19. Wahlperiode

Deutscher Bundestag
Verteidigungsausschuss

Stenografisches Protokoll
der 80. Sitzung

Verteidigungsausschuss
Berlin, den 15. März 2021, 13.00 Uhr
Marie-Elisabeth-Lüders-Haus, Saal 3.101
10117 Berlin, Adele-Schreiber-Krieger-Straße

Vorsitz: Wolfgang Hellmich, MdB

Tagesordnung

Tagesordnungspunkt **Seite**

Öffentliche Anhörung

Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen

19. Wahlperiode

Deutscher Bundestag
Verteidigungsausschuss

Schriftliche Stellungnahme von FKpt Dr. Dr. habil. Robert Koch
Bundesministerium der Verteidigung

Schriftliche Stellungnahme von Dipl.-Inf. Thomas Reinhold
Technische Universität Darmstadt

Schriftliche Stellungnahme von Julia Schuetze
Stiftung Neue Verantwortung e. V.

Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
CDU/CSU	Brandl, Reinhard, Dr. Gädechens, Ingo Gnodtke, Eckhard Hahn, Florian Lamers, Karl A., Prof. h. c. Dr. Lehmann, Jens Manderla, Gisela Otte, Henning Schäfer, Anita Sensburg, Patrick, Prof. Dr. Siebert, Bernd Strenz, Karin Vieregge, Kerstin	Brand, Michael Grübel, Markus Grundmann, Oliver Hardt, Jürgen Irmer, Hans-Jürgen Kiesewetter, Roderich Kuffer, Michael Oster, Josef Stier, Dieter Wadephul, Johann, Dr. Weinberg, Marcus Willsch, Klaus-Peter Zeulner, Emmi
SPD	Brecht, Eberhard, Dr. Brunner, Karl-Heinz, Dr. Budde, Katrin Felgentreu, Fritz, Dr. Hellmich, Wolfgang Möller, Siemtje Vöpel, Dirk Weingarten, Joe, Dr.	Dittmar, Sabine Heinrich, Gabriela Hitschler, Thomas Klingbeil, Lars Schwarz, Andreas Stein, Mathias Völlers, Marja-Liisa Weber, Gabi
AfD	Elsner von Gronow, Berengar Lucassen, Rüdiger Nolte, Jan Otten, Gerold	Felser, Peter Hess, Martin Kestner, Jens Neumann, Christoph
FDP	Faber, Marcus, Dr. Müller, Alexander Sauter, Christian Strack-Zimmermann, Marie-Agnes, Dr.	Aschenberg-Dugnus, Christine Klein, Karsten Kober, Pascal Graf Lambsdorff, Alexander
DIE LINKE.	Buchholz, Christine Höhn, Matthias Neu, Alexander S., Dr. Pflüger, Tobias	Dağdelen, Sevim Hänsel, Heike Sommer, Helin Evrim Vogler, Kathrin
BÜNDNIS 90/DIE GRÜNEN	Brugger, Agnieszka Keul, Katja Lindner, Tobias, Dr.	Bayram, Canan von Holtz, Ottmar Nouripour, Omid

Eine Kopie der Unterschriftenliste der anwesenden Ausschussmitglieder ist dem Originalprotokoll als Anhang beigefügt.

Verzeichnis der Sachverständigen

Prof. Dr. Wolff Heintschel von Heinegg
Europa-Universität Viadrina

Dr. Sven Herpig
Stiftung Neue Verantwortung e. V.

Fregattenkapitän PD Dr. Dr. habil. Robert Koch
Bundesministerium der Verteidigung

Julia Schuetze
Stiftung Neue Verantwortung e. V.

Prof. Dr. Elmar Padilla
Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie

Vizeadmiral Dr. Thomas Daum
Inspekteur Kommando Cyber- und Informationsraum der Bundeswehr

Dipl.-Inf. Thomas Reinhold
Technische Universität Darmstadt

(Beginn: 12.59 Uhr)

Vorsitzender Wolfgang Hellmich: Meine sehr geehrten Damen und Herren! Liebe Kolleginnen und Kollegen! Ich eröffne die 80. Sitzung des Verteidigungsausschusses, zu der ich alle herzlich begrüße.

Einziger Tagesordnungspunkt ist heute:

> Öffentliche Anhörung
>
> Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen

Zunächst möchte ich alle Anwesenden darauf hinweisen, dass die heutige Anhörung zur Herstellung der Öffentlichkeit live im Internet auf www.bundestag.de und in der Bundestags-App übertragen wird. Im Anschluss ist die Aufzeichnung in der Mediathek des Deutschen Bundestages auf ewig abrufbar.

Vor Eintritt in die Tagesordnung erlaube ich mir, die vor Ort Anwesenden, diejenigen, die im Sitzungssaal sind, darauf hinzuweisen, entsprechende Mund-Nasen-Bedeckungen zu tragen. Bei allen anderen, die am Bildschirm sitzen, ist das nicht nötig. Ich bitte außerdem darum, die Masken auch bei den einzelnen Wegstrecken durch den Saal zu tragen.

Dann begrüße ich die Sachverständigen. Dies sind: Professor Dr. Wolff Heintschel von Heinegg von der Europa-Universität Viadrina, Professor Dr. Elmar Padilla, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie, Dr. Sven Herpig von der Stiftung Neue Verantwortung, Vizeadmiral Dr. Thomas Daum, Inspekteur Kommando Cyber- und Informationsraum der Bundeswehr, Fregattenkapitän Privatdozent Dr. Robert Koch vom Bundesministerium der Verteidigung - er sitzt vor Ort im Sitzungssaal -, Diplom-Informatiker Thomas Reinhold von der Technischen Universität Darmstadt - er ist ebenfalls vor Ort - und Frau Julia Schuetze von der Stiftung Neue Verantwortung. Ich danke Ihnen, dass Sie unserer Einladung zu dieser öffentlichen Anhörung nachgekommen sind, um die Fragen meiner Kolleginnen und Kollegen zu beantworten. Wir haben den Termin für diese Anhörung wegen der Coronapandemie ja schon häufiger verschieben müssen. Somit freue ich mich, dass er nun zustande gekommen ist und wir diese Anhörung durchführen können.

Begrüßen darf ich weiter die Vertreter des Bundesministeriums der Verteidigung sowie des Auswärtigen Amtes.

Es geht dem Ausschuss darum, sich einen Überblick über den aktuellen Diskussionsstand zur Thematik zu verschaffen. Bereits vor einigen Jahren haben wir eine solche Anhörung durchgeführt. Die Ergebnisse dieser Anhörung dienen dazu, die weiteren Beratungen im Ausschuss und auch in der Öffentlichkeit auf eine fundierte wissenschaftliche Grundlage zu stellen. Deshalb begrüße ich nochmals ganz herzlich die Sachverständigen.

Wir haben Ihnen mit dem Einladungsschreiben die Möglichkeit eingeräumt, eine schriftliche Stellungnahme zum Thema der Anhörung abzugeben. Für die eingegangenen Stellungnahmen, die an die Kolleginnen und Kollegen weitergeleitet worden sind, bedanke ich mich ganz herzlich. Diese Stellungnahmen werden am Ende dem Protokoll dieser Sitzung beigefügt.

Von der heutigen Sitzung wird ein Stenografisches Protokoll erstellt. Ich bitte Sie deshalb, bei jedem Wortbeitrag das Mikrofon zu benutzen sowie Ihren Namen zu nennen. Dies gilt auch für die per Videokonferenz zugeschalteten Teilnehmerinnen und Teilnehmer. Bitte versuchen Sie, soweit möglich, Hintergrundgeräusche zu vermeiden. Das neudeutsche Wort „unmuten“ kennt ja inzwischen jeder; es wird täglich mehrmals benutzt. Außerdem bitte ich Sie, Ihr Mikrofon nach dem Ende Ihres Beitrages wieder stumm zu schalten.

Für diese Anhörung haben wir die Zeit von 13 Uhr bis circa 17 Uhr vorgesehen.

Einleitend möchte ich den Sachverständigen Gelegenheit geben, in einer kurzen Erklärung von etwa fünf bis zehn Minuten zu dem Thema Stellung zu nehmen. Danach werden wir mit der Befragung durch die Fraktionen fortfahren.

Die Fraktionen im Verteidigungsausschuss haben sich einvernehmlich darauf verständigt, je nach Zeitverfügbarkeit bis zu drei Fragerunden durchzuführen, für die jeweils die sogenannte Berliner Stunde zugrunde gelegt wird. Das heißt, es beginnt die CDU/CSU-Fraktion mit 21 Minuten, gefolgt von der Fraktion der AfD mit 7 Minuten, der SPD-Fraktion mit 13 Minuten, der FDP-Fraktion mit 7 Minuten, der Fraktion Die Linke mit 6 Minuten und der Fraktion Bündnis 90/Die Grünen ebenfalls mit 6 Minuten. Innerhalb der Zeitkontingente bestimmen die Fraktionen eigenständig, wer eine Frage stellt und an wen sich die Frage jeweils richtet. Das Zeitkontingent umfasst dabei Fragen und Antworten. Bitte teilen Sie Ihre Wortmeldungen dem Vorsitzenden über den Chat mit, sobald Sie von der dem Sekretariat zur Verfügung gestellten Reihenfolge der Rednerinnen und Redner abweichen möchten.

Wir beginnen nun mit den Eingangsstatements der Sachverständigen. Wir gehen hierbei der Einfachheit halber nach der Reihenfolge auf der Tagesordnung vor. - Es beginnt Herr Professor Dr. Wolff Heintschel von Heinegg. Herr Professor, Sie haben das Wort.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Vielen Dank. - Herr Vorsitzender! Ich hoffe, dass ich gut zu verstehen bin. Wenn nicht, dann bitte ich um eine entsprechende Nachricht.

Ich habe mich in meiner Stellungnahme, wie Sie gesehen haben, sehr stark auf die Frage konzentriert, ob und unter welchen Voraussetzungen Operationen im oder durch den Cyberraum eine Gewaltanwendung im Sinne des Völkerrechts oder gar einen bewaffneten Angriff darstellen können. Wie Sie meiner Stellungnahme wohl auch entnommen haben, sieht es im Augenblick so aus, dass hier kein hinreichender Konsens unter den Staaten besteht, der ja auch dafür notwendig ist, zu klären, wie bestimmte Normen zu verstehen sind, und nicht nur dafür, zu klären, ob möglicherweise eine neue Gewohnheitsrechtsnorm entsteht. Das Beste, was wir festhalten können, ist, dass bestimmte Operationen durch den Cyberraum, die Wirkungen in der physischen Domäne zeitigen, die dem Einsatz traditioneller Mittel und Methoden der Kriegführung gleichkommen, als Gewaltanwendung und, wenn eine hinreichende Schwere gegeben ist, auch als bewaffneter Angriff eingeordnet werden können.

Allerdings darf in diesem Zusammenhang der schillernde Begriff der kritischen Infrastruktur auch nicht überbewertet werden, weil insoweit keine echte Einigkeit besteht. Hinzu kommt, dass in den zahlreichen nationalen Cybersicherheitsstrategien der Begriff der kritischen Infrastruktur unter einem, wenn Sie so wollen, multifunktionalen Ansatz verstanden wird. Das heißt, hier geht es auch um Kriminalitätsbekämpfung und um andere Fragen, nicht nur um solche der nationalen Sicherheit oder gar der nationalen Verteidigung oder der Bündnisverteidigung.

Ich will mich in meiner kurzen Eingangsstellungnahme aber nicht auf die Frage der Gewaltanwendung und die Frage der Selbstverteidigung beschränken; darauf bin ich, glaube ich, in meiner schriftlichen Stellungnahme ausführlich genug eingegangen.

Worüber wir uns klar werden müssen, ist die Frage, wie es sich mit Operationen im und durch den Cyberraum verhält, die unterhalb der Gewaltschwelle verbleiben. Es gibt eine Vielzahl von solchen Beispielen. Dazu zählen nicht nur die Versuche, etwa Daten des Deutschen Bundestages abzuzapfen in einer Art und Weise, die die Funktionalität des IT-Systems des Bundestages nachhaltig gestört hat, mit der Folge, dass sogar die Hardware ausgetauscht werden musste, sondern natürlich auch eine Vielzahl weiterer Operationen, die auch gegen private Akteure oder private Unternehmen gerichtet sind. Ich glaube, wir müssen uns darüber Gedanken machen, ob und wie wir solche Cyberoperationen rechtlich einordnen. Ich glaube, das ist durchaus möglich. Es ist nicht unbedingt erforderlich, hier besondere neue völkerrechtliche Regeln zu schaffen.

