliert. Entsprechend denkt man darüber nach, wie man der schwierigen cyberstrategischen Position Deutschlands am besten gerecht wird und sich an den Erfahrungen des Ost-West-Konflikts orientiert.

Seit den späten 1950ern profitiert Deutschland von der sogenannten „erweiterten Nuklearabschreckung“

²⁷ Vgl. Bundesamt für Sicherheit in der Informationstechnik 2017 und Bundesregierung 2016.

²⁸ Vgl. Krüger 2016.

²⁹ Vgl. „Wir haben ein gigantisches digitales Handelsdefizit“, Interview mit Klaus Hommels in Tagesspiegel vom 11.12.2017.

seitens der USA. Die nukleare Abschreckungsdoktrin der NATO beruhte auf dem Grundsatz, mittels der nuklearen Potenziale einen konventionellen Angriff abzuschrecken. Falls das nicht gelingt, sollte im Wege "vorbedachter Eskalation" die Abschreckungswirkung der Nuklearwaffen wieder hergestellt und der Gegner zur Preisgabe seines konventionellen Angriffsziels bewogen werden.³⁰ Heute, im Angesicht der neu entstehenden vierten Welle von Abschreckungstheorien, tendieren deutsche Führungsspitzen dazu, auf Cyberstrategie und -abschreckung eine ähnliche Denkweise anzuwenden wie auf die erweiterte Nuklearabschreckung im Kalten Krieg: Über Abschreckung im nationalen Rahmen nachzudenken schwächt unsere Position.

Diese Denkweise ignoriert die Tatsache, dass Vorstellungen von Abschreckung aus den Zeiten des Kalten Krieges, nämlich das Drohen mit nuklearen Vergeltungsschlägen als Reaktion auf einen konventionellen Angriff, nicht zur Realität eines Cyberkonflikts passen. Wie Joseph S. Nye Jr. beobachtet: „Nuklearabschreckung ist irreführend, weil unser Ziel (bisher auch erreicht) eine komplette Prävention war, wohingegen viele Aspekte von Cyberverhalten eher denen von kriminellen Verhalten oder Störungskampagnen entsprechen, die wir versuchen, teilweise, zu verhindern.“³¹ Die spezielle Natur der Cyberbedrohung führt also zur Notwendigkeit, eine spezifische Abschreckungsstrategie für Cyberkonfliktsituationen zu entwickeln. Eine solche Strategie sollte nicht auf "absolute Verhinderung" abzielen, sondern auf Schadensminimierung.

In Anbetracht dieses wesentlichen Unterschieds, der deutschlandspezifischen Cybervulnerabilität sowie der eskalierenden Natur der aktuellen Cyberkonflikte (und der daraus resultierenden Schäden an der deutschen wie auch anderer EU Volkswirtschaften und Gesellschaften) scheint es unrealistisch, sich wieder auf Konzepte aus der Zeit des Kalten Krieges in gewohnter Passivität zu verlassen.

Dieses konzeptuelle Abschreckungsmissverständnis („Cold War Deterrence Bias“) wird noch dadurch verschärft, dass die wenigen Stimmen zu deutscher Cyberabschreckung (und Cyberabschreckung überhaupt) bislang überwiegend aus dem politikwissenschaftlichen Umfeld kommen. Die Computerwissenschafts-Community, insbesondere die Cybersicherheits-Community, hat sich bisher zum größten Teil aus der Debatte herausge-

halten. Um jedoch mit realistischen Modellen aufwarten zu können, ist interdisziplinäres empirisches und analytisches Arbeiten erforderlich, ähnlich den in den 60ern interdisziplinär an Abschreckung arbeitenden Forschungsteams rund um Thomas Schelling. Das Projekt ‚Agile Cyberabschreckung‘ begründet seine Arbeit daher sowohl auf internationale Sicherheitspolitik als auch auf Computerwissenschaften.

In der Praxis führt der oben beschriebene „Bias“ zu einem gefährlichen Ungleichgewicht zwischen aktuellen, praktischen Cyberinitiativen und einem Mangel an Cyberstrategie. 2017 z. B. startete die Bundeswehr KdoCIR (das Kommando Cyber- und Informationsraum), eine neue militärische Teilstreitmacht für die Cyberdomäne. Jedoch hat das BMVg weder eine umfassende cyberstrategische Vision entwickelt noch einen Prozess angekurbelt, der zu einem solchen Rahmenwerk führen könnte.³² In gleicher Weise skizzieren das sogenannte *Bühler-Papier*³³ und das *Framework Nation Concept* (FNC)³⁴ eine neue, ambitionierte und ungewohnte politisch-militärische Führungsrolle für Deutschland, sie sprechen Cyberstrategie und – Abschreckung aber nur am Rande an.

Dieses Ungleichgewicht zwischen Strategie und Implementierung spiegelt sich in der Verteilung der Cyberabschreckungs- und strategierollen im Kanzleramt wieder, sowie der inter-ministerialen Cyber-Rollenverteilung zwischen BMI bzw. BSI, BMVg, AA sowie BND, BfV und Bundespolizei (nicht zu vergessen neue Cyberrelevante Projekte wie ZITIS, CODE und ADIC). Bis heute wird Cyberabschreckung in Deutschland nicht ausreichend auf interministerialer Ebene koordiniert. Ganz zu schweigen von EU-weiter Koordination. Das „Default Setting“ war und ist ein Verweis auf die NATO.

Angesichts Donald Trump's „America First“ Politik auch gegenüber dem transatlantischen Bündnis, angesichts der Tatsache, dass es zwar zahlreiche NATO Konferenzen und Papiere zum Thema gibt aber noch keine ernst zu nehmenden militärischen Pläne (abgesehen von der Abschirmung von NATO Netzwerken), und angesichts der

³⁰ Deutschland ist Teil des Entscheidungsprozesses beim Einsatz nuklearer Kräfte im europäischen Raum: Athener Guidelines von 1962 und Richtlinien der Nuklearen Planungsgruppe für den Erst- und den Folgeinsatz nuklearer Kampfmittel.

³¹ Nye 2016.

³² Zum Beispiel die Gründung einer interdisziplinär arbeitenden Expertengruppe mit dem Mandat der Verfassung eines internen sogenannten „Non-Papers“, ähnlich der DoD – RAND – Harvard Zusammenarbeit der 1960er Jahre.

³³ Da es ein neues „Konzept der Bundeswehr“ nicht gibt, ist dieses Dokument zurzeit de facto die Planungsbasis für die deutschen Streitkräfte.

³⁴ Deutschland hat 2013 das sogenannte Framework Nations Concept der NATO vorgestellt, um die Entwicklung multinationaler Einheiten – und damit eine Wiederbelebung der europäischen Verteidigungszusammenarbeit – zu fördern; siehe auch den Beitrag von Rainer Meyer zum Felde in diesem Heft.

Tatsache, dass die NATO bisher keine etablierten Mechanismen hat um sich auf das US oder UK Cyber Kommando zu stützen, ist der Deutsche Verweis auf und die Abhängigkeit von der NATO keine adäquate Antwort auf die ansteigenden Cyberbedrohungen. Wenig überraschend experimentieren einige der EU-Mitgliedsstaaten wie die Niederlande und das derzeit noch der EU angehörende Vereinigte Königreich mit Cyberabschreckungsansätzen.

Jegliche Deutsche Cyberabschreckung muss daher damit beginnen, die konzeptuellen nuklearen Abschreckungsmissverständnisse („Biases“) als solche zu identifizieren, um anschließend darüber hinaus sehen und auch agieren zu können. In diesem Zusammenhang hilft es, die fünf Schlüsselunterschiede zwischen Cyberabschreckung und erweiterter nuklearer Abschreckung hervorzuheben:

1. Der Cyberspace besteht aus einem anderen Spielfeld, anderen Spielregeln, Angriffsvektoren und Eskalationsdynamiken. Zum Beispiel ist im Cyberspace jeder eines jeden Nachbar, und das Konzept von Cybergrenzen und Cybersouveränität ist im besten Fall flexibel.
2. Im Cyberspace gibt es keine absolute Abschreckung. Dementsprechend sind geringe bis moderate Maßnahmen und Subversionen keine Verbote von Cyberkrieg, sondern stellen bereits den Krieg selbst dar.
3. Nicht nur Staaten treten als Cyberakteure auf, sondern auch sub-staatliche und nicht-staatliche Organisationen sowie vermehrt halb- und komplett-automatisierte Systeme (Maschinen).
4. Technischer Reifegrad einer Nation bedeutet nicht gleich strategische Vorteile. Stattdessen können Cyberasymmetrien die gegenteilige Wirkung haben: digitale Vergeltungsmaßnahmen seitens eines hochdigitalisierten Landes wie den USA gegen einen digital unterentwickelten Aggressor wie Nordkorea können mangels digitaler Angriffsziele ineffektiv sein. Der Titel Cybersupermacht kann schnell bedeutungslos werden, wie man nach dem Hack der US Wahl gesehen hat.
5. Es existiert noch keine erweiterte NATO Cyberabschreckung (im Gegensatz zur erweiterten Nuklearabschreckung). Im Gegenteil: Die USA kämpfen nicht nur damit, ein eigenes nationales Cyberabschreckungsmodell zu entwickeln, sondern einige Alliierte haben auch nach den Edward Snowden Leaks und in Zeiten von „America First“ damit begonnen, die USA als potenziellen „Spoiler“ im Cyberspace wahrzunehmen.

5 Agile Cyberabschreckung

Wie kann angesichts dieser Herausforderungen eine effektive Cyberabschreckung aussehen? Eine Strategie, die nicht nur die grundsätzlich virtuelle (technologische) Natur der Domäne berücksichtigt, sondern auch die schwierige Startposition von Cyber-Mittelmächten wie Deutschland (im EU Kontext)? Es geht darum eine neue, interdisziplinäre, analytische Arbeit zu initiieren, die als „agile Cyberabschreckung“ bezeichnet werden soll. Es ist eine Herangehensweise, die Grundsätze aus den Computerwissenschaften mit der vierten Welle der Abschreckungstheorie (beispielsweise kumulative Abschreckung) vereint. Das Modell bezieht seinen Namen vom sogenannten „agilen Softwareentwicklungsprinzip“ und konzentriert sich auf die Untersuchung und Optimierung von Verteilungs-, und Kostenauflegungsmechanismen unter dem sogenannten datenzentrischen Cybersicherheitsparadigma (mehr dazu unten). Die empirischen Studien aus diesem Projekt untersuchen neue dogmatische Herangehensweisen, wie z. B. die neue US Cyber Command Vision, sowie Bedrohungs- und Angriffsanalysedaten (beispielsweise zu APTs). Damit soll das Projekt zur Entwicklung eines für Deutschland und die EU funktionierenden und umfassenden Cyberabschreckungsrahmen beisteuern.

5.1 Niederschwellige Cyberoperationen

Die Mehrheit der analytischen Arbeit im Bereich Cyberabschreckung befasst sich mit dem Übergang von Vor-konfliktumgebungen zu einer Umgebung, in der man Cyberkonflikt direkt wahrnimmt, beispielsweise Cyberkrieg.³⁵ Dies übersieht die Tatsache, dass die geringen bis moderaten Maßnahmen und Subversionen von heute kein Verbote vom Krieg im Cyberspace sind, sondern der Krieg selbst (vergleichbar mit der modernen Russischen „Kriegspraxis“, welche fälschlicherweise Valery Gerasimov zugeschrieben wurde).³⁶ Dementsprechend verfeinert das Tallinn Handbuch 2.0 zum Völkerrecht bezüglich Cyberoperationen richtigerweise seine Definition von Cyberkriegsführung, indem es sich statt auf „Cyber-Kriegsführung“ auf „Cyberoperationen“ konzentriert: Taten, welche noch nicht als Kriegshandlungen gelten, jedoch regelmäßig Probleme für Nationalstaaten im Cyberspace verursachen.³⁷

³⁵ Vgl. Lin 2016.

³⁶ Vgl. Galeotti 2018.

³⁷ NATO CCD COE 2017.

Der Fokus auf diese niederschwellige oder „left of boom“ Cyberkonfliktumgebung ändert nicht nur unser Verständnis von Bedrohungen, sondern auch unsere komplette Einstellung zu effektiver Abschreckung in dieser Domäne. Ein Beispiel dafür ist der russische „Hack“ der US Wahlen von 2016. Mehrere einzelne geringe bis moderate Cyber- und Infowar-Operationen wie Hacking, Doxxing, Leaking, und Desinformationskampagnen auf sozialen Netzwerken wurden zusammen verwendet, um eine demokratische Institution (Wahlen) zu unterminieren. Diese Art Angriff passte nicht in die bisherigen IO (Informationsope-ration) Definitionen, die für Konfliktszenarien einer hohen Intensität (kriegerisch) konzipiert wurden. Deswegen versagte die Cyberverteidigung sowie Cyberabschreckung. Agile Cyberabschreckung untersucht deshalb Akteure, Intentionen, Verhalten, Ziele, und Bedrohungen, in den frühen, niederschweligen Phasen eines Cyberkonflikts.

5.2 Anwendung der Grundsätze der agilen Softwareentwicklung

Der aktuellen Cyberabschreckungsforschung fehlt es oft an einer klaren Abgrenzung zwischen Abschreckung in einer physischen Domäne und derjenigen in einer virtuellen Domäne. Cyberspace ist die einzige von Menschen gemachte der fünf militärischen Domänen. Die anderen vier – Land, See, Luft, und Weltall – sind physische, unabhängig vom Menschen existierende Domänen. Dies hat zur Folge, dass der Cyberspace zu einem Grad manipuliert werden kann, der in der physischen Welt unmöglich ist.

Diese inhärente virtuelle (technologische) Natur des Cyberspace hat einen beträchtlichen Einfluss auf elementare Abschreckungsaspekte wie Attribution und „Signalling“: Nukleare Forensik und damit nukleare Attribution basiert überwiegend auf unveränderlichen, nicht-manipulierbaren Isotopenspuren. Die Cyberforensik muss wortwörtlich virtuellen Spuren folgen, die leicht manipulierbar sind. Deswegen müssen Cyberabschreckungsakteure invasive Werkzeuge wie Netzwerk-eingebettete Cyberspionage (SIGINT, HUMINT, GEOINT, OSINT, MASINT) in Betracht ziehen, um eine zuverlässige und zeitnahe Attribution zu erreichen.

Nukleares „Signalling“ basiert auf der Tatsache, dass meine Fähigkeiten einen tatsächlichen Angriff durchzuführen nicht dadurch beeinträchtigt werden, dass sie meinem Gegner bekannt sind (etwa mittels des öffentlichen Testens von Nuklearwaffen). Cybersignalling ist komplizierter: Wenn ich bestimmte Cyberfähigkeiten preisgebe, kann mein Gegner die Wirksamkeit dieser Fähigkeiten oft schwächen oder gänzlich eliminieren,

indem er die Schwachstelle oder den Zero Day schließt. In der Praxis führt diese Situation zu gefährlichen „erst schießen, dann fragen“ Szenarien in Cybereskalationsdynamiken, welche nicht mit den klassischen Abschreckungsmodellen gelöst werden können.

Noch wichtiger: die inhärente technologische Natur des Cyberspace erfordert, dass wir kontinuierlich bereits existierende Cyberabschreckungsmodelle weiterentwickeln, um einen realen Einfluss auf das sich stets ändernde Verhalten der Akteure innerhalb dieser fluktuierenden Domäne zu haben (vergleichbar mit einem Schachbrett, dessen Form, Figuren, und Regeln sich stets ändern). So wie Nuklearwaffen und Raketentechnologie den technologischen Kern der Nukleareskalationsdynamiken bilden, stehen Softwareentwicklung, Automatisierung, und digitale Konnektivität im Zentrum der Cyberabschreckungsdynamiken. Agile Cyberabschreckung wird dieser Tatsache gerecht, indem es Prinzipien aus der sogenannten agilen Softwareentwicklung auf die Cyberabschreckung anwendet. In den Computerwissenschaften beschreibt das Konzept der agilen Softwareentwicklung eine Herangehensweise an Softwareentwicklung, bei der sich Anforderungen und Lösungen durch die kumulative Interaktion von selbst-organisierenden und funktionsübergreifenden Knotenpunkten („Nodes“) und deren Nutzern „emergent“ weiterentwickeln. Agile Cyberabschreckung bedeutet deshalb „breite, inklusive Abschreckung“³⁸ als ein sich entwickelnder, integrierter Mix aus in-domain und out-domain Strategien.

In der Praxis geht agile Cyberabschreckung von höchst flexiblen und instabilen Abschreckungsdynamiken aus, um die Spieltheorie basierten mathematischen Modelle, die das Fundament klassischer Abschreckungstheorie bilden, zu erweitern. Darüber hinaus werden Maschinen (semi- und voll automatisierte Systeme) in einer von voranschreitender Automatisierung gekennzeichneten virtuellen Domäne, selbst zu (semi-unabhängigen) Akteuren die mit der Geschwindigkeit von Elektronen agieren. Eine Tatsache, mit der sich die DARPA Cyber Grand Challenge (CGC) 2016 zurecht beschäftigte.³⁹ Die CGC organisierte erfolgreich einen Wettbewerb zur Erstellung automatischer Cyberabwehrsysteme, die in Echtzeit Schwachstellen untersuchen und „Patches“ kreieren sowie implementieren können. Indem sie mit Maschinengeschwindigkeit und Maschinenreichweite agieren, könnten diese Technologien in Zukunft den heutigen Angreifer-dominierten Status Quo auf den Kopf stellen. Agile Cyberabschreckung berücksichtigt diese steigende Automatisierung von

³⁸ Valeriano/Maness 2015.

³⁹ <http://archive.darpa.mil/cybergrandchallenge/about.html>.

Cybersicherheitsumgebungen und sogenannte „Cognitive Security“ Technologien.

5.3 Beachtung der variierenden Intentionen von Cyberoperationsakteuren

Ein weiteres Element welches eine agile Herangehensweise an Cyberabschreckung erfordert, ist die Tatsache, dass die Intention eines Akteurs in Cyberoperationen sich rapid ändern kann, wenn die Bedeutung oder Grundzustände des Cyberspace selbst sich verändern. Stuxnet gilt traditionell bei Amerikanern als Beweis für einen spezifischen Cyberangriffsvektor, nämlich, dass sie in jedes System eindringen und jedes System sabotieren können. Laut dieser Deutung ist der Cyberspace eine Plattform für kritische Infrastrukturen (die zerstört werden mussten). Aber Stuxnet hat eine oft übersehene IO (Informationsoperationen) Komponente: Stuxnet belieferte „Admins“ mit falschen Informationen, welche besagten, dass das System fehlerfrei operierte. Für einen anderen Akteur, die Russen, ist diese Komponente Beweis für einen komplett anderen Cyberangriffsvektor: dass Menschen Maschinen mehr glauben als ihren eigenen Augen. In diesem Fall ist Cyberspace eine Plattform für die Datenintegrität (welche untergraben werden musste).

Zurückblickend kann diese „kreative“ russische Sicht auf Stuxnet als Vorreiter der späteren Cyber- und Desinformationsoperationen gegen die US Wahlen verstanden werden. Eine solch innovative Sicht auf einen spezifischen Angriff kann die Absicht eines Angreifers schlagartig ändern – mit weitreichenden Konsequenzen für sein Verhalten und damit für die Wirksamkeit möglicher Vereitelungs-, Kostenauflegungs-, oder Resilienz-Maßnahmen des Angriffsoffers. Das gesamte Spiel ändert sich über Nacht. Agile Cyber Abschreckung stellt deshalb eine neue Taxonomie für Cyber Akteure vor. Diese basiert auf deren Intentionen, insbesondere differenziert sie zwischen so genannten Hacktivists, Defacern, Penetration Testern, Red Teams, Cyber Kriminellen, Cyber Spionagediensten wie NSA, GCHQ oder GRU, militärische Cyberkommandoeinheiten und Hybriden Teams.

5.4 Integration des datenzentrischen Cybersicherheitsparadigmas

Die aktuellen Cyberabschreckungsmodelle nutzen überwiegend ein „netzwerkzentrisches“ Paradigma von Cybersicherheit, um kritische Ziele zu definieren. Netzwerkzentrische Cyberabwehr versucht einen Dieb daran zu

hindern an Daten zu gelangen (es bewacht den „Zaun“), während das neue „datenzentrische“ Cyberabwehrparadigma davon ausgeht, dass der Dieb letztendlich die Daten erreichen wird (den „Zaun“ überwinden wird). Dementsprechend machen solche neuen Abwehrmechanismen Informationen schwer auffindbar und unmöglich zu lesen. Das kritische Ziel ist also nicht mehr die Integrität des Netzwerks. Es ist die Integrität der Daten selbst.

Der Unterschied zwischen den alten und neuen Herangehensweisen ist profund. Indem die Machtverhältnisse zwischen Räuber und Beute geändert werden, wird eine neue Price-Performance Kurve für Cybersicherheit eingeführt, die wichtige Implikationen für die Kosten-Nutzen Bewertung der Cyberabschreckungsakteure hat.⁴⁰ Das heißt, dass ein richtig implementiertes datenzentrisches Paradigma signifikante Asymmetrien zwischen Freund und Feind hervorrufen kann. Authentifizierte Freunde haben die Schlüssel, während der Gegner einen enormen Rechenaufwand bewältigen muss, um an nur einen einzigen Datenaustausch heranzukommen. So werden sämtliche abgefangenen Daten bedeutungslos. Die agile Cyberabschreckung untersucht somit die technologischen Entwicklungen in Kryptotechnologie (z. B. Postquantum-Krypto), in der Cyber-Forensik und Big Data Analysen, und deren Auswirkungen auf Cyberabschreckung durch Vereitelung und Resilienz.⁴¹

5.5 Asymmetrien

Derzeitige Cyberabschreckungsmodelle berücksichtigen nicht in ausreichendem Maße die Asymmetrien (und ihre Auswirkung auf Eskalationsdynamiken), die der neuen operativen Domäne zu eigen sind. Die agile Cyberabschreckung berücksichtigt drei Cyberabschreckungs-Asymmetrien:

- Cyber-Entwicklungsgrad-Asymmetrie: Länder, die über die höchste Cyber- und Internet-Bildung und Entwicklung verfügen (z. B. die USA) können gegenüber Angriffen aus weniger cyber-entwickelten Ländern (z. B. Nordkorea) hoch verwundbar sein, da in-domain Vergeltungsmaßnahmen keine symmetrischen Ziele identifizieren können.
- Cyber-Ausbildungs-Asymmetrie: Cybersecurity Bildungsinhalte (z. B. Curricula für Computerwissen-

⁴⁰ Vgl. O'Hare/Berkeley 2015.

⁴¹ Vgl. Philipp S. Krüger, „Krypto-Krieg 2.0: Warum der Streit zwischen Apple und dem FBI so wichtig ist“, *Süddeutsche Zeitung*, 17.3.2016, sowie Peter Schmitz, „Was ist ZITIS?“, *Security Insider*, März 2018 <https://www.security-insider.de/was-ist-zitis-a-699634/>.

schaften und Hacking) konzentrieren sich in Ländern mit geringerem Cyber-Entwicklungsgrad in der Regel auf technisch einfache, sogenannte „Reverse Engineering“ Ansätze, wohingegen in Cyber-versierten Ländern das Hauptaugenmerk eher auf high-end Software und Hardware Szenarien liegt. Dies kann zu einem großen Lager an hoch ausgebildeten und kreativen „Hackern“ in Cyber-Entwicklungsländern führen, da diese Reverse Engineering Fähigkeiten auch höchst effiziente Hacking-Ansätze hervorbringen.

- Cyber-Angriffsverbreitungs-Asymmetrie: wie die russische Desinformationskampagne gegen die US Wahlen 2016 zeigte, können hohe Standards bei der Meinungsfreiheit und eine unabhängige Presse (in den USA) zu einer destruktiven Mainstream-Verbreitung (Fox News) von “fake news” führen, die Angreifer in hybriden Mensch-Maschine Troll Farmen generiert haben (russische Cyberkriegsführungseinrichtungen in St. Petersburg). Ein gleich gearteter Desinformations- oder Propagandagegenangriff gegen den repressiven und autoritären Angreifen führt vermutlich nicht zum selben Ziel, da die Verbreitung der Desinformation (und damit ihr Einfluss) vom Zielland kontrolliert werden kann. Ein entsprechender Desinformationsgegenangriff ist darüber hinaus unter den hohen ethischen und legalen Normen, denen das Opferland meist unterliegt, oftmals nicht erlaubt.

6 Agile Cyberabschreckungsoptionen für Deutschland

Das oben beschriebene agile Cyberabschreckungsmodell führt zu 4 Optionen für Deutschland hinsichtlich Vereitelung und Kostenauflegung bei Cyberkonflikten:

1. Die Entwicklung einer „emergenten“ Taxonomie, die beschreibt, welche Arten von Aktivitäten das neue Modell abschrecken soll. Insbesondere eine Beschreibung der Reichweite, des Umfangs und der Konsequenzen von bösartigen Cyberoperationen, die die Sicherheit, wirtschaftliche Stabilität, öffentliche Sicherheitsbelange, Privatsphäre und Freiheiten von Deutschland bzw. der EU beeinflussen könnten.
2. Die Entwicklung von Vereitelungsmechanismen und –fähigkeiten (den von einem Feind erwarteten Gewinn vereiteln, indem der Aufwand zu sehr in die Höhe getrieben wird – vor allem durch Verteidigung z. B. durch „Isolierung“ des Angreifers, Verschlüsselung, Resilienz und Wiederaufbaukapazitäten und –prozesse).
3. Die Entwicklung von Kostenauflegungsmechanismen und –fähigkeiten: die voraussichtlichen Kosten bzw. Strafen für Aktionen des Kontrahenten so schmerzhaft in die Höhe treiben dass er diese Kosten nicht mehr akzeptieren will). Insbesondere durch wirtschaftliche, diplomatische, Strafverfolgungs- und (als äußerstes Mittel) militärische Instrumente, sowohl in-domain (Cyber) wie auch out-domain. Wichtig ist in diesem Kontext die Unterscheidung zwischen Präventivmaßnahmen und vergeltenden Gegenangriffen. Einige Experten in den USA plädieren zwar für präventive Cyberangriffe, jedoch sollte dies keine Option für Deutschland sein, nicht nur in Anbetracht seiner historischen und ethischen Verantwortung, sondern auch wegen der schwer zu kontrollierenden Eigendynamik, die ein solcher Ansatz eines Cyber-Präventivangriffs entwickelt. Außerdem missversteht dieser Ansatz die Mechanismen der vergeltenden Kostenauflegung, da er auf absolute bzw. fast-absolute Abschreckung (fälschliche Anwendung der Prinzipien der nuklearen Abschreckung auf den Cyberraum) abzielt. Unter dem neuen agilen Cyberabschreckungsmodell sind (kumulative) offensive Maßnahmen möglich, die sich auf die Kosten-Nutzen Kalkulation sowie die zugrundeliegenden Cyberangriffsfähigkeiten eines Angreifers auswirken. Um aber eine Eskalation zu vermeiden, müssen sie von Natur aus vergeltend sein.
4. Die Entwicklung unterstützender Maßnahmen und Fähigkeiten einschließlich Cyber-bezogene Diplomatie, öffentliche Aufklärung bzw. „gesellschaftliche Cyber-Hygiene“, Cyber-effektive Industrie- bzw. Schlüsseltechnologepolitik (insbesondere auf EU-Ebene), nachrichtendienstliche Instrumente, sowie Forschung und Entwicklung, um durch die Planung von und Investitionen in Werkzeuge, Techniken und Arbeitskräfte die Zukunft von Cybersicherheit in Europa zu formen. Ziel ist es die Resilienz der digitalen Umgebung zu verbessern und neue technologische Möglichkeiten zur Abschreckung von bösartigen Cyber-Aktivitäten verfügbar zu machen. Ein gutes Beispiel hierfür ist das neue gemeinsame BMVg-BMI Projekt ADIC, eine DARPA-ähnliche Agentur für disruptive Cybersicherheitsforschung.

Auf praktischer Ebene befördert die agile Cyberabschreckung die Entwicklung von sogenannten Eskalations-Playbooks, die an die besonderen Anforderungen einer Organisation angepasst sind. Diese Playbooks basieren auf 4 Kernkomponenten: (1) Cyberangriff-Fallstudien, (2) Muster für Fallstudien, (3) Agile Cyberabschreckungsplanung, (4) Agile Cyberabschreckungsausführung.

Jedes digital vernetzte Land braucht eine effektive Antwort auf strategische Cyber-Attacken. Kann reine Cyberabwehr die Antwort im Sinne von Abschreckung und Kostensteigerung für den Aggressor nicht liefern, wird eine breite, inklusive Cyberabschreckungstheorie und –praxis – beruhend auf einem emergenten, integrierten Mix aus in-domain und out-domain Strategien notwendig („Agile Cyberabschreckung“). Insbesondere auch unter Einbeziehung proportionaler und kumulativer Cyberoperationen sowie politischer, juristischer und wirtschaftlicher Sanktionen. Trotz seiner besonderen Cyber-Verwundbarkeiten hat Deutschland eine Vielzahl an Möglichkeiten, wirksame Cyber-Vereitelungs- und Kostenauflegungsmechanismen und –fähigkeiten zu entwickeln, insbesondere auch auf europäischer Ebene und im Zusammenspiel mit europäischen Cyber-Partnern wie Holland, Estland oder Frankreich. Dabei sind Optionen anzustreben, die in vollem Einklang mit Deutschlands militärischen, verfassungsrechtlichen und ethischen Prinzipien stehen. Weitere Untersuchungen des agilen Cyberabschreckungsmodells und dessen Anwendbarkeit auf die Bedrohungsvektoren spezifischer Interessensgruppen werden Deutschland dabei helfen, Cyberkonflikte in Zeiten steigender weltweiter Cyberunsicherheit besser zu kontrollieren, zu deeskalieren oder zu beenden.

Literatur

- AIVD – General Intelligence and Security Service (2017): Annual Report. Den Haag; Ministry of the Interior and Kingdom Relations; <https://english.aivd.nl/binaries/aivd-en/documents/annual-report/2018/03/09/annual-report-2017-aivd/Annual+Report+2017+AIVD.pdf>
- Black Hat (2017): Black Hat Attendee Survey. Portrait of an Imminent Cyberthreat. Black Hat; <http://www.blackhat.com>.
- Bundesamt für Sicherheit in der Informationstechnik – BSI (2017): Die Lage der IT-Sicherheit in Deutschland. Berlin; Bundesregierung; <https://www.bsi.bund.de>
- Bundesregierung (2016): Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016. Berlin; Bundesregierung.
- Carter, Ashton (2017): *A Lasting Defeat: The Campaign To Destroy ISIS*. Cambridge, Mass.; Belfer Center for Science and International Affairs, Harvard Kennedy School Report.
- Dunn Cavelty, Myriam (2011): Unlocking the ‘Stuxnet Effect’: On Continuity and Change in the Discourse on Cyber Threats’, *Military and Strategic Affairs* 3/3 (herausgegeben vom INSS, in hebräischer Sprache)
- Falliere, Nicolas/Murchu, Liam O./Chien, Eric (2011) W32. Stuxnet Dossier – Version 1.4. Mountain View, Cal.; Symantec; https://www.symantec.com/content/.../w32_stuxnet_dossier.pdf
- Farwell, James P./Rohozinski, Rafal (2011): Stuxnet and the Future of Cyber War’, *Survival*, 53 (1), 23–40
- Galeotti, Mark (2018): I’m Sorry for Creating the ‘Gerasimov Doctrine’, *Foreign Affairs*, 8. März; <http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/>
- Harknett, Richard J. (2018): United States Cyber Command’s New Vision: What It Entails and Why It Matters, *Lawfare Blog*, March, <https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters>.
- Harknett, Richard J./Callaghan, John P./Kauffman, Rudi (2010): Leaving Deterrence Behind: War-Fighting and National Cybersecurity’, *Journal of Homeland Security and Emergency Management* 7 (1), keine Seitenzahlen, da online erschienen (www.degruyter.com)
- Hodges, Duncan/Creese, Sadie (2015): Understanding Cyber-Attacks.’ In: Green, James A. (Hrsg.) *Cyber Warfare: A Multidisciplinary Analysis*, Abingdon, Oxon/New York; Routledge, 33–60.
- Krüger, Philipp S.(2016): *Measuring the Digital Economy: The Second Digital Revolution*. Berlin; Stiftung Neue Verantwortung.
- Libicki, Martin (2009): Cyber Deterrence and Cyber War. Santa Monica, California; RAND Corporation.
- Lin, Herbert (2012): Operational Considerations in Cyber Attack and Exploitation; in: Reveron, Derek S. Reveron (Hrsg.): *Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World*, Washington, D.C.; Georgetown University Press, 37–56.
- Lin, Herbert (2016): An Evolving Research Agenda in Cyber Policy and Security. Stanford, Cal.; Stanford University Center for International Security and Cooperation.
- Lupovici, Amir (2011): Cyber War and Deterrence: Trends and Challenges in Research, *Military and Strategic Affairs* 3 (3) 49–62
- Mandel, Robert (2017): *Optimizing Cyberdeterrence*. Washington, D.C.; Georgetown University Press.
- NATO CCD COE (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Brüssel: NATO.
- Nye, Joseph S., jr. (2016): Deterrence and Dissuasion in Cyberspace, *International Security*, 41 (3), 44–71.
- Nye, Joseph S., jr. (2018): Wie wird sich die Entwicklung neuer Normen für Cybersicherheit gestalten? Project Syndicate, 8. März, <https://www.project-syndicate.org/commentary/origin-of-new-cybersecurity-norms-by-joseph-s--nye-2018-03/german>.
- O’Hare, Mark S./Berkeley, Alfred R., III (2015): The New Paradigm for Cyber Security, *Proceedings, U.S. Naval Institute*, 141 (3), 82–84.
- Porche, Isaac R. III/Sollinger, Jerry M./McKay, Shawn (2011): *A Cyber Worm that Knows no Boundaries*. Santa Monica, California; RAND Corporation.
- Poznansky, Michael/Perkoski, Evan (2016): *Rethinking Secrecy in Cyberspace*, verfügbar in Social Science Research Network; <https://ssrn.com/abstract=2836087>.
- PWC – Price, Waterhouse, Coopers (2018): *PWC Survey ‘The Global State of Information Security Survey’ 2018*. <https://www.pwc.com/us/en/cybersecurity/information-security-survey.html>
- Tor, Uri (2017): ‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence, *Journal of Strategic Studies*, 40 (1–2), 92–117.
- Valeriano, Brandon/Maness, Ryan C. (2015): *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford; Oxford University Press.
- Wilner, Alex (2015): Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far? *Journal of International Law and Politics*, 47 (2), 439–462