Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)945
10.12.2020 - 19/3507
5410

Stiftung Neue Verantwortung

Sachverständigen Statement

Stellungnahme von Julia Schuetze[1], Projektmanagerin im Bereich Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die öffentliche Anhörung des Verteidigungsausschusses am 14. Dezember 2020 zum Thema "Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehaltes, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen".

Die vorliegende Stellungnahme bezieht sich vor allem auf die Bereiche des Fragenkatalogs, die sich nicht mit völkerrechtlichen Aspekten oder Fragen des "Informationsraums" auseinandersetzen.

"Es ist die gleiche Domäne."

Vorab ist es wichtig kurz auf die folgende Frage einzugehen, deren Beantwortung den Rahmen der Diskussion stellt: *Ist in einem grenzenlosen Cyberraum eine Abgrenzung zwischen innerer und äußerer Sicherheit möglich und praktikabel?* Diese Frage hat meiner Meinung nach bisher niemand besser und deutlicher beantwortet als Ciaran Martin, Professor of Practice at the Blavatnik School of Government at Oxford University, ehemals UK Government's National Cyber Security Centre (NCSC) in seiner Rede im November im King's College London. Daraus möchte ich einen Ausschnitt zitieren und empfehle, die gesamte Rede zu lesen:

"*Cyber is now a strategic domain of operations for nation states. But the second appointment, a message of basic consumer protection, reflects, in my view, the primary characteristic of cyber as a domain.* (...) *You are a civilian in the cyber domain even as you ponder its strategic national security implications in the context of this talk." "Cyber as a domain of military and national security operations co-exists with cyber as a domain of everyday life. It's the same domain.[2]"*

Aus diesem Zitat lässt sich schließen, dass die Domäne Cyberraum sowohl für Verteidigung als auch friedliche Aktivitäten untrennbar ist. Es handelt sich um dieselbe Domäne. Dies muss mitbedacht werden, da die Nutzung der Domäne für Verteidigung potenziell positive und/oder negative Auswirkungen auf die Nutzung derselben Domäne für friedliche Aktivitäten haben kann, weil es untrennbar ist. Dies bedeutet auch, dass in allen Politikfeldern, in denen der Cyberraum eine Rolle spielt, mitbedacht werden muss, welche positiven oder negativen Auswirkungen bestimmte Maßnahmen in einem Politikfeld auf die Erreichung der Ziele in einem anderen haben. Deswegen sollte Cyberverteidigungspolitik nicht in einem Silo stattfinden.

Vom sicherheitspolitischen Selbstverständnis hin zu Maßnahmen bei der Cyberverteidigungspolitik

[1] Stiftung Neue Verantwortung (2020): Experten-Profil von Julia Schuetze.
[2] Ciaran Martin (2020): Cyber Attacks: What actual harm do they do?.

Welche Aktivitäten im Bereich Cyberverteidungspolitik eingesetzt werden können, lässt sich nicht nur durch die verfassungsrechtlichen Grenzen ableiten, sondern werden auch vom sicherheitspolitische Selbstverständnis eines Landes bestimmt. Dieses hat dann zum Beispiel auch Auswirkungen darauf, welche internationale Normen für verantwortungsvolles staatliches Verhalten Anwendung finden oder unterstützt werden.

Das deutsche sicherheitspolitische Selbstverständnis ist im Weißbuch aus dem Jahre 2016 niedergeschrieben und beschreibt Deutschlands Rolle in der Welt, Deutschlands Werte und sicherheitspolitische Interessen geprägt durch die Lehren aus unserer Geschichte. Daraus lassen sich strategische Standort- und Kursbestimmung für die deutsche Sicherheitspolitik ableiten. Es wird deshalb als wesentlicher Leitfaden für Entscheidungen und Handlungen, auch bei der Bundeswehr, genutzt[3]. Seit 2016 hat sich viel in der internationalen Cybersicherheitspolitik verändert. Einige Länder haben zwischen 2018 und 2020 aus ihrem sicherheitspolitisches Selbstverständnis heraus, Antworten für die Rolle von Cyber Verteidigung für ihr Land gefunden. Die USA, aber auch viele andere Länder haben ihre Strategien beispielsweise weiterentwickelt[4] und ihren Pool an Maßnahmen verändert[5]. Auf EU Ebene wurden neue Frameworks für die Zusammenarbeit an Cybersicherheit geschaffen, die auch neue Maßnahmen enthielten, wie zum Beispiel die Cyber Diplomacy Toolbox. Auf UN-Ebene findet darüber hinaus aktive Arbeit zu Normen statt. Auch in Deutschland wurden in den letzten Jahren immer wieder neue Maßnahmen diskutiert[6] und vorgeschlagen[7], weitere Maßnahmen fanden zum ersten Mal Anwendung[8]. Was bisher jedoch fehlt ist eine klare Positionierung, welche Strategie Deutschland damit verfolgt und wie sich diese Strategie aus dem sicherheitspolitischen Selbstverständnis, welches im Weißbuch beschrieben ist, ableitet. Eine solche transparente und nachvollziehbare Haltung, würde es Deutschland ermöglichen, gezielter mit Konflikten umzugehen und Kooperationen mit anderen Ländern im Sinne von gemeinsamen Zielen auszubauen.

Ich sehe deswegen den Ausschuss hier als Anlass, diesen Diskurs anzustoßen und noch einmal genau zu hinterfragen, wie die neuen Entwicklungen zum sicherheitspolitischen Selbstverständnis von 2016 passen. Darüber hinaus gilt es zu analysieren, welche neuen Maßnahmen zu Deutschland passen würden. Andere Staaten haben dies schon für sich gemacht. Sie können als Beispiel dafür dienen, wie tief verankert die Auswahl der Maßnahmen mit dem sicherheitspolitischen Selbstverständnis sind. Aus dieser Perspektive kann geschlossen werden, welche zukünftige Rolle der Cyberraum für Verteidigung haben könnte.

---

[3] BMVG (2016) Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr.
[4] z.B. USA: White House (2018) National Cyber Strategy, Australia: Australian Government (2020): Australia's Cyber Security Strategy 2020; Japan: Ministry of Defense (2020) Defense of Japan 2020 Frankreich: Ministere des Armées (2019) Stratégie cyber des Armées (pdf Download).
[5] z.B. E-Estonia (2020):Estonia and the United States to build a joint cyber threat intelligence platform; Nikkai Asia (2020) Japan to lead first cyber defense drill with ASEAN, US and Europe
[6] Sven Herpig (2020) Aktive Cyber-Abwehr / Hackback Leseliste
[7] Offener Brief an das Bundesministerium des Innern, für Bau und Heimat Betreff: Geplanter Eingriff in Verschlüsselung von Messenger-Diensten hätte fatale Konsequenzen
[8] Council of Europe (2017) Cyber attacks: EU ready to respond with a range of measures, including sanctions; Council of Europe (2020) EU imposes the first ever sanctions against cyber-attacks

Die USA und Japan sind zwei Länder, die sehr unterschiedliche sicherheitspolitische Selbstverständnisse haben und daraus Strategien und Maßnahmen für ihre Cyberverteidungspolitik abgeleitet haben. Wegen eines unterschiedlichen Verständnis von ihrer Rolle in der Welt, haben sie verschiedene Strategien und Maßnahmen gefunden, um mit Bedrohungen aus dem Cyberraum umzugehen. Die beiden Beispiele sollen zeigen, wie eng verknüpft Entscheidungen über Strategie und Maßnahmen mit dem sicherheitspolitischen Selbstverständnis eines Landes sind.

Anwendung des US-Amerikanischen sicherheitspolitischen Verständnisses mit folgendem Update der Cyberverteidungspolitik

Die USA sieht sich im Wettbewerb mit bestimmten Staaten und organisierter Kriminalität[9], welche die Vorherrschaft der USA infrage stellen und dafür auch den Cyberraum nutzen. In den USA wurde deswegen die Schlussfolgerung getroffen, dass dieser Wettbewerb kontinuierlich auch im Cyberraum ausgefochten werden muss mit dem Ziel, dass die USA als Sieger hervorgeht. Durch den Einsatz von offensiven Cyberoperationen soll zum Einen versucht werden, Angriffe frühzeitig zu erkennen und abzuwehren. Zum anderen gilt es, bereit für eine mögliche Verteidigung zu sein. Um dies zu erfüllen, führen US Militärs im Zweifelsfall auch offensive Cyberoperationen in "grauen Netzen" durch - das könnten zum Beispiel IT-Systeme deutscher Firmen und Behörden sein[10]. Diese Aktivität wird aus dem Selbstverständnis abgeleitet, dass ein offensives Vorgehen auch in anderen Feldern weit verbreitet ist: „Wir müssen uns im Cyberspace wie in den physischen Bereichen vorwärts verteidigen. Unsere Seestreitkräfte verteidigen nicht, indem sie im Hafen bleiben, und unsere Luftwaffe bleibt nicht auf Flugplätzen. Sie patrouillieren über Meere und Himmel, um sicherzustellen, dass sie in der Lage sind, unser Land zu verteidigen, bevor unsere Grenzen überschritten werden. Die gleiche Logik gilt im Cyberspace. Ein anhaltendes Engagement unserer Gegner im Cyberspace kann nicht erfolgreich sein, wenn unsere Aktionen auf Department-of-Defense-Netzwerke beschränkt sind."[11] Es gilt das Credo: "Ein Amerika, das erfolgreich konkurriert, ist der beste Weg, um Konflikte zu vermeiden." Die USA versucht seitdem, eine Überlegenheit im Cyberraum zu erreichen. Zu diesem Zweck nutzen die USA Maßnahmen verschiedener Behörden, zum Beispiel Überwachungstechniken, Spionageabwehr und offensiven Cyber-Operationen, um ausländische Operationen zu verfolgen und ihnen entgegenzuwirken.[12] Die Rolle der Cyberverteidigung ist dabei eng verknüpft mit den Missionen anderer Behörden, wie der NSA oder dem Department of Homeland Security[13]. Um den Einsatz von offensiven Mitteln zu rechtfertigen, identifizieren die USA diejenigen Länder, die ein Risiko für die Cybersicherheit in den USA darstellen - mit denen sie im Wettbewerb stehen. Die USA werden mit Ländern, die als Risikoland eingestuft wurden, kontinuierlich im Cyberraum konkurrieren. In der Nationalen Cyber-Strategie 2018 wurden der Iran, China, Nordkorea und Russland identifiziert. Dabei geht die USA davon aus, dass dieser Wettbewerb nicht unweigerlich zu Konflikten führt. Sollte es jedoch dazu kommen, solle niemand daran zweifeln, dass sich die USA

[9] White House (2018) National Cyber Strategy: "The Administration recognizes that the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. Russia, China, Iran, and North Korea all use cyberspace as a means to challenge the United States, its allies, and partners, often with a recklessness they would never consider in other domains."
[10] Smeets (2019) Cyber Command's Strategy Risks Friction With Allies
[11] Paul M. Nakasone (2019), 'A Cyber Force for Persistent Operations,' Joint Force Quarterly, vol. 92
[12] Gen. Joseph F. Dunford Jr (2019) 'Defending Forward,' Joint Force Quarterly, vol. 92
[13] Schuetze (2020) EU-US Cybersecurity Policy Coming Together, Seite 40 "interagency missions"

entsprechend verteidigt, heißt es weiter[14]. Deswegen verfolgt die USA zusätzlich das strategische Ziel der Abschreckung, welches sich aber nicht nur auf Cyber-Angelegenheiten konzentriert: „Die Führer des Pentagon konzentrierten sich auf Abschreckung, wenn auch nicht speziell auf Cyber-Abschreckung. Stattdessen untersuchten sie, wie Cyberspace-Operationen zu einer breiteren Abschreckungsmaßnahme führen würden.[15] Die US-Strategie besagt, dass die Regierung alle in ihrer Macht stehenden Instrumente einsetzen wird, um Cyberangriffe abzuwehren und böswilligen Akteuren mit schnellen und transparenten Konsequenzen entgegentreten wird.[16] Dies bedeutet theoretisch, dass die USA auf einen Cyberangriff, auch mit einer Bombe reagieren könnten. Dieses Beispiel verdeutlicht, dass die USA ihr sicherheitspolitisches Selbstverständnis in den Cyberraum ausweitet und durch eine neue Strategie unterlegt, welche mit passenden Maßnahmen unterfüttert wurde. Dies hat wiederum Auswirkungen auf die US-amerikanische Cyberaußenpolitik im Bereich internationale Normen. Hier gibt es seitdem ein Mangel an Engagement für einige der diskutierten Normen für verantwortungsbewusstes staatliches Verhalten, insbesondere für die Norm zum Schutz des öffentlichen Kerns des Internets. Diese Norm besagt, dass „staatliche und nichtstaatliche Akteure Aktivitäten, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des Internets absichtlich und erheblich beeinträchtigen, weder durchgeführt noch wissentlich zugelassen werden sollten“.

Anwendung des sicherheitspolitischen Verständnisses Japans auf neue Herausforderung im Bereich Cyberteidungspolitik

Im Kontrast zum Beispiel der USA hat Japan das Prinzip des Pazifismus in Artikel 9 seiner Verfassung verankert. Dies hat den Verzicht auf Krieg, das Verbot des Kriegspotentials und die Verweigerung des Rechts auf Kriegführung des Staates zur Folge[17]. Die ausschließlich verteidigungsorientierte Politik bedeutet, dass die Abwehrkraft nur im Falle eines Angriffs eingesetzt werden darf. Außerdem bedeutet es, dass das Ausmaß des Einsatzes von Verteidigungsfähigkeiten auf ein Minimum beschränkt wird, welches notwendig sei für die Selbstverteidigung. Deswegen draf Japan nur Verteidgungsfähigkeiten aufbauen, die zur Selbstverteidigung notwendig sind. 2015 wurde eine Neuinterpretation von Artikel 9 der pazifistischen Verfassung Japans (die 'Gesetzgebung für Frieden und Sicherheit von 2015') verabschiedet Diese beinhaltete, dass Japan unter anderem Verbündeten zu Hilfe kommen darf, auch wenn Japan selbst nicht angegriffen wurde. Nun stand Japan vor der Herausforderung, wie es Fähigkeiten für die Cyberabwehr in den Einklang mit dieser Verfassung und dem Update aus 2015 bringen sollte. Konkret ging es um die Frage, welche Rolle die zivile Verteidigungsgruppe (Japan Self-Defense Forces, JSDF) unter dem Ministerium für Verteidigung im Innern und international einnehmen sollte. Die Antworten finden sich in der Verteidigungsstrategie von 2020[18]. Hier erkennt Japan öffentlich an, dass es momentan eine Gefährdungslage gibt, die im Graubereich zwischen Frieden und Krieg liegt. Daraus hat die japanische Regierung geschlussfolgert, dass sich die zivile

[14] White House (2017) National Security Strategy
[15] Mark Pomerleau, ‘Is There Such a Concept as “Cyber Deterrence?”,’ Fifth Domain, 30 April 2019./ .
[16] US Congress, ‘FY2019 NDAA: Policy of the United States on Cyberspace, Cybersecurity, Cyber Warfare, and Cyber Deterrence,’ ; White House (2017) National Security Strategy (2017)
[17] Japan Ministry of Defense (2020): Constitution and the Basis of Defense Policy: “Under the Constitution, Japan is permitted to possess the required minimum self-defense capability. The specific limit is subject to change according to the prevailing international situation, the level of military technologies, and various other factors, and it is discussed and decided through annual budget and other deliberations by the Diet on behalf of the people.”
[18] Japan Ministry of Defense (2020) Defense of Japan 2020

Verteidigungsgruppe ständig bereit halten müsste, üben muss, und weiträumig, beständige Aufklärung und Überwachung im Innern zu betreiben. Konkret für die Cyber-Verteidigung und Cyberabwehr bedeutet dies zum Beispiel 24-Stunden-Überwachung von eigenen Netzwerken und Informationssystemen sowie erweiterte Maßnahmen gegen Cyber-Angriffe (Malware-Analyse) durch die Cyberverteidungsgruppe. Dies bedeutet im Vergleich zu den USA, dass Japan aktivere Cyberabwehr nur für die Informationsgewinnung[19] in den eigenen Netzen betreibt, aber nicht in die Netze anderer Staaten eingreift. In Bezug auf Offensivfähigkeiten zur Aufklärung oder Wirkung von Angriffen[20] erklärte Shinzo Abe wiederholt, dass die Neuinterpretation von Artikel 9 der pazifistischen Verfassung Japans (die 'Gesetzgebung für Frieden und Sicherheit von 2015') nicht für JSDF-Aktivitäten im Cyberraum gilt. Daher beschränkt sich das Verteidigungsministerium auf das Studium offensiver Cyberoperationen zur Informationsgewinnung für die Verbesserung der Defensive[21]. International beteiligt sich Japan vor allem an Cybersicherheit-Übungen zur Verbesserung der Reaktion auf Cyberangriffe. Japan hat sein sicherheitspolitisches Verständnis nicht komplett verändert, sondern eher an die neuen Herausforderungen angepasst, indem es sich strategisch weiterhin defensiv positioniert, aber durch eine Resilienzstrategie und passenden Maßnahmen kontinuierlich an der Cybersicherheit des Landes arbeitet und sich dafür auch international einsetzt.

Deutschlands sicherheitspolitisches Verständnis und seine Auswirkungen auf die Cyberverteidigungspolitik

In Deutschland müsste genau so wie in Japan und den USA und weiteren Ländern, das sicherheitspolitische Selbstverständnis unter Einbeziehung der aktuellen Herausforderungen und Entwicklungen in Einklang mit der Cyberverteidungstsrtageie gebracht werden. Es gilt also, transparent zu erklären, inwieweit die Maßnahmen im Bereich Cyberverteidungspolitik konsistent zu Deutschlands Selbstverständnis passen.
Dass dies momentan noch nicht gemacht wird, sieht man an den Diskussionen zu Maßnahmen, ohne jegliche Begründung und Verknüpfung zum sicherheitspolitischen Selbstverständnis herzustellen. Dieses Vorgehen lähmt sicherheitspolitische Entscheidungen oder führt im schlimmsten Falle dazu, dass Deutschland Maßnahmen entgegen des eigenen Interesse durchführt oder sich aktuellen Entwicklungen gegenüber nicht aktiv positioniert. Zum Beispiel müsste adressiert werden, inwieweit die Aktivitäten der USA im Bereich “defending forward” auch Deutschland betreffen. Momentan ist nicht klar, inwieweit Deutschlands sicherheitspolitisches Interesse “Schutz der Bürgerinnen und Bürger sowie der Souveränität und territorialen Integrität unseres Landes;”[22] mit US-amerikanischen Cyberoperationen in deutschen Netzen, in Einklang zu bringen ist. Hier lässt das Weißbuch der Bundeswehr eine besondere Rolle zukommen, nämlich: “Deutschlands Souveränität und territoriale Integrität zu verteidigen und seine Bürgerinnen und Bürger zu schützen”. Wie genau soll die Bundeswehr bei so einmal Fall vorgehen? Wie weit geht der Begriff territoriale Integrität? Eine Positionierung bei diesen Fragen könnte auch gemeinsam mit anderen EU Staaten erfolgen.

[19] Siehe Dr. Sven Herpig Sachverständigenstatement
[20] Siehe Dr. Sven Herpig Sachverständigenstatement
[21] Schuetze (2020) Japan Cybersecurity Policy: An Introduction
[22] BMVg (2016) Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr.

Eine Beschreibung der Cyberverteidung abgeleitet aus dem Weißbuch 2016 sollte auch darlegen, inwieweit verschiedene Maßnahmen aus den anderen Feldern e.g. Cyberaußenpolitik und Cybersicherheitspolitik strategisch ineinander greifen[23]. Zum Beispiel im Fall eines Cyberangriffs, wann werden Maßnahmen auf EU Ebene erwogen, welche aus den Bereichen Cyberaußen- Cybersicherheit und Cyberverteidungspolitik kommen könnten. Hier könnte auch noch einmal genauer darauf eingegangen werden, welche Maßnahmen die Bundeswehr noch einsetzen kann, um ihrer Rolle als Förderer für "Sicherheit und Stabilität im internationalen Rahmen"[24] auch für den Cyberraum zu erfüllen. Dies kann anderen Staaten signalisieren, wie Deutschland in bestimmten Fällen reagieren würde und wie andere Staaten mit der Bundeswehr koordinieren und kooperieren könnten. Deutschland könnte sich bei der Zusammenarbeit dann auf seine bestimmten Fähigkeiten konzentrieren und diese einbringen.

Zuletzt, ein übergeordnetes Ziel, welches im Weißbuch definiert wurde, drückt zum Beispiel aus, woran Deutschland bestimmte neue Maßnahmen messen könnte:

"Dabei ist Cybersicherheit in Deutschland der anzustrebende Zustand der IT-Sicherheitslage, in dem die Risiken, die Deutschland aus dem Cyberraum erwachsen, auf ein tragbares Maß reduziert sind. Cyberabwehr, Cyberverteidigung und Cybersicherheits- sowie -außenpolitik sind Mittel zum Erreichen dieses Zielzustandes."[25]

Bei neuen Maßnahmen sollte dann auch bewertet werden, inwieweit der Einsatz dieser Maßnahme den Zustand der IT-Sicherheitslage, in dem die Risiken, die Deutschland aus dem Cyberraum erwachsen, auf ein tragbares Maß reduziert. Zudem ist es eine Möglichkeit genauer zu definieren, inwieweit Risiken bei der Nutzung von offensiven Fähigkeiten durch die Bundeswehr bei Mandatsfällen mitigiert werden könnten[26].

Neben dem Risiko, dass zum Beispiel die eigene IT-Sicherheit durch offensive Maßnahmen geschwächt wird oder die Fähigkeiten der Bundeswehr gestohlen werden, ist auch ein Risiko, dass der Gegner auf Deutschlands Maßnahme mit einer Gegenmaßnahme reagiert. Solche Vergeltungsmaßnahmen könnten daher zu einer Eskalation führen und mehr Probleme verursachen. Nur Maßnahmen im Bereich Anforderung von Unterstützung bei der defensiven Cyberabwehr und Kapazitätsaufbau beinhalten kaum das Risiko einer feindlichen Reaktion.

Wenn das Weißbuch 2016 als Leitlinie gelten sollte, dann müsste Deutschland es auch bei der Cyberverteidungsstrategie anwenden. Gegebenenfalls müsste dann auch auf Maßnahmen verzichtet werden, die nicht mit dem Interesse und Deutschlands Rolle in der Welt, vereinbar sind. Zum Beispiel stellt sich die Frage, inwieweit aktive Cyberabwehr als Mittel zur Aufklärung oder Wirkung, wie es die USA macht, in das aktuelle

[23] Seit November 2020 arbeitet die Stiftung Neue Verantwortung an einem Projekt, welches den strategischen Rahmen, aktuelle Herausforderungen und mögliche Lösungsvorschläge zur Beantwortung von maliziösen Cyberaktivitäten identifizieren wird. Die Studie wird voraussichtlich im 2. Quartal 2021 erscheinen.
[24] BMVg (2016) Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr.
[25] BMVg (2016) Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr.
[26] Siehe dazu auch Sachverständigenstatement von Sven Herpig

sicherheitspolitische Selbstverständnis Deutschlands passen würde. “Unser Land ist in besonderem Maße auf gesicherte Versorgungswege, stabile Märkte sowie funktionierende Informations- und Kommunikationssysteme angewiesen.” Solche Maßnahmen birgen einige Risiken, die die Funktion von Informations- und Kommunikationssystemen destabilisieren könnten. Zudem ist bisher nicht belegt, dass sie den gewollten positiven Effekt auf Cybersicherheit tatsächlich erfüllen[27]. Außerdem müsste Deutschland bedenken, wie die Anwendung auf die Staaten wirkt, in denen diese Maßnahmen eingesetzt werden sollen. Das könnte zum Beispiel China und Russland betreffen. Wie würde eine solche Maßnahme in die Russlandpolitik Deutschlands passen? Wie erklärt Deutschland den Einsatz gegenüber diesem Staat?

Zusammenfassend stelle ich fest, dass einige neue Maßnahmen zum Beispiel im Bereich aktiver Cyberabwehr, sollten diese Anwendung finden, und die strategische Neuausrichtung anderer Staaten seit 2016, zum Beispiel der USA, bedeuten, dass auch Deutschlands Cyberverteidungsstrategie angepasst werden müsste. Diese müsste besser im Einklang mit Deutschlands sicherheitspolitischen Selbstverständnis stehen und zum Beispiel die genannten Inkonsistenzen adressieren. Dies ist insbesondere wichtig, da ein transparente und kohärente Strategie, die erklärt wie Deutschland agiert, auch förderlich sein kann für die Schaffung von Vertrauen und allgemein anerkannten Normen des Verhaltens im Cyberraum. Durch die Verbesserung der zwischenstaatlichen Zusammenarbeit, Transparenz und Vorhersehbarkeit des Verhaltens im Cyberraum seitens Deutschlands könnte auch das Risiko von Fehlwahrnehmung, Eskalation und Konflikten verringert werden.

[27] Ciaran Martin (2020): Cyber Attacks: What actual harm do they do?: “These days, the question is often asked: “what does the cyber domain mean for warfare?”. There is not enough attention paid to the question the other way round: how do we minimise the impact of digital harassment by adversaries on the domain of peaceful social and economic activity that is cyberspace? It is, to me, far from proven that escalating tensions in the so-called grey zone is an effective way of doing this.”