Entscheidend aber ist, dass wir bei Souveränitätsverletzungen, egal in welcher Form und in welchem Ausmaß, klar- und deutlich machen, dass wir solche Souveränitätsverletzungen als nicht im Einklang mit dem Völkerrecht stehend begreifen. Es ist wichtig, nicht einfach zur Tagesordnung überzugehen und nicht sozusagen schulterzuckend hinzunehmen, dass man mal wieder Opfer einer Cyberoperation geworden ist, die selbstverständlich den selbstgeschaffenen Verwundbarkeiten geschuldet ist. Das gilt es immer wieder im Hinterkopf zu behalten.

Es ist auch nicht damit getan, die Rufe nach Resilienz usw. zu verstärken. Wir müssen hier sehr viel weitergehen und müssen, wenn Sie so wollen, unsere forensischen Fähigkeiten im Cyberraum deutlich ausbauen. Aber wenn wir nicht bereit sind, gegen die Bundesrepublik Deutschland gerichtete maliziöse Cyperoperationen auch rechtlich beim Namen zu nennen, dann, meine ich, machen wir einen erheblichen Fehler. Bei Verletzung unserer territorialen Souveränität, bei der nachhaltigen Beeinträchtigung von Staatsfunktionen, bei Beeinträchtigungen des Gesundheitswesens, der Energieversorgung müssen wir, wenn Sie mir diesen saloppen Ausdruck erlauben, klare Kante zeigen; denn wenn wir dies nicht tun, wird man die Bundesrepublik Deutschland auch in diesem Bereich nicht ernst nehmen.

Selbstverständlich müssen wir berücksichtigen, dass die Bundesrepublik Deutschland, was Cyberkapazitäten und -fähigkeiten anbelangt, nicht notwendigerweise in der ersten oder in der zweiten Liga spielt. Andere Staaten sind uns meilenweit voraus, und wir müssen einfach zur Kenntnis nehmen, dass die Staaten, die uns so weit voraus sind, von diesen Möglichkeiten und Fähigkeiten notfalls auch Gebrauch machen werden. Wir werden fast täglich Zeuge von Cyberoperationen, wahrscheinlich von anderen Staaten, die gegen die Bundesrepublik Deutschland gerichtet sind. Dagegen können wir zurzeit nicht viel tun - wie gesagt, das ist größtenteils selbstverschuldet -; aber wir müssen, was die rechtliche Einordnung anbelangt, wenigstens eine klare Linie ziehen und eine klare Position beziehen.

In diesem Zusammenhang müssen wir uns auch darüber im Klaren sein - damit komme ich zum Schluss meiner Eingangsstellungnahme -, dass die leidige Diskussion über die Unterscheidung zwischen offensiven und defensiven Cyberoperationen nicht allzu viel Sinn macht. Allein die Tatsache, dass eine Cyberoperation gegen einen bestimmten Akteur gerichtet ist, bedeutet noch nicht, dass sie offensiven Charakters ist. Oder wenn eine Operation „allein der Abwehr eines Cyberangriffs“ - in Anführungsstrichen - dient, ist sie nicht rein defensiv, und häufig kann sie auch gar nicht rein defensiv sein. Wir werden uns hier auch darüber klar werden müssen, ob und inwieweit wir bereit sind, unsere Fähigkeiten im und durch den Cyberraum zu verbessern. Damit, Herr Vorsitzender, komme ich zum Ende meines Eingangsstatements. - Ich danke Ihnen.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Professor von Heinegg. - Dann hat Herr Professor Padilla das Wort.

Sachverständiger Prof. Dr. Elmar Padilla (Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie): Vielen Dank. - Ich werde mich in meinem Statement daran orientieren, was wir als Fragenkatalog bekommen haben. Wegen meines Hintergrundes werde ich eher auf die technischen Fragen und nicht so sehr auf die rechtliche Fragestellung eingehen.

Ich fange an mit den Möglichkeiten, die ich bei Cyberoperationen sehe. Diese sind vielfältig.

Zum einen sehe ich die große Möglichkeit, dass man militärische Operationen über Cyberoperationen a) besser vorbereiten und b) effizienter durchführen kann, also dass man darüber die Wahrscheinlichkeit für eine erfolgreiche Durchführung und letztlich für die Erreichung des Missionsziels erhöhen kann.

Des Weiteren bieten in meinen Augen Cyberoperationen die Möglichkeit, menschliche Verluste zu minimieren, sei es bei eigenen Kräften, bei feindlichen Kräften oder auch bei zivilen Personen im Operationsgebiet. Denn letztlich geht es bei einer militärischen Operation ja darum, dass

man feindliche Systeme durchaus ausschalten möchte.

Dann stellt sich die Frage nach der Alternative. Wenn die Alternative darin besteht, mit einem kinetischen Wirkmittel zu operieren oder mit einer Cyberoperation das gleiche Ziel zu erreichen, dann ist es, glaube ich, offensichtlich, dass die Wahrscheinlichkeit, menschliche Verluste in Kauf nehmen zu müssen, so deutlich geringer ist.

Das Vierte ist, dass eine Cyberoperation potenziell auch eine abschreckende Wirkung haben kann. Natürlich habe ich die SWP-Studie gelesen. Im Moment, da wir mit der Attribuierung einfach nicht gut genug sind, ist hier ein gewisses Abschreckungspotenzial genommen, einfach weil man das nicht gut zuordnen kann. Nichtdestotrotz bieten Cyberoperationen, wenn man über Möglichkeiten redet, logischerweise auch die Möglichkeit der Abschreckung.

Nächster Punkt. Wenn man in Richtung von Info Ops, also Information Operations, denkt, sieht man: Cyberoperationen bieten die Möglichkeit, Akzeptanz und Unterstützung eigener Operationen herbeizuführen. Wenn man es zum Beispiel mit feindlicher Propaganda zu tun hat, dann kann man dem ein eigenes Narrativ entgegenstellen. Letztlich ist natürlich die Bekämpfung von Cyberkriminalität, -spionage im Sinne von gesamtstaatlicher Cyberabwehr auch noch eine Möglichkeit für das, was man mit Cyberoperationen erreichen kann. - Das sind also die Möglichkeiten.

Natürlich sind dem auch gewisse Grenzen gesetzt. Insbesondere, denke ich, sollte man unterscheiden zwischen reinen Cyberoperationen und cyberunterstützten Operationen. Also, wenn ich an militärische Operationen denke, sehe ich den großen Mehrwert eher in Richtung der cyberunterstützten Operationen. Bei reinen Cyberoperationen ist man mit seinem Wirken erst einmal vordringlich auf den Cyber- und Informationsraum beschränkt. Das heißt, wenn man da eine weitergehende Wirkung erzielen will, muss man schon einen vergleichsweise hohen Aufwand betreiben.

Was man sich beim Thema Grenzen noch bewusst machen muss, ist: Wenn man Cyberoperationen und deren Potenzial nutzen will, dann braucht man eine hohe Geschwindigkeit, Flexibilität und Reaktionsfähigkeit. Das heißt, wenn man dem Ganzen einen sehr schwerfälligen Prozess vorschaltet, dann nimmt man sich selbst sehr viele Möglichkeiten, die Cyberoperationen eigentlich bieten würden.

Was man bei dem Ganzen natürlich auch beachten muss, ist die Verhältnismäßigkeit. Also, man sollte schon darüber nachdenken, dass es potenziell auch Kollateralschäden geben kann; mein Vorredner hat das gerade schon angesprochen. Wenn man - Beispiel Energieversorgung - versucht, über eine Cyberoperation die Energieversorgung eines Landes lahmzulegen, dann ist, glaube ich, unmittelbar offensichtlich, dass das größere Kollateralschäden mit sich bringt. Dann muss man sich fragen, ob das mit Blick darauf, was man erreichen will, verhältnismäßig ist.

Die nächste Grenze würde ich unter dem Begriff „Kaltstartfähigkeit“ fassen. Sie müssen sich bewusst machen: Wenn Sie sich heute überlegen, eine Cyberoperation durchzuführen, dann können Sie nicht einfach loslegen, sondern so etwas müssen Sie vorbereiten. Dann müssen Sie entsprechende Kapazitäten vorhalten. Sie müssen auch im Vorfeld eine Aufklärung durchführen. Das will heißen: Vorbereitungen müssen Sie im Zweifel schon in Friedenszeiten tätigen. Und was man nicht verhehlen sollte, ist: Einen gewissen Aufwand hat das Ganze natürlich auch. Wir reden hier ja schon über Operationen. Wie bei jeglichen anderen militärischen Operationen auch bringt das natürlich einen gewissen Aufwand mit sich. - So viel in meinem Eingangsstatement zu Möglichkeiten und Grenzen.

Kurz möchte ich noch das Thema Lage streifen. Das war auch noch eine Frage: Welche Bedeutung hat die Lage? Ich würde sagen: natürlich eine entscheidende; denn die Lage ist die Basis zielgerichteten Handelns. Also sollte man schon gute Informationen darüber haben, welche Gruppierungen mit welchen Fähigkeiten gerade welche Kampagnen durchführen, so im Sinne von „Kenne deinen Feind - know your enemy“. Und

es ist für Operationen natürlich sehr wichtig, zu wissen, wie denn so die Stimmungslage ist, das heißt, wie die Stimmung hinsichtlich der eigenen Operation ist, wie es im Operationsland aussieht. Gegebenenfalls sollte man, wie ich gerade schon gesagt habe, auch darüber nachdenken, ob es nicht sinnvoll ist, zu versuchen, die Stimmung aktiv zu beeinflussen, also quasi ein eigenes Narrativ zu platzieren.

Zu Besonderheiten von Cyberwirkmitteln gab es auch eine Frage. Drei Gedanken dazu:

Zum einen müssen Sie sich darüber klar sein, dass so ein Cyberwirkmittel, wie wir es nennen, halt nicht wieder weggeht. Das heißt, es bleibt, und es ist kopierbar. Sie können davon ausgehen, dass das über die Zeit irgendwann zu so einer Art Commodity Software wird. Also, Sie können nicht davon ausgehen, dass Sie das auf ewig werden geheim halten können. Irgendwann wird das bekannt werden.

Zum Zweiten. Denken Sie zum Beispiel an eine Rakete. Sie können mit höherer Wahrscheinlichkeit davon ausgehen, dass sie irgendwann explodiert. Bei einem Cyberwirkmittel wissen Sie das nicht so genau. Es kann sein, dass es gar nicht funktioniert, weil das Zielsystem inzwischen geändert worden ist. Es kann sein, dass es einmal funktioniert. Es kann sein, dass es ganz häufig funktioniert. Sie haben also eine hohe Unsicherheit über das Zeitfenster, in dem Ihr Cyberwirkmittel nutzbar sein wird.

Was man sich dann noch bewusst machen muss, ist: Solche Wirkmittel sind nicht rein in militärischer oder regulierter Hand. Im Prinzip kann jeder, der Software schreiben kann, auch eine Malware schreiben. Und letztlich kann man - das hatte ich gerade schon kurz erwähnt - in bestimmten Fällen ein Cyberwirkmittel als Ersatz für ein kinetisches Wirkmittel nehmen.

Das letzte Thema aus dem Fragenkatalog, das ich noch streifen möchte, ist: Was sind Maßnahmen zur Verbesserung? Ich bin ein Fan davon, das Ganze als einen Dreiklang zu sehen aus Prävention, Detektion und Reaktion.

Bei Prävention haben die meisten auf dem Schirm, zu versuchen, die Angriffsfläche zu minimieren. Da ist man dann bei Ansätzen wie Mikrokernel, Virtualisierung, Security über Default oder so etwas. Was in meinen Augen aber auf jeden Fall dazugehören sollte, ist Transparenz. Sie können in Richtung Automatisierung von Sicherheitstests gehen, um tatsächlich überhaupt eine Transparenz zum Sicherheitszustand Ihrer Systeme zu erhalten. Da sind wir im Moment immer noch nicht sonderlich gut; da gibt es in meinen Augen noch Arbeit und Forschungsbedarf.

Bei Detektion sind die Ansätze aktuell verschiedene: KI, Kill-Chain-basierte Korrelation von Einzelevents.

Was häufig noch als Stiefkind behandelt wird, ist die Reaktion. Erst einmal müssen wir uns klarmachen: Egal was wir bei Prävention und Detektion treiben, wir werden keine hundertprozentige Sicherheit erreichen. Wir müssen uns also schon eine Reaktion überlegen. Wir brauchen - das ist der klassische Weg - Antworten auf die sogenannten W-Fragen: Was ist passiert? Welche Daten sind abgeflossen? Welche Systeme sind betroffen? Welche Werkzeuge wurden eingesetzt? Und - das ist ganz zentral -: Wer war es?

Da sind wir wieder bei der Attributionsthematik. Damit komme ich dann auch zum Ende. Ich glaube nämlich, Attribution ist eine der dringendsten Fragen, wenn nicht sogar die dringendste Frage, die wir eigentlich lösen müssten. Wir brauchen ganz klar eine eindeutige und unabstreitbare Attribution. Wenn wir das nicht geregelt kriegen, dann laufen viele der möglichen Maßnahmen einfach dadurch ins Leere, dass für den Angreifer der Erwartungswert immer enorm hoch ist. Also, wenn Sie keinerlei Repression zu befürchten haben und was zu gewinnen haben, dann ist Ihr Erwartungswert natürlich entsprechend hoch und dann sind die Leute eher nicht gewillt, sich an Regeln, die man dann lustig definiert, zu halten. - Das sollte es von mir erst einmal gewesen sein. Danke schön und bis später.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Padilla. - Dann gebe ich das Wort an Herrn Dr. Sven Herpig zu seinem Beitrag.

Sachverständiger Dr. Sven Herpig (Stiftung Neue Verantwortung e. V.): Vielen Dank. - Lieber Vorsitzender! Liebe Abgeordnete! Liebe Menschen! Ich stelle gleich mal die drei wichtigsten Punkte voran:

Erstens. Die IT- und Cybersicherheit in Deutschland wird durch den Einsatz von offensiven intrusiven Maßnahmen im Cyberraum durch die Bundeswehr nicht erhöht. IT- und Cybersicherheit in Deutschland können nur durch den Einsatz defensiver Maßnahmen nach Subsidiaritätsprinzip mit Unterstützung der entsprechenden Behörden und flankiert von Legislativvorhaben erhöht werden.

Zweitens. Ziel einer Cyberoperation ist die Unterscheidung zwischen oft geduldeter Spionage und der Vorbereitung einer militärischen Aktivität, sogenanntes Pre-Positioning; dies ist schwierig zu erkennen. Es muss daher eine klare Strategie der Bundesregierung für den Einsatz offensiver intrusiver Maßnahmen der Bundeswehr geben, und die Strategie muss anderen Ländern kommuniziert werden, um Missverständnisse und Eskalationsspiralen zu vermeiden.

Drittens. Der Einsatz von Cyberwirkmitteln ist lediglich eine Ergänzung zu weiteren Wirkmitteln und muss domänenübergreifend gedacht und in eine gesamtstaatliche Strategie eingebettet werden.

Jetzt ein wenig zur Rolle der Bundeswehr. Die Rolle der Bundeswehr bei der gesamtstaatlichen Sicherheitsvorsorge im Bereich „Cybersicherheit in Friedenszeiten“ ist verfassungsrechtlich in der Praxis bisher hauptsächlich auf den Eigenschutz, also auf defensive Aktivitäten, begrenzt. Auf Basis der Anzahl und Heterogenität der eigenen IT-Systeme der Bundeswehr ist dies eine sinnvolle Nutzung der vorhandenen Ressourcen zur Steigerung der Resilienz der Bundeswehr-IT und über die Lagebilderstellung und Übermittlung an das Bundesamt für Sicherheit in der Informationstechnik auch für die IT-Infrastrukturen in Deutschland allgemein.

Zukünftig könnte die Möglichkeit der Amtshilfe durch die Bundeswehr bei schweren Cybervorfällen noch weiter beleuchtet werden, zum Beispiel durch konkrete Einsatzszenarios.

Die Grenze zwischen defensiv und offensiv - sie wurde ja gerade schon genannt - wird im Cyberraum in der Regel dann überschritten, wenn die getätigten Maßnahmen nicht mehr die eigenen Systeme, sondern Systeme von Dritten und/oder Systeme des intendierten Ziels betreffen. Innerhalb offensiver Maßnahmen wäre eine trennscharfe Grenze zwischen Informationsgewinnung auf der einen und Aufklärung und Wirkung auf der anderen Seite dann gegeben, wenn die IT-Schutzziele, also Vertraulichkeit, Integrität und Verfügbarkeit, der Zielsysteme beeinträchtigt und Sicherheitsmechanismen ausgehebelt werden. Solange das nicht der Fall ist, zum Beispiel durch Portscans, ist die Maßnahme nicht intrusiv, trotzdem offensiv, und es kann von Informationsgewinnung im Sinne der technischen Sondierung gesprochen werden. Dies kann auch dann der Fall sein, wenn zwar das Schutzziel Vertraulichkeit verletzt wird, aber das Zielsystem über keinerlei Sicherheitsmechanismen verfügt, die ausgehebelt werden müssen, zum Beispiel bei falsch konfigurierten Cloud-Storage-Systemen.

Informationsgewinnung dient zur Identifikation von möglichen Zielsystemen und ihren Schwachstellen sowie - es wurde gerade schon genannt - zur Formulierung der Einsatzgrundsätze und Auswahl der Wirkmittel. Das daraus resultierende Wissen bildet die Grundlage, um die eigenen intrusiven offensiven Maßnahmen für Aufklärung und Wirken vorzubereiten, die im Spannungs- und Verteidigungsfall, also im Rahmen der Landes- und Bündnisverteidigung, sowie bei Auslandsmandaten zum Einsatz kommen. Hierfür müssen zum Beispiel Exploits entwickelt und beschafft und in Offensivwerkzeuge und Plattformen integriert werden. Es ist daher unentbehrlich, eine Folgenabschätzung für Cyberwirkmittel anzufertigen, die über den Einsatz hinausgeht, zum Beispiel: Von welchen Firmen

kauft die Bundesrepublik Angriffswerkzeuge und Exploits? Mit welchen anderen Akteuren und Regimen handeln diese Firmen noch, und was bedeutet es, wenn wir diese Firmen aus Steuergeldern bezahlen?

Strategisch müsste zusätzlich analysiert werden, ob die Notwendigkeit besteht, unbekannte Schwachstellen, sogenannte Zero-Days, für den Einsatz gegen Hochwertziele zu nutzen, oder ob bekannte und sich im Disclosure-Prozess befindliche Schwachstellen mit einem durchschnittlichen Window of Exposure von circa 70 Tagen nicht ausreichend sind, um den Einsatz durchzuführen.

Aufklärung und Wirkungen im Cyberraum sollten dem Parlamentsvorbehalt unterliegen. Für Aufklärung könnte alternativ möglicherweise auch die Parlamentszustimmung im vereinfachten Verfahren vorgesehen werden. Dieses Verfahren könnte auch bei der Informationsgewinnung Anwendung finden, während hier ein Parlamentsvorbehalt möglicherweise nicht zwingend notwendig ist.

Es ist zwar begrüßenswert, dass die Bundesregierung die Anwendbarkeit der UN-Charta, des Völkergewohnheitsrechts und des humanitären Völkerrechts auf im Cyberraum anerkennt; jedoch sollte sie dringend prüfen, ob man auf Basis der Gegebenheiten des Cyberraums nicht weitergehen müsste. Im aktuellen Positionspapier der Bundesregierung „On the Application of International Law in Cyberspace“ wird zum Beispiel beschrieben, dass eine Cyberoperation gegen kritische Infrastrukturen in Friedenszeiten nicht immer auch eine Gefährdung der Souveränität darstellt und dass der Einsatz einer wurmfähigen Schadsoftware in zivilen Infrastrukturen gemäß humanitärem Völkerrecht legitim wäre, wenn sie ihre Wirkung wirklich nur bei den militärischen Zielen entfaltet.

Beide Beispiele sind vermutlich völkerrechtlich dogmatisch vertretbar, unter anderem wegen der Verharmlosung von Cyberoperationen gegen kritische Infrastrukturen. Aber man sollte bei der Nutzung von gefährlichen wurmfähigen Zero-Days zurückhaltend agieren, um nicht intendierte Kollateralschäden zu vermeiden. Dies sollte keine Einsatzgrundlage der Bundeswehr im Cyberraum darstellen. Deutschland muss hier mutiger werden und sollte sich nicht nur daran halten, was rechtlich zulässig ist, sondern Rahmenbedingungen kreieren, die normativ sinnvoll für die Stabilität des Cyberraums sind.

Als letzter Punkt ist es wichtig, anzuerkennen, dass die bisherige und die aktuelle Cybergefährdungslage in Deutschland fast ausschließlich von organisierter Kriminalität und Nachrichtendiensten und Geheimdiensten geprägt ist. Um diesen Aktivitäten entgegenzuwirken, muss die Bundesregierung gesamtstaatlich IT-Sicherheit und Resilienz fördern. Da der Bundeswehr als Teil dieses Ansatzes vor allem die Rolle des Eigenschutzes und gegebenenfalls der Amtshilfe zukommt, sollte hier auch der politische und organisatorische Fokus liegen und nicht auf offensiven intrusiven Cyberfähigkeiten. Für Sicherheit im Cyberraum gilt: IT-Sicherheit und Resilienz sind die beste Verteidigung. - Vielen Dank.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Herpig. - Dann hat der Vizeadmiral Dr. Thomas Daum das Wort. Bitte sehr, Herr Admiral.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur Kommando Cyber- und Informationsraum der Bundeswehr): Vielen Dank, Herr Vorsitzender. - Ich hoffe, ich bin zu hören. Könnte ich ein Signal bekommen? - Ja, ich sehe Nicken.

Verehrte Abgeordnete! Als meinen Einstieg in die heute vorwiegend rechtlich geprägte Anhörung möchte ich zu Ihrer Diskussion in der gebotenen Kürze einige grundsätzliche Aspekte zum militärischen Cyber- und Informationsraum beitragen, die ich dann natürlich bei Interesse in der Fragerunde gerne vertiefe.

Das Thema Bedrohung will ich vor die Klammer ziehen. Jede vernetzte Gesellschaft bietet zahlreiche Einfallstore für hybride Bedrohung, und dabei kann jeder Aspekt des politischen, gesellschaftlichen, kulturellen und wirtschaftlichen Lebens zur Angriffsfläche werden. Diese Anfälligkeit bedeutet enorme Risiken für die äußere

und innere Sicherheit, aber auch für die politische Entscheidungs- und Handlungsfähigkeit.

Dass der Cyber- und Informationsraum keine Grenzen aufweist und dass damit die Abgrenzung von innerer und äußerer Sicherheit verschwimmt, ist wohl anerkannt. Daraus ergeben sich beträchtliche Herausforderungen auch für die Bundeswehr. Aus militärischer Sicht ist die hybride Kriegführung das wahrscheinlichste, aber auch das komplexeste Szenario zukünftiger Konflikte. Zugleich ist aber die hybride Einflussnahme, also Aktivitäten unterhalb der Schwelle zur Gewaltanwendung, als Vorstufe eines Konflikts genauso relevant. Vielleicht bleibt es sogar bei dieser Stufe, wenn die Einflussnahme schon den gewünschten Zweck erfüllt. Das bedeutet ein erhebliches Erkenntnisinteresse der Bundeswehr gerade bezüglich des Aufklärens solcher Absichten und Aktivitäten.

Das Thema Recht will ich ebenso kurz vor die Klammer ziehen. Nach meinem Verständnis vertritt Deutschland die feste Auffassung, dass das Völkerrecht, einschließlich der Charta der Vereinten Nationen und des humanitären Völkerrechts, vorbehaltlos auf die Aktivitäten der Staaten im Cyberspace Anwendung findet und dass natürlich das Völkerrecht im internationalen Kontext insoweit von besonderer und entscheidender Bedeutung ist.

Ich will als ersten Aspekt auf das Verständnis des Cyber- und Informationsraums als eigene militärische Dimension eingehen. Dieser besteht - Sie kennen unsere Definition - aus dem Cyberraum, dem elektromagnetischen Umfeld sowie dem Informationsumfeld. Wir sprechen in Deutschland vom Cyber- und Informationsraum. Einige Partnernationen sprechen nur vom Cyberraum. Ich will aber den Anteil Informationsraum betonen. Ein zentraler Faktor in allen Konfliktformen sind die Menschen, die Informationen aufnehmen, miteinander teilen, austauschen und sie schließlich zur Grundlage ihrer eigenen Einstellung und ihres Handelns machen. Hier haben potenzielle militärische Gegner Möglichkeiten, schon im Rahmen hybrider Einflussnahme Stimmung zu machen oder im Rahmen hybrider Kriegführung konsequent auf Zielgruppen einzuwirken und Einfluss zu nehmen. Deshalb ist das Informationsumfeld ein wesentliches militärisches Handlungsfeld im militärischen Cyber- und Informationsraum.

Daneben gilt natürlich für den Cyberraum: Digitalisierung birgt bei allen Vorteilen auch eine Vielzahl von potenziellen Gefahren. Das gilt natürlich ebenso für den militärischen Bereich, für das digitalisierte Gefechtsfeld, für Battle-Management-Systeme und für vernetzte Waffensysteme und -plattformen. Hierfür steht bekanntlich das C in CIR als zweites wesentliches Handlungsfeld.

Mein zweiter Impuls soll die Prioritäten im CIR herausarbeiten. Meine Kernaufträge als Inspekteur Cyber- und Informationsraum sind natürlich der Betrieb und Schutz der eigenen Systeme sowie die Aufklärung von gegnerischen militärischen Potenzialen. Den gegnerischen Absichten stellen wir dann, wenn erforderlich, das Wirken gegen gegnerische Ziele als weiteren Kernauftrag entgegen. Ein umfassender Kernauftrag ist die Unterstützung aller anderen Teilstreitkräfte, der anderen Organisationsbereiche mit IT, mit IuK, wenn es sein muss mit operativer Kommunikation und allen Geoinformationen.

Im Vordergrund unserer Aktivitäten als militärischer Org-Bereich steht dabei zum einen der Schutz unserer eigenen IT-Systeme, also ganz generell die Informationssicherheit in der Bundeswehr; denn unsere Abhängigkeit von IT-basierter Infrastruktur fordert eine angemessene Verteilungsfähigkeit. Die Bundeswehr benötigt zur Erfüllung dieser Aufgabe im CIR natürlich alle verfügbaren Mittel und Möglichkeiten, insbesondere auch im äußersten Fall, nämlich der Kriegführung in der Dimension CIR.

Im Vordergrund steht aber genauso der Anteil der Aufklärung im CIR. Aufklärungsmaßnahmen kommt eine wesentliche Bedeutung zu. Es gilt, gegnerische Fähigkeiten, Potenziale und militärische Absichten und Aktivitäten fremder Staaten aufzuklären und Angriffsvorbereitungen möglichst frühzeitig zu erkennen. Das Ziel ist also hierbei, bereits im Vorfeld eines bewaffneten Konflikts die eigene Verteidigungsfähigkeit zu erhalten bzw. zu erhöhen. Deshalb sind beide

Aufgaben, Schutz und Aufklärung, bei uns auch „Daueraufträg 24/7“, wie wir das bezeichnen.

Ich will nun die wesentlichen Charakteristika von Cyberwirkmitteln noch einmal anreißen; das haben meine Vorredner ja auch schon getan. Auf die in der Bundeswehr gültige Unterscheidung zwischen defensiven und offensiven Cyberwirkmitteln will ich hier gar nicht weiter eingehen.

Aus meiner Sicht haben Cyberwirkmittel den Vorteil, dass sie in der Regel speziell für ein Zielsystem und einen Effekt vorbereitet werden können. Damit können sie letztlich auch eine Bandbreite einnehmen von „chirurgisch präzise“ bis „breit gestreut“ und hoffentlich exakt das bewirken, was zur Zielerreichung erforderlich ist. Je präziser, je vorsichtiger und je kontrollierter dabei das Vorgehen ist, umso geringer ist die Wahrscheinlichkeit von Kollateralschäden.

Im Grunde weisen Cyberwirkmittel also Charakteristika auf, die an herkömmliche konventionelle Wirkmittel erinnern. Natürlich liegt in dem Vorteil auch eine Schwäche; denn einen Effekt vorbereiten zu müssen, bedingt stets einen zeitlichen Vorlauf. Grundsätzlich sind die Maßnahmen durchaus reversibel, aber das bedingt natürlich, dass man den Zugang zu einem Zielsystem entsprechend erhalten muss.

Ich will nun noch auf einige grundlegende Vorgaben und daraus folgende Ableitungen für die Bundeswehr eingehen. Möglichkeiten und Grenzen militärischer Operationen sind natürlich genau an solchen Vorgaben zu bemessen. Der grundgesetzlich festgelegt Zweck für die Aufstellung deutscher Streitkräfte ist die Verteidigung. Dafür sind Vorbereitungen zu treffen und auf einen möglichen Gegner hin auszurichten. Das setzt voraus, dass man technisch auf dem neuesten Stand der Entwicklung ist und auch hinsichtlich der personellen Fähigkeiten auf der Höhe der Zeit agieren kann. Es gilt insoweit - Stichwort: Aufklärung -, fortlaufend Erkenntnisse über potenzielle gegnerische Zielsysteme und deren Schwachstellen zu gewinnen, um handlungsfähig zu sein, wenn es erforderlich ist. Es geht also letztlich darum, dem Auftrag der Streitkräfte gerecht zu werden.

Unbenommen davon muss die Bundeswehr auch im Frieden in der Lage sein, sich gegen Cyberangriffe von unterschiedlichen Akteuren zur Wehr zu setzen. Ich greife hier noch einmal den Aspekt des Verschwimmens von äußerer und innerer Sicherheit auf. Die Cybersicherheit Deutschlands mit dem Teilauftrag Cyberverteidigung für die Bundeswehr kann nur in einem gesamtstaatlichen Ansatz aller zuständigen Ressorts tragfähig sein. Mit dem Nationalen Cyber-Abwehrzentrum besteht hier ein Kernelement der nationalen Cybersicherheitsstrategie für den ressort- und behördenübergreifenden Austausch. Sie wissen das.

Eine reaktive Handlungsfähigkeit ist auch grundsätzlich gegeben. Doch eine schnelle Reaktionsfähigkeit und eine koordinierte Krisenbewältigung sind aus meiner Sicht das noch zu erreichende notwendige Ziel, damit wir in nationalen IT-Krisenlagen unmittelbar reagieren und diese hoffentlich auch bewältigen können.

Um hier ganz klar dem Argwohn sozusagen nicht zu entsprechen: Nicht die Teilhabe, aber ein mögliches Agieren der Bundeswehr innerhalb des Cyber-Abwehrzentrums ist natürlich an Voraussetzungen gebunden, beispielsweise an Artikel 35 Grundgesetz. Das ist klar.

Ich schließe mit der Feststellung, dass die Möglichkeiten und Grenzen eigener militärischer Cyberoperationen gleichermaßen durch politische, aber vor allem rechtliche Rahmenbedingungen bestimmt werden. Dazu gehören grundsätzliche Vorgaben wie aber auch Vorgaben für konkrete militärische Operationen.

Verehrte Abgeordnete, ich hoffe, meine Gedanken geben Ihnen Impulse für Ihre wichtige Diskussion zu den verfassungs- und völkerrechtlichen Fragen im militärischen Cyber- und Informationsraum. Ihre Diskussion ist nach meiner Auffassung für die Bundeswehr zu begrüßen und für alle, insbesondere für die mir als Inspekteur CIR anvertrauten Soldatinnen und Soldaten, wichtig. Alle Soldatinnen und Soldaten und ganz besonders die CIR-Kräfte erwarten nämlich zu Recht, dass sie bei jedem Einsatz auf dem festen

Boden des Völkerrechts und des Verfassungsrechts stehen. Militärische Handlungssicherheit kann immer nur durch Rechtssicherheit entstehen.

Ich bedanke mich für Ihre Aufmerksamkeit und gebe zurück zu Ihnen, Herr Vorsitzender.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Admiral. - Dann hat als Nächster der Fregattenkapitän Dr. Koch das Wort. Bitte sehr.

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (Bundesministerium der Verteidigung): Vielen Dank. - Sehr geehrter Herr Vorsitzender! Sehr geehrte Abgeordnete! Ich möchte zu Beginn der Anhörung und unserer Diskussion vier Aspekte kurz beleuchten: die Rolle von und den Umgang mit Schwachstellen in IT-Systemen, die Bedeutung des gesamtstaatlichen Ansatzes bei der Cybersicherheit, die Möglichkeiten und Grenzen der Resilienz und schließlich die Bedeutung solcher Aspekte für Cyberoperationen.

Schwachstellen in IT-Systemen spielen für militärische Cyberoperationen eine wichtige Rolle, aber natürlich nicht nur da. Beispielsweise werden auch im Bereich der Cyberkriminalität Schwachstellen ausgenutzt. Dies führt häufig dazu, dass Forderungen nach einer strikten Verpflichtung zur Offenlegung aller entdeckten Schwachstellen aufkommen, mit der Argumentation, dass eine Zurückhaltung der Sicherheit abträglich sei und zu umfassenden negativen Konsequenzen führe.

Dabei werden häufig Beispiele wie die Schadstoffsoftware WannaCry oder NotPetya genannt, die sich mittels des öffentlich gewordenen EternalBlue Exploits der NSA weltweit verbreiten konnten. Schaut man diese Vorfälle jedoch genauer an, zeigt sich, dass zu den jeweiligen Angriffszeiten der Hersteller längst informiert war und auch schon Patches längst bereitgestellt hatte, jedoch zunächst nur für die noch unterstützten Betriebssystemversionen. Dies zeigt insbesondere, dass das eigentliche Problem nicht im Abhandenkommen und der Veröffentlichung des Angriffscodes lag, sondern in der Herausforderung der Schließung von Schwachstellen in der Praxis, selbst bei einem vorhandenen Patch.

Die jüngsten Angriffe auf MS Exchange unterstreichen dies noch mal. Während Microsoft bereits am 5. Januar 2021 über entsprechende Angriffsmöglichkeiten informiert wurde, war eine Behebung der Schwachstelle im Rahmen des Patchdays Anfang März geplant. Durch die massiven Angriffe Ende Februar wurde dies etwas vorgezogen. Es sind aber bereits viele Systeme betroffen. Nach den USA ist Deutschland hier als Land mit der zweithöchsten Zahl zu nennen, und das BSI hat ja auch entsprechend zum zweiten Mal überhaupt eine Warnung der Stufe Rot, der Stufe 4, verschickt.

Dies zeigt die Herausforderung bei Patchen schon in einfacheren Fällen; denn trotz des vorliegenden Desasters - das muss man sagen - reden wir auch hier über einen einfacherer Fall, was das Patchen anbelangt, weil die Schwachstellen grundsätzlich patchbar sind. Dies ist aus technischen Gründen nicht immer der Fall. Es darf keine Systeme betreffen, die 24/7 laufen müssen und nur selten eingeplante Maintenance-Zeiten haben, keine Systeme betreffen, die bei Änderungen, also auch beim Einspielen eines Patches, rezertifiziert werden müssen, beispielsweise im Bereich der Avionik oder im medizinischen Bereich, und es darf keine Systeme betreffen, die harte Echtzeitanforderungen erfüllen müssen, beispielsweise im Bereich von Schalt- und Automatisierungstechnik. Trotzdem funktioniert es selbst in diesen einfacheren Fällen in der Praxis regelmäßig nur ungenügend.

Schauen wir auf andere Bereiche, beispielsweise auf den Bereich der kritischen Infrastrukturen. Da sind die Herausforderungen noch größer. Zu den genannten Aspekten kommt beispielsweise hinzu, dass der eine oder andere Hersteller von Legacy-Systemen, die lange betrieben werden, gar nicht mehr existent ist. Wer soll also die Schwachstelle schließen, wenn sie denn veröffentlicht wird?

Die Forderung nach einer strikten Offenlegung aller Schwachstellen berücksichtigt daher nicht

die Komplexität der realen IT-Landschaft. Entsprechend ist vielmehr ein holistischer Prozess zum verantwortungsvollen Umgang mit Schwachstellen erforderlich, der alle Aspekte einbezieht, beispielsweise die Verbreitung und Gefährlichkeit, inklusive der Ausnutzbarkeit einer Schwachstelle in der Praxis, die Möglichkeiten der Schließung und die Vor- und Nachteile einer Veröffentlichung bzw. Geheimhaltung.

Im Hinblick auf entsprechende Prozesse und die Komplexität der deutschen Cybersicherheitsarchitektur versus der Dynamik des Cyberraums ergibt sich somit insbesondere die Notwendigkeit des weiteren Ausbaus des gesamtstaatlichen Ansatzes.

Cybervorfälle zeichnen sich oftmals dadurch aus, dass sie insbesondere zu Beginn schwer attribuierbar sind und oftmals auch das eigentliche Ziel nicht unmittelbar zu identifizieren ist und somit auch die entsprechenden Zuständigkeiten gegebenenfalls erst mal nicht klar sind. Im Hinblick auf komplexe Cyberkrisen erfordert dies eine leistungsfähige Koordinationsfähigkeit zwischen allen beteiligten Akteuren. Das Nationale Cyber-Abwehrzentrum kann hier der geeignete Ansatzpunkt sein und ist entsprechend weiter auszubauen und zu befähigen.

Um entsprechenden Cyberkrisen jedoch zuvorzukommen, ist die Steigerung der Resilienz unserer Netze und Systeme von besonderer Bedeutung. Ziel muss es sein, die Angriffsoberfläche so weit wie möglich zu reduzieren und die Systeme zu härten, um so die Hürde für den Angreifer höher zu legen.

Ein grundlegender Aspekt ist die konsequente Nutzung von Produkten mit einem hohen Sicherheitsniveau. Die Bundeswehr nutzt beispielsweise auch Systeme, welche auf Mikrokernbetriebssystemen wie L4 mit nachgewiesenen Sicherheitsmechanismen basieren und welche auch durch das BSI zertifiziert sind. Mikrokernbetriebssysteme haben insbesondere nur eine minimale Anzahl von Programmzeilen und dementsprechend auch eine minimale Anzahl potenzieller Fehler. Viel zu oft finden sich aber auch in sicherheitskritischen Bereichen noch Systeme, welche auf „full-blown operating systems“ basieren, also Betriebssysteme, wie Sie sie auch auf Ihrem Laptop nutzen, mit denen Sie prinzipiell alles machen können, die über sehr viele Zeilen Programmiercode mit entsprechend hoher Anzahl an potenziellen Schwachstellen verfügen und viele Funktionalitäten aufweisen, welche in vielen Anwendungsbereichen gar nicht benötigt werden, aber die Basis für einen Missbrauch darstellen können.

Mikrokerne wie beispielsweise der als Open Source verfügbare seL4 werden noch immer viel zu selten eingesetzt. Der Mehrwert für die Sicherheit bei der Nutzung solcher Elemente wurde in der Praxis eindrucksvoll demonstriert, beispielsweise durch das High-Assurance-Cyber-Military-Systems-Programm der DARPA in den Jahren 2012 bis 2017. Auch die Arbeiten der EU, die Ansätze „Security by Design“ und „Privacy by Default“ voranzubringen, sind in diesem Kontext sehr zu begrüßen. Es ist aber immer auch auf die praktische Umsetzung zu achten, welche mitunter suboptimal ausfallen kann; als Beispiel sei hier die EU-Cookie-Richtlinie gewählt, die wohl allen gut bekannt ist.

Wichtig ist aber auch, zu beachten, dass solch eine avisierte Resilienzsteigerung auch unter optimalen Bedingungen eine lange Zeit benötigt und keine spürbaren Verbesserungen von heute auf morgen bringen kann. Die Transition von IPv4 auf IPv6 - also den Protokollen, die für die Adressierung der Rechner im Internet zuständig sind - mit der entsprechenden Parallelnutzung beider Protokolle seit über 20 Jahren und den damit verbundenen Sicherheitsimplikationen ist ein Beispiel hierfür.

Weiterhin muss berücksichtigt werden, dass auch optimal gebaute Systeme - das heißt Systeme, die gemäß der physikalischen Theorie sicher sind, wie beispielsweise im Bereich des Quantenschlüsselaustauschs - in der Praxis angreifbar bleiben werden, sei es durch bewusst eingebrachte und schwer bis nahezu unmöglich detektierbare Manipulationen, durch neue Möglichkeiten, die im Rahmen von Sprunginnovationen entstehen, oder durch die Limitierung in der physikalischen Umsetzung, die beispielsweise

Seitenkanalangriffe eröffnen können. Die Gewährleistung der Cybersicherheit und die Reduzierung des Risikos im Cyberraum auf ein tragbares Maß, insbesondere auch mit Hinblick auf die exponentiell verlaufende technologische Entwicklung, werden daher sehr herausfordernd bleiben.

Bei der Risikoanalyse ist daher immer eine holistische Betrachtung durchzuführen, welche die drei grundlegendenden Bedrohungsebenen - das Ausnutzen vorhandener Schwachstellen, das Finden neuer, bis dato unbekannter Schwachstellen in sogenannten Zero-Days sowie das bewusste Einbringen von Schwachstellen - berücksichtigt. Die daraus in der Praxis resultierenden komplexen Herausforderungen erfordern entsprechende, stets weiterzuentwickelnde Verteidigungsfähigkeiten auf höchstem Niveau.

Durch die Asymmetrie im Cyberraum, die Komplexität der Systeme und die Grenzen der Resilienz ist daher das Vorhalten offensiver Fähigkeiten zur Gewährleistung der eigenen Durchsetzungsfähigkeit unumgänglich. Selbst bei besten Sicherheitsmaßnahmen muss jederzeit mit einem wirkungsvollen Cyberangriff gerechnet werden. Und Notfallpläne für die Wiederherstellung von Systemen im Worst-Case-Fall sind gegebenenfalls in Firmen ausreichend, aber nicht auf dem Gefechtsfeld.

Gleichzeitig bieten offensive Cyberoperationen auch die besondere Möglichkeit, mit im Vergleich zu anderen Erbringungsdimensionen gewaltärmsten Effekten Operationsziele zielgenau und typischerweise reversibel zu erreichen, beispielsweise das temporäre Ausschalten eines Kraftwerkes oder eines Kommunikationsknotens - das wurde bereits angerissen -, was bei der Nutzung von beispielsweise Luft-Boden-Raketen bekanntermaßen regelmäßig nicht der Fall ist.

Meine sehr geehrte Damen und Herren, vielen Dank für Ihre Aufmerksamkeit. Ich freue mich auf die Diskussionen.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Kapitän. - Dann hat Herr Thomas Reinhold von der TU Darmstadt das Wort. Bitte sehr.

Sachverständiger Dipl.-Inf. Thomas Reinhold (Technische Universität Darmstadt): Sehr geehrte Abgeordnete! Sehr geehrte Mitarbeiterinnen und Mitarbeiter des Bundestages! Vielen Dank für Ihre Einladung. Mit Blick auf die verfassungs- und völkerrechtlichen Fragen im militärischen Cyber- und Informationsraum ist es mir als Friedens- und Sicherheitsforscher und Informatiker wichtig, eingangs kurz auf einige Aspekte hinzuweisen, die für diese Fragestellung meiner Meinung nach maßgeblich sind.

Zum einen muss festgehalten werden, dass nahezu jegliche unerlaubten Aktivitäten gegen oder in IT-Systemen Maßnahmen erfordern, um Schutzmechanismen zu umgehen, um Zugangs- oder Ausführungsberechtigungen zu erlangen sowie um digitale Fußspuren zu beseitigen. Aus der Perspektive der IT-Sicherheit entspricht dies in jedem Falle einer Manipulation des Regelverhaltens des betroffenen Systems, das sich daraufhin unerwartet verhalten kann. Dies kann beispielsweise die Störung bei der Ausführung der regulären Dienste bedeuten, den Ausfall eines IT-Systems verursachen oder Effekte in anderen abhängigen Systemen hervorrufen. Gleichzeitig sieht man einem IT-System von außen nicht mit ausreichender Sicherheit den Zweck sowie diese wechselseitigen Abhängigkeiten an. Die indirekten und direkten Konsequenzen von Manipulation sind dadurch kaum sicher abzuschätzen oder einzugrenzen. Das bedeutet, dass jegliche Aktivitäten gegen IT-Systeme diese potenziell gefährden, und zwar unabhängig vom eigentlichen Zweck der Cyberoperation.

Zweitens muss hinsichtlich der technischen Aspekte von nachrichtendienstlichen und militärischen Aktivitäten im Cyberraum festgehalten werden, dass eine rein passive Aufklärung kaum möglich ist oder einen marginalen nachrichtendienstlichen Erkenntnisgewinn liefert. Hochwertziele sind zumeist tief in IT-Netzwerke eingebettet, und ein Zugriff auf diese erfordert ein sukzessives Ausspähen, Unterwandern und Manipulieren vorgeschalteter Systeme. Somit werden in der Regel auch unbeteiligte Systeme beeinträchtigt. Derartige Aktivitäten könnten damit potenziell Effekte auslösen, bei denen Men-

schen verletzt oder getötet oder Sachgüter erheblich beschädigt werden. Mit Verweis auf ein Gutachten des Wissenschaftlichen Dienstes des Bundestages von 2018 würde dies das Verbot friedensstörender Handlungen nach Artikel 26 des Grundgesetzes berühren.

Drittens. Offensive Cyberoperationen, auch die im Rahmen der Bundeswehrfähigkeiten diskutierte aktive Cyberabwehr, erhöhen den Bedarf an Aufklärungsaktivitäten in Friedenszeiten. Um im Konfliktfall zeitnah über Informationen zu potenziellen Zielsystemen und deren Schwächen zu verfügen, müssen diese bereits im Vorfeld gesammelt und bereitgestellt werden. Wie aus einer kürzlich erfolgten Antwort der Bundesregierung auf eine Kleine Anfrage deutlich wird, kommt diese Aufgabe der Informationsgewinnung und -weitergabe mutmaßlich dem Bundesnachrichtendienst zu. Aufgrund des umfangreichen und kontinuierlichen Informationsbedarfs für die Erstellung und Aktualisierung eines Cyberlagebildes bedeutet dies einen erheblichen technisch-operativen Mehraufwand für den BND, der über die gezielte nachrichtendienstliche Aufklärung sorgfältig ausgewählter Systeme deutlich hinausgehen dürfte. Eine solche regelmäßige Informationsgewinnung und -weitergabe unterstreicht damit erneut die Frage nach der Legitimität sowie nach den Möglichkeiten der parlamentarischen Kontrolle und Steuerung einer de facto verstetigten Kooperation zwischen Bundesnachrichtendienst und Bundeswehr. Darauf ist in den vergangenen Monaten bereits mehrfach an verschiedenen anderen Stellen hingewiesen worden.

Schlussendlich ist anzumerken, dass dem Trend einer zunehmenden Militarisierung des Cyberspace kaum geeignete konfliktreduzierende Maßnahmen gegenüberstehen. Dies betrifft Hilfsmittel und Verfahren zur Unterstützung von Vertrauensbildung im Cyberspace sowie für die Nichtverbreitung von Cyberwaffen oder die Rüstungskontrolle und Abrüstung. Etablierte Ansätze versagen, und geeignete technische Verfahren existieren bislang bestenfalls als Konzepte. Eine gezielte Förderung technischer Forschung ist daher dringend geboten und kann im Rahmen deutscher außenpolitischer Initiativen wichtige Impulse als Gegengewicht bieten. - Vielen Dank.

Vorsitzender Wolfgang Hellmich: Vielen Dank, Herr Reinhold. - Dann hat Frau Schuetze das Wort. Bitte sehr.

Sachverständige Julia Schuetze (Stiftung Neue Verantwortung e. V.): Vielen Dank. Danke für die Einladung. - Eingangs ist mir wichtig, zu sagen, dass die Domäne, in der sich die Bundeswehr und andere Sicherheitsbehörden aus Deutschland und anderen Ländern bewegen, untrennbar von der Domäne ist, die wir für eigene wirtschaftliche und soziale Aktivitäten selbst nutzen. Es handelt sich um dieselbe Domäne. Dies muss mitbedacht werden, da die Nutzung der Domäne für Verteidigung potenziell positive als auch negative Auswirkungen auf die Nutzung derselben Domäne für die friedlichen Aktivitäten haben kann. Deswegen sollte die Cyberverteidigungspolitik gesamtstaatlich gedacht werden.

In meiner Stellungnahme gehe ich vor allem auf drei Problemfelder ein, die die Verteidigungspolitik betreffen.

Erstens. Der Einsatz offensiver Mittel im Rahmen eines Mandats darf unsere eigene Defensive nicht schwächen. Nehmen wir an, die Bundeswehr soll einen internationalen Einsatz durchführen können und dort auch offensive Cyberwirkmittel nutzen. Hier stellt sich vor allem die Frage: Welche offensiven Mittel darf die Bundeswehr einsetzen? Es sollte vermieden werden, dass solche Mittel negativen Einfluss auf unsere eigene Defensive haben. Deswegen ist es wichtig, Risiken bei der Nutzung von offensiven Fähigkeiten durch die Bundeswehr bei Mandatsfällen zu mitigieren. Dabei spielt vor allem der Umgang mit Schwachstellen eine Rolle.

Hier ist als gut zu befinden, dass die Bundeswehr ein eigenes Disclosure-Programm aufgesetzt hat, wo sie mithilfe von Externen Schwachstellen in ihren eigenen Systemen identifiziert. Dies ist ganz im Sinne der IT-Sicherheit. Allerdings handelt es sich nur um Schwachstellen in ihren Systemen, während der Umgang mit Schwachstellen, die sie selbst für offensive Operationen nutzt, noch ungeklärt ist. Hier wäre es wichtig, zu untersuchen, inwieweit zum Beispiel die Nut-

zung von bekannten Schwachstellen der Bundeswehr ausreichen würde, um ihre verteidigungspolitischen Ziele zu erreichen.

Zweitens. Die klare Trennung von Mitteln zur Vorbereitung eines möglichen Einsatzes und eines Einsatzes durch Mandat ist wichtig, um vor allem Eskalationen zu vermeiden. Der Einsatz offensiver Mittel muss im Ernstfall, zum Beispiel wenn der Zielstaat davon mitbekommt, außenpolitisch klar und transparent kommunizierbar sein, um Eskalationen oder falsche Einschätzungen des Zielstaates zu vermeiden. Deshalb braucht es eine klare Trennung zwischen der Vorbereitung eines möglichen Einsatzes mit offensiven Mitteln und eines Einsatzes offensiver Mittel mit Mandat. Technisch hat mein Kollege Sven Herpig hier einen Vorschlag gemacht, wo die Linie ist. Wenn es um die Rolle von nachrichtendienstlichen Operationen der Bundeswehr oder anderer Behörden vor Mandat geht, sollte der Unterschied zwischen Maßnahmen zur Informationsgewinnung und Maßnahmen zur Aufklärung und Wirkung klarer kommuniziert und kontrolliert werden.

Im BND-Gesetz ist eine privilegierte Partnerschaft zwischen BND und Bundeswehr vorgesehen; demnach kann der BND Informationen an die Bundeswehr weiterleiten. Hier stellt sich die Frage: Wie kommt der BND an diese Informationen? Wie geht man momentan damit um, wenn der BND Informationen durch offensive Cyberoperationen im Sinne der Aufklärung und Wirkung in einem Land bekommt, wo die Bundeswehr kein Mandat hat, und diese Informationen dann aber an die Bundeswehr weiterleitet? Wenn die Operation entdeckt werden sollte, wie kann die Bundesregierung dann glaubhaft sagen, dass diese Operation rein nachrichtendienstlicher Natur war und nicht genutzt wurde, um einen Militäreinsatz vorzubereiten? Das ist wichtig; denn letztendlich muss der Zielstaat einer solchen Operation glaubhaft überzeugt werden.

Drittens: Klarheit über Deutschlands Reaktion, wenn andere Staaten unsere IT-Infrastrukturen für ihre Verteidigungszwecke nutzen. Ich hatte in meiner Stellungnahme im Dezember über US-Cyberverteidigungspolitik geschrieben, die unter anderem besagt: Es gilt, 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 dann zum Beispiel IT-Systeme deutscher Firmen und Behörden sein. - Ich hatte gefragt, wie Deutschland mit solchen US-amerikanischen Cyberoperationen in deutschen Netzen umgeht.

Nun gab es seitdem ein Statement des Auswärtigen Amts in Zusammenarbeit mit dem Bundesverteidigungsministerium; allerdings schafft es nur bedingt Klarheit und könnte noch etwas geschärft werden. In dem Statement gelangt man zu dem Schluss, dass vernachlässigbare physische Auswirkungen und Funktionsstörungen unterhalb einer bestimmten Auswirkungsschwelle keine Verstöße gegen die Souveränität darstellen, selbst wenn sie sich auf eine kritische Infrastruktur auswirken. Zudem wird beschrieben, dass Deutschland die Sorgfaltspflicht anwenden würde. Unter Berufung auf den ersten Fall des Internationalen Gerichtshofs - Korfu-Kanal-Fall - macht Deutschland geltend, dass Staaten verpflichtet sind, nicht zuzulassen, dass ihr Hoheitsgebiet wissentlich für Handlungen verwendet wird, die den Rechten anderer Staaten zuwiderlaufen. Wie sind diese Aussagen der Bundesregierung dann in dem Fall zu bewerten, dass die USA möglicherweise unsere Infrastrukturen - gegebenenfalls kritische - nutzt, um in einem Land, mit dem wir nicht im Konflikt stehen, IT-Infrastrukturen anzugreifen, vor allem, wenn wir davon mitbekommen?

Zusammenfassend stelle ich deswegen fest, dass die strategische Neuausrichtung anderer Staaten wie zum Beispiel der USA und der Einsatz offensiver Mittel von der Bundeswehr bedeuten, dass Deutschland seine Strategie gesamtstaatlich anpassen muss. Diese müsste die genannten Inkonsistenzen adressieren. Dies ist besonders wichtig, da eine 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. - Vielen Dank.

Vorsitzender Wolfgang Hellmich: Danke sehr an alle Sachverständigen für ihren Beitrag. - Wir beginnen auf dieser Grundlage jetzt mit der Fragerunde der einzelnen Fraktionen. Als Erstes hat die Fraktion der CDU/CSU das Wort. Herr Otte.

Henning Otte (CDU/CSU): Herr Vorsitzender! Liebe Kolleginnen und Kollegen! Meine sehr verehrten Damen und Herren Sachverständige! Liebe Gäste! Lassen Sie mich zunächst einmal herzlich danken, dass wir heute zusammen diese Anhörung zum Thema Cybersicherheit durchführen. Herzlichen Dank - ich denke, im Namen aller - auch an das Sekretariat für die sehr gute Vorbereitung!

Das Eingangsstatement des ersten Sachverständigen, Professor Dr. Heintschel von Heinegg, hat - zumindest für mich - auf den Punkt gebracht, dass wir im Vergleich zu anderen Nationen weit zurückliegen. Wir müssen einmal die konkurrierenden Aufgaben betrachten, um die es im Rahmen der Cybersicherheit geht. Wir müssen aber auch deutlich machen, dass es neben der Abwägung von ethischen und juristischen Argumenten darauf ankommt, dass wir die Sicherheit unseres Landes gewährleisten können. Hier müssen wir die Sicherheit und die Verteidigung Deutschlands umfassend betrachten.

Es ist Auftrag der Bundeswehr, die Verteidigung unseres Landes für die Bürgerinnen und Bürger sicherzustellen, und zwar zusammen mit unseren Bündnispartnern. Dabei geht es auch darum, dass wir neben den Kategorien Fregatten, Panzer, Flugzeuge bzw. See, Land und Luft deutlich machen, dass wir auch den virtuellen Raum verteidigen müssen, um Angriffe mit weiter reichenden Auswirkungen verhindern zu können. Denn was wäre, wenn wir GPS oder die Stromnetze nicht schützen können bzw. diese so angegriffen werden, dass sie zusammenbrechen? Davor gilt es unser Land zu schützen.

Ich sage auch sehr deutlich, dass ein solcher Cyberangriff, wie er vielfach an jedem Tag in unseren Institutionen stattfindet, nicht von einem klassischen militärischen Angriff zu unterscheiden ist, zumindest nicht von der Intention her. So gilt es, dass wir die klassischen Domänen - Schutz, Verteidigung, Angriff, Abschreckung - wie in den Bereichen Luft, Land und See genauso im Cyberraum anwenden. Klar gilt es, Besonderheiten zu beachten, nicht über das Ziel hinauszuschießen, insbesondere völkerrechtliche Rahmenbedingungen zu sehen: Diskriminierungsverbot, Verhältnismäßigkeit, Ultima Ratio, Achtung des Gewaltverbots. Auch das muss man im Cyberraum sehr deutlich im Auge haben.

Nach Auffassung der CDU/CSU-Bundestagsfraktion gilt es aber, in diesem Bereich mehr zu tun, aufzuschließen, um deutlich zu machen, dass die Sicherheit unseres Landes umfassend, in einem 360-Grad-Blickwinkel zu betrachten ist. Deswegen ist die heutige Anhörung für uns sehr wichtig, da sie mehr als nur ergänzt; vielmehr macht sie auf einen ganz sensiblen Bereich aufmerksam.

Wir haben uns in der Fraktion dahin gehend die Aufgaben geteilt, dass zunächst einmal Dr. Reinhard Brandl anschließen wird und für die weiteren Fragerunden Herr Professor Dr. Patrick Sensburg und Herr Eckhard Gnodtke zur Verfügung stehen. - Herzlichen Dank erst einmal von meiner Seite. Ich gebe weiter an Herrn Dr. Brandl.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank, auch für die interessanten und sehr inhaltsreichen Eingangsstatements der Experten. - Ich habe eine Reihe von Fragen an verschiedene Experten und möchte beginnen mit dem Inspekteur Daum.

Herr Daum, wir stellen die Bundeswehr zur Verteidigung auf. Das haben Sie in Ihrem Eingangsstatement auch deutlich gemacht. Meine erste Frage an Sie ist: Was wäre aus Ihrer Sicht, wenn Deutschland unzweifelhaft von einem anderen Staat mittels eines Cyberangriffs - zu der Frage, was ein Cyberangriff ist, kommen wir später noch - angegriffen worden wäre oder angegriffen wird, eine mögliche Strategie zur Verteidigung, und wie würden sich dabei konventionelle Mittel

und Cybermittel zur Verteidigung unter Umständen ergänzen?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank, Herr Abgeordneter, für die Frage. - Wenn Deutschland in Form eines Cyberangriffs angegriffen wird, gilt es für die Bundeswehr natürlich erst mal, die eigenen Netze, die eigenen Systeme zu schützen; das ist natürlich mit dem Auftrag der Bundeswehr einhergehend. Wenn ein solcher Angriff sich auf zivile Infrastruktur etc. erstreckt, dann wird das natürlich durch die anderen Ressorts, insbesondere durch das BMI, wahrgenommen.

Wenn es zu einem Vorgang kommt, der das Cyber-Abwehrzentrum berührt, dann wird die Bundeswehr im Rahmen des ressortübergreifenden Austausches davon natürlich Kenntnis erlangen. Wenn wir dabei den Eindruck haben, dass wir bei der Bereinigung dieses Angriffes unterstützen können - beispielsweise könnte das bei uns Cybersicherheitsexperten auf den Plan rufen -, dann handelt es sich offensichtlich um eine Fähigkeit, die möglicherweise hier hilfreich sein kann. Das setzt aber, weil es dann, wenn es um zivile Infrastruktur geht, ein Einsatz der Bundeswehr im Inneren wäre, natürlich voraus, dass Hilfeleistung durch die Bundeswehr auf Grundlage von Artikel 35 des Grundgesetzes, also Amtshilfe, angefordert wird. Dann könnten wir natürlich entsprechend Hilfe leisten, etwa durch Unterstützung in der Frage des Aufstellens von entsprechenden Abwehrmechanismen, Firewalls etc. oder im Kontext forensischer Untersuchungen, wenn der Angriff beendet oder abgewehrt ist.

Eine aktive, unmittelbare Teilnahme an Verteidigungsaktivitäten sehe ich dabei jetzt erst mal nicht. Also ich sehe keinen Gegenangriff, ich sehe kein offensives Vorgehen in dieser Hinsicht. Das ist da sicherlich nicht die Rolle. - So würde ich die Frage beantworten.

Dr. Reinhard Brandl (CDU/CSU): Sie sind jetzt vom Friedensfall ausgegangen, der ja - Gott sei Dank - zurzeit und hoffentlich auch ewig anhält. Wie wäre die Lage im Verteidigungsfall?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Der Verteidigungsfall wäre eine Situation, in der wir uns im Konfliktzustand mit einer Nation befinden. Dann kommt es natürlich auf die Frage an, ob wir mittels aktiver, offensiver Maßnahmen einen Angriff abwehren können. Das setzt natürlich voraus, dass man überhaupt die Fähigkeit und die entsprechenden Zugänge besitzt, um einen solchen Schritt zu erzielen.

Wenn wir uns im Konflikt befinden, ist aber auch die Rechtslage eine andere. Dann ist natürlich die Frage zu stellen: Wer ist denn der Angreifer? Und da sind wir bei dem schon angesprochenen Thema der Attribuierung, die da immer schwierig ist. Aber wenn wir von einem Angriff ausgehen, dann gilt es natürlich, das entsprechend zu untersuchen. Wir sind uns darüber im Klaren, dass das dazu führen kann, dass wir auf einmal auf eine Nation A schauen, von der möglicherweise ein Angriff kommt, obwohl wir uns mit der Nation B im möglichen Konflikt befinden. Das verkompliziert die Thematik natürlich. - Das würde ich erst mal so beantworten.

Dr. Reinhard Brandl (CDU/CSU): Die Bundeswehr stellt sich ja in allen Teilstreitkräften auf Verteidigung ein. Ganz wesentliche Waffensysteme, die die Bundeswehr vorhält, würden ja auch nur in einem Verteidigungsfall zum Einsatz kommen. Meine Frage ist: Welche Mittel müssten wir vorhalten, wenn wir uns auch in der Cyberteilstreitkraft und im Organisationsbereich CIR so aufstellen wollen, um im Verteidigungsfall auf einen Angriff reagieren zu können?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank. - Grundsätzlich gilt für einen solchen Verteidigungsfall natürlich, dass der Angriff auf verschiedenen Wegen erfolgen kann. Es können sowohl konventionelle Angriffe - Heer, Luftwaffe, Marine - als auch Angriffe im Cyberraum sein. Die Reaktion darauf sollte aus meiner Sicht letztlich genauso vielfältig sein. Sie können natürlich einen Cyberangriff de facto auch mit konventionellen Kräften beantworten und dabei auf ganz andere Ziele operieren.

Für offensive Maßnahmen im Cyber- und Informationsraum braucht die Bundeswehr natürlich entsprechende Tools, entsprechende Werkzeuge und entsprechende Menschen, die dazu befähigt sind. - Danke.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Das leitet schon zu meiner nächsten Frage über, ebenfalls an Herrn Daum. Meine Frage betrifft die Trennung von äußerer und innerer Sicherheit. Wir erleben ja - das wurde vorher schon gesagt -, dass die Grenze zwischen äußerer und innerer Sicherheit gerade im Cyberraum sehr stark verschwimmt. Das wird dazu führen, dass wir auch die Aufgabenverteilung zwischen den Behörden ein Stück weit anpassen müssen. Dabei wird natürlich auch eine Rolle spielen, welche Behörde, welche Organisation was am besten kann. Die Frage ist: Was kann die Bundeswehr eigentlich am besten, oder wie könnte der Beitrag der Bundeswehr zur gesamtstaatlichen IT-Sicherheitsvorsorge im Cyberraum aussehen?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank. - Wir haben natürlich Fähigkeiten, die, wie ich schon betont habe, zum Schutz der eigenen Systeme dienen. Diese Mechanismen, die wir dort zur Anwendung bringen, sind natürlich genauso geeignet für jeden anderen Schutzauftrag, der sich auf zivile Infrastruktur etc. richtet. Gerade beim Schutzauftrag orientieren wir uns natürlich massiv an den entsprechenden Aufstellungen des Bundesamtes für Sicherheit in der Informationstechnik.

Zu der Frage, was wir im Falle eines Falles beitragen können - ich will in diesem Format jetzt nicht zu weit gehen -: Das sind natürlich alle Fähigkeiten, die wir haben. Diese werden sich möglicherweise qualitativ von den Fähigkeiten der entsprechenden Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik gar nicht so sehr unterscheiden, aber sie können durchaus quantitativ Ergänzungen bringen. Dann liegt es am Ende sicherlich auch an den einzelnen handelnden Personen, inwieweit das auch qualitativ eine Verstärkung darstellt. - Vielen Dank.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Meine nächste Frage geht an Herrn Dr. Koch zur Attribution. Für mich stellt sich die Frage, ob die Attribution ein so großes technisches Problem ist, wie es immer dargestellt wird. Meine Erfahrung bei allen Cyberangriffen, die ich näher begleitet habe, insbesondere in meiner Rolle als Mitglied des Verteidigungsausschusses, und von denen man auch in der Presse lesen konnte, ist, dass eine Attribution dann doch möglich war, wenn auch mit einem gewissen Aufwand. Das haben wir ja auch beim Cyberangriff auf den Deutschen Bundestag erreicht. Ich habe eher den Verdacht, dass die Attribution politisch oftmals gar nicht so sehr gewollt ist; denn wenn man es nicht attribuiert, ist es politisch einfacher, keine Antwort bzw. nur eine abgestufte Antwort zu geben, mit der man eben nicht in diese Eskalationsmechanismen mit Wenn-dann-Fragen kommt. Wie sehen Sie das aus technischer Sicht, Herr Koch?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Vielen Dank. - Das ist auf jeden Fall eine sehr interessante Fragestellung. Ich denke, eine Attribuierung ist technisch mit einem hinreichenden Aufwand und entsprechendem zeitlichen Fenster - das geht natürlich nicht von heute auf morgen; wir haben im Falle des Hacks vom Bundestag ja gesehen, wie lange so etwas dauern kann - in vielen Bereichen möglich.

Die Herausforderung, nicht in Fehlattribuierungen hineinzulaufen, weil man Falsche beschuldigt, ist natürlich maßgeblich abhängig von der Qualität des Angreifers. Wir finden beispielsweise im Rahmen der Vault-7-, Vault-8-Leaks - das waren Dokumente, die von den Hacking-Abteilungen der CIA veröffentlicht worden sind - Frameworks, die spezifisch dafür konstruiert wurden, eine Fehlattribuierung zu machen. Da sind Elemente drin, die beispielsweise die Sprachpakete anpassen, also solche Indizien, die wir verwenden, um eine Attribuierung zu machen, wenn wir den Source Code analysieren, verschleiern. Man muss immer darauf achten, dass solche Elemente enthalten sein können.

Aber wenn Sie einen so komplexen Code analysieren und es im Detail und mit viel Zeit machen, dann sehen Sie beispielsweise an der Art und

Weise der Programmierung, auf welcher Basis der eine oder andere Code entstanden ist, welches die typischen Handschriften sind. Für hochspezialisierte Bereiche gibt es immer nur wenige Leute, die das entsprechend machen können. Dann können Sie tatsächlich auch eine Attribuierung technischer Natur erreichen, aber eben mit sehr hohen Aufwänden. Es ist gerade vor dem Hintergrund der vorschnellen bzw. der schnellen Attribuierung durch IT-Sicherheitsfirmen in den letzten Jahren wichtig, dass man da genug Zeit und Qualität reinlegt; dann ist es komplex, aber definitiv machbar.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Hat eigentlich die Bundeswehr Kapazitäten zur Attribution, Herr Koch?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Eine Attribuierung nimmt die Bundeswehr im Augenblick nicht vor. Wir haben natürlich entsprechendes forensisches Personal, das sehr, sehr gut ausgebildet ist, also die grundlegenden Elemente, um so etwas durchzuführen. Aber für uns ist es im Augenblick keine entsprechende Aufgabe. Im Zweifelsfall weiß es der Inspekteur aber besser als ich.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Ich habe jetzt nur noch sechs Minuten. Deswegen würde ich auf den Inspekteur vielleicht später noch mal zurückkommen.

Ich habe noch eine Frage an Herrn Professor Heinegg, und zwar zur Rechtslage, wenn die Angriffshandlung von sogenannten patriotischen Hackern ausgeht, das heißt von Hackern, wo der Staatsauftrag nicht eindeutig erkennbar ist, aber die Handlung im nützlichen Interesse eines fremden Staates liegt. Mit anderen Worten: Reicht die Befürwortung bzw. die nichtöffentliche Zustimmung zu einem Cyberangriff eines nichtstaatlichen Akteurs für die Zurechnung zu einem staatlichen Handeln aus? Wie geht man also damit rechtlich um, wenn ein Klima, ein Umfeld entsteht, wo nichtstaatliche Akteure gegen fremde Staaten hacken können, ohne dass der Link zur Regierung direkt hergestellt wird?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Hier gibt es eine Vorschrift in den Entwurfsartikeln der Völkerrechtskommission der Vereinten Nationen. Danach ist ein solches Verhalten einer Privatperson nur dann zurechenbar, wenn der Staat dieses Verhalten anerkennt und - darauf kommt es jetzt an - sich zu eigen macht. Das heißt: Das bloße Befürworten des Handelns Privater, etwa weil es den nationalen Interessen oder welchem Zweck auch immer dienen mag, ist nicht ausreichend, sondern der Staat muss auf der Grundlage dieses Privatverhaltens für sich eigene Konsequenzen daraus herleiten, etwa indem er Ansprüche gegen den Zielstaat erhebt oder ihm beispielsweise Vorschläge macht, was zu tun wäre, damit dieser Angriff unterbleibt. Aber die bloße Befürwortung ist nicht ausreichend.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Wir hatten in den Statements vorher die Frage: Wie ist es rechtlich zu beurteilen, wenn ein Cyberangriff vom Server eines unbeteiligten Drittstaates ausgeht? Wäre in einem solchen Fall eine offensive Reaktion, eine Cyberreaktion gegen den Drittstaat bzw. gegen den Server in diesem Drittstaat als Verteidigungshandlung völkerrechtlich zulässig?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Zunächst muss dieser Drittstaat, von dessen Territorium der Angriff seinen Ausgang nimmt, darüber informiert werden. Er muss also in Kenntnis gesetzt werden, falls er nicht ohnehin schon Kenntnis hat. Dann müssen die entsprechenden Konsequenzen daraus gezogen werden. Hier würde es sich, wenn Sie so wollen, um eine Form der extraterritorialen Selbstverteidigung handeln, wenn und soweit der Staat, von dessen Staatsgebiet diese Handlungen ihren Ausgang nehmen, nicht willens oder in der Lage ist, diese Verhaltensweise oder diese Nutzung seines Staatsgebiets zu unterbinden.

In diesem Zusammenhang sei darauf hingewiesen: Das ist keine Sorgfaltspflicht - das ist eine falsche Übersetzung des englischen Begriffs „due diligence“-, sondern das ist eine Verpflichtung des Staates, einzuschreiten, wenn sich etwas auf

seinem Territorium ereignet. Das bedeutet keineswegs, dass der Staat verpflichtet wäre, alle Cyberaktivitäten auf seinem Territorium oder über seinem Territorium zu überwachen und präventiv tätig zu werden.

Dr. Reinhard Brandl (CDU/CSU): Das würde bedeuten, dass wir bei solch einem Vorgang, also wenn wir von einem Server, der sich in einem Drittstaat befindet, angegriffen werden, den Drittstaat erst mal darauf hinweisen müssten und erst dann, wenn er nach einer bestimmten Frist und einer bestimmten Anzahl von Hinweisen nicht reagiert, tätig werden könnten. Habe ich das jetzt so richtig verstanden?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Nein, es reicht eigentlich aus, dass er es weiß oder wissen können muss. Gerade im Bereich Cyber ist es so, dass einige Staaten wie etwa das Vereinigte Königreich der Auffassung sind, dass ein solches vorheriges Inkenntnissetzen nicht erforderlich sei, weil die Umstände des jeweiligen Falles, insbesondere die Besonderheiten des Cyberraums, dies gar nicht erlaubten. Das ist umstritten. Aber, um Ihre Frage endgültig zu beantworten: Das einmalige Inkenntnissetzen würde im Zweifelsfalle ausreichen.

Dr. Reinhard Brandl (CDU/CSU): Okay. - Dann hätte ich noch eine letzte kurze Frage an Herrn Padilla in dieser Runde, und zwar: Besteht in Deutschland ausreichend Know-how in Forschungseinrichtungen, in Universitäten und anderen Bildungseinrichtungen, in der Wissenschaft, um im Vergleich zu anderen Ländern auch erforderliche Cyberkapazitäten vorzuhalten?

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Ich glaube, das Know-how ist an der Stelle unser kleinstes Problem. Wir haben inzwischen mannigfaltig entsprechende Studiengänge. Wir haben viele intelligente Köpfe. Wir haben auch viele Forschungsansätze in diese Richtung. Unser Problem ist eher ein Umsetzungsproblem. Ich bin an verschiedenen Kooperationen, auch mit den Israelis, die immer als eines der leuchtenden Vorbilder bezeichnet werden, beteiligt. Es ist nicht so, dass wir uns auf technischer Ebene verstecken müssten; da würde ich dem bisher Gesagten eher widersprechen wollen. Vielmehr sind die Israelis froh, dass sie uns in verschiedenen Bereichen dazu fragen können. Wo wir nicht sonderlich gut sind, ist, das nachher in irgendwelche nutzbaren Produkte zu bekommen. Zu Ihrer Frage: Ich glaube nicht, dass wir ein Know-how-Problem haben. Wir haben eher ein deutliches Umsetzungs- und Nutzungsproblem des Know-hows.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann geht das Fragerecht an die Fraktion der AfD, an Herrn Nolte.

Jan Ralf Nolte (AfD): Zunächst vielen Dank, sowohl für die eben gehaltenen Vorträge als auch für die schriftlich eingereichten Stellungnahmen. Auf einige davon möchte ich gleich kurz eingehen und im Anschluss zwei Fragen stellen. Einige, die ich mir aufgeschrieben hatte, wurden eben schon von meinem Vorredner gestellt.

Wir gehen davon aus, dass es selbstverständlich ist, dass sich bei der Wirkung im Cyberraum an das Völkerrecht gehalten wird - vollkommen klar. Gleichwohl muss eine Aufklärung im Cyberraum natürlich durchführbar sein. Sofern das Informationsbeschaffung ist und nicht Informationsgewinnung, dürfte das zumindest außerhalb der Mandatsgebiete ja in der Zuständigkeit des BND liegen. Es ist richtig so, dass der BND das macht. Das muss er unserer Meinung nach auch machen; denn das ist normale nachrichtendienstliche Tätigkeit. Nachrichtendienste beschaffen sich Informationen letztlich ja immer irgendwo gegen den Willen von anderen Staaten. Das ist also nachrichtendienstliche Tätigkeit.

Wirkung im Cyberraum ist natürlich etwas anderes. Das muss beschränkt sein, wenn wir jetzt von der Bundeswehr sprechen oder meinetwegen auch vom BND, etwa auf Einsatzgebiete der Bundeswehr. Auch da sagen wir: Das ist eine gute Möglichkeit, sich dort auszuwirken. Wenn man ein Wirkmittel im Cyberraum wirklich speziell auf einen bestimmten Zweck zuschneiden kann,

dann kann man sich damit vielleicht das eine oder andere kinetische Wirkmittel sparen und auch den einen oder anderen Kollateralschaden verhindern. Auch aus völkerrechtlicher Sicht ist das potenziell eine ganz gute Sache.

Wir lehnen daher auch den Parlamentsvorbehalt für Informationsgewinnung, für Informationsbeschaffung - auch das klang ja an - als unzweckmäßig ab, zumal wir ja Einsätze im Bundestag mandatieren, in denen zur Not ein Soldat auch feindliche Kräfte töten dürfte; dann darf er natürlich aufklären oder Wirkmittel im Cyberraum anwenden. Das ist für uns ganz klar.

Ich komme jetzt zu meinen beiden Fragen, die an Sie, Herr Vizeadmiral, gehen. Mich würde interessieren, wer eigentlich zuständig ist, wenn die Bundeswehr im Inland zum Ziel eines Cyberangriffs wird. Ich denke mal, in den eigenen Systemen wird natürlich die Bundeswehr zunächst zuständig sein. Aber irgendwann, wenn es um Attribuierung - wer war es? - geht oder darum, sich Informationen wiederzubeschaffen, dann kann ich mir vorstellen, dass irgendwo eine Schwelle überschritten wird, ab der vielleicht der BND zuständig ist. Ich würde gern verstehen: Wie läuft das da mit den Zuständigkeiten genau?

Die zweite Frage bezieht sich auf das Urteil des Bundesverfassungsgerichts zur nachrichtendienstlichen Aufklärung. Da würde ich gerne wissen, wie sich das auf die Aufklärung im Cyberraum in Einsatzgebieten auswirkt.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Herzlichen Dank, Herr Abgeordneter. - Zu den Zuständigkeiten: Grundsätzlich werden wir natürlich als Bundeswehr erst mal selber tätig, wenn sich irgendjemand gegen uns richtet. Den Angriff im Cyberraum will ich mal ganz frei vergleichen mit einer eingezäunten Kasernenanlage, in die jemand versucht einzudringen. Dann liegt die erste Maßnahme, dies zu verhindern, natürlich bei den Streitkräften. Genau das macht bei uns das Zentrum für Cyber-Sicherheit in der Bundeswehr, das die Netze überwacht.

Wir wissen, dass nur ein Teil der Bundeswehrnetze von der Bundeswehr selber betrieben wird und dass die IT-Gesellschaft der Bundeswehr, die BWI, dort eine entsprechende Aufgabe hat. Natürlich gibt es auch dort einen Cybersicherheitsoffizier, der für die Netze zuständig ist.

Die sozusagen erste Verteidigungslinie sind also die Bundeswehr und die BWI. Wenn es ihnen gelingt, einen Angriff - das ist wie bei dem Versuch, den Kasernenzaun zu überwinden; hier muss im Falle eines Falles die Bundeswehr-Firewall überwunden werden - abzuwehren, stellt sich natürlich die Frage: Wer war es, welche Maßnahmen sind erforderlich und wie kann man ihn dafür zur Rechenschaft ziehen?

Das ist zunächst kein Auftrag der Bundeswehr, sondern es werden per se erst mal Strafverfolgungsbehörden auf den Plan gerufen. Dabei sind natürlich entsprechende verfahrenstechnische Vorgehensweisen anzuwenden. Unser Anteil besteht darin, dass wir über unsere Systeme, die einen Angriff beobachtet haben, entsprechende Informationen zur Verfügung stellen. Diese sind natürlich letztlich wie Beweismaterial zu behandeln. Insofern ist dieser Prozess für den Fall, dass wir angegriffen werden, aus meiner Sicht gut zu verstehen und nachzuvollziehen. Sie haben sich ausdrücklich auf den Zustand im Frieden beschränkt.

Was das Bundesverfassungsgericht über das BND-Gesetz und notwendige Nachbesserungen formuliert hat, hat erst mal keine unmittelbaren Auswirkungen auf den Auftrag der Streitkräfte, nämlich Aufklärung. Gleichwohl - das ist vorhin in einer Stellungnahme angeklungen - gibt es natürlich einen gewissen Informationsaustausch zwischen dem Bundesnachrichtendienst und der Bundeswehr. Das ist ja durch Rahmenvereinbarungen alles entsprechend geregelt. Diese Regelungen werden jetzt auf den Prüfstand gestellt: Inwieweit wirkt sich eine veränderte Rechtslage für den BND dann auch auf die Bundeswehr aus? - Vielen Dank.

Vorsitzender Wolfgang Hellmich: Dann geht das Fragerecht für die SPD-Fraktion an Frau Möller.

Siemtje Möller (SPD): Moin aus Friesland! - Zunächst meinen herzlichen Dank an die Sachverständigen für die ausführlichen Stellungnahmen und auch für die bereitwilligen Auskünfte. Sie waren für den Beginn auf jeden Fall schon sehr aufschlussreich.

Bevor ich an die weiteren Mitglieder meiner AG übergebe, würde ich mich auf die Fragen rund um Parlamentsvorbehalte und Attribution beschränken. Zum Thema Attribution lautet die erste Frage: Wie viel Zeit vergeht, bis man überhaupt eine Attribution vornehmen kann? Die zweite Frage ist: Was passiert eigentlich, wenn am Ende tatsächlich keine Attribution möglich ist, aber man trotzdem ein Sicherheitsvorkommnis im Land hat? Ist es auch dann möglich, im Cyberoperationsraum vorzugehen und dort auch ein offensives Wirkmittel einzusetzen?

Als Erstes würde ich diese Fragen gerne an Herrn Herpig und auch an Herrn von Heinegg als Rechtswissenschaftler richten.

Sachverständiger Dr. Sven Herpig (SNV e. V.): Danke für die Frage. - Das ist genau der Grund, warum ich am Anfang gesagt habe, dass offensive intrusive Cyberoperationen der Bundeswehr nicht zur IT-Sicherheit führen werden. Wenn wir einen Cyberangriff, eine Cyberoperation im Friedensfall gegen Deutschland haben, dann ist, wie gerade schon von Herrn Daum ausgeführt, natürlich die Bundeswehr zuständig, wenn es um den Eigenschutz geht. Ansonsten ist das BMI-Ressort zuständig, vor allem das BSI. Wenn kriminelle Energie dahintersteckt, ist vielleicht das BKA zuständig und bei Spionagetätigkeiten das BfV; das BfV hat die Befugnis zur Zurechnung, also zu der technischen Attribution oder Attribuierung des Angriffs. Und natürlich sind die Länder bzw. die Firmen oder die direkt betroffenen Behörden selbst dafür verantwortlich, sich mit diesem Schadensvorfall zu befassen.

Die Attribuierung - das wurde gerade schon angesprochen - kann lange dauern; im Bundestag hatte es auch länger gedauert. Von daher kann man sich, wenn eine Attribution erfolgt ist, überlegen: Wie reagieren wir jetzt? Da kann natürlich eine offensive intrusive Cyberoperation benutzt werden. Da können andere domänenübergreifende Wirkmittel oder andere Maßnahmen - diplomatische Maßnahmen, Sanktionen usw. - zum Einsatz kommen. Das ist dann vielleicht eine direkte Antwort auf eine Cyberoperation, was aber nicht das Eintreten des Schadens verhindert und nicht direkt dafür sorgt, die Sicherheit in Deutschland zu erhöhen.

Von daher sind diese beiden Sachen auch so ein bisschen losgelöst voneinander zu betrachten. Wenn ich irgendetwas durchführe - ob das nun eine Sanktion ist, eine diplomatische Maßnahme oder von mir aus auch eine offensive intrusive Cyberoperation -, dann ist das eine Vergeltung, eine Art Beantwortung, aber nur auf den Fall bezogen, der irgendwann mal passiert ist. Zuerst muss aber die IT-Sicherheit gewährleistet werden, die Sachen müssen wieder ins Laufen kommen, der Angriff muss abgewehrt werden. Das alles findet hauptsächlich in der Domäne des BMI oder im Sinne des Eigenschutzes bei der Bundeswehr statt.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Grundsätzlich darf man gegen einen fremden Staat nur Maßnahmen ergreifen, wenn ihm ein bestimmtes Verhalten zurechenbar ist. Es gibt aber eine Ausnahme im Völkerrecht, und das ist der sogenannte Notstand. Es mag also sein, dass die Bundesrepublik Deutschland Ziel von massiven Cyberangriffen ist, die essenzielle Interessen der Bundesrepublik Deutschland entweder beeinträchtigen oder unmittelbar zu gefährden drohen. Falls diese enge Voraussetzung gegeben ist, dann darf die Bundesrepublik Deutschland zum Beispiel mit einer offensiven Cyberoperation antworten, selbst wenn diese nicht gegen einen bestimmten Staat gerichtet, aber erforderlich ist, um unsere essenziellen Interessen zu schützen und zu wahren. Das ist aber eine sehr enge Ausnahmevorschrift.

Im Übrigen besteht keine rechte Einigkeit über die Frage, was unter dem Begriff „essenzielle Interessen“ zu verstehen ist. Wahrscheinlich sind damit grundlegende Staatsfunktionen gemeint. Möglicherweise lassen sich auch etwa der Ener-

giesektor oder das Gesundheitswesen miteinbeziehen, sodass hier eine gewisse Überlappung mit dem Begriff der „kritischen Infrastruktur“ bestehen könnte. Aber keineswegs sind die beiden Begriffe „essenzielle Interessen“ und „kritische Infrastruktur“ notwendigerweise gleichbedeutend.

Siemtje Möller (SPD): Vielen Dank. - Sie haben ja vorhin - ich weiß nicht mehr genau, wer von Ihnen es war; ich glaube, es war auf jeden Fall Herr Herpig und ein weiterer Sachverständiger - diese Ausführungen gemacht und darauf hingewiesen, dass es die Möglichkeit gibt, zwischen dem Einsatz von offensiven Mitteln und der Informationsgewinnung zu unterscheiden und dass man für die Informationsgewinnung keine Mandatierung durch das Parlament benötige. Meine Frage geht auch da an den Staatsrechtler: Gibt es einen Unterschied zwischen Cybermaßnahmen zur Informationsgewinnung und dem Einsatz von beispielsweise AWACS-Flugzeugen? Denn für die AWACS brauchen wir eine Mandatierung durch den Bundestag.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Ja, das ist auffällig im Einklang mit der Rechtsprechung des Bundesverfassungsgerichts, weil jeder Einsatz der Bundeswehr - selbst wenn er kein Kampfeinsatz ist, aber ein Eskalationspotenzial in sich trägt - grundsätzlich der Zustimmung des Deutschen Bundestages bedarf, zumindest einer nachträglichen Genehmigung.

In Bezug auf den Cyberraum verhält es sich nicht viel anders. Allerdings muss man hier sehr vorsichtig sein. Ich will jetzt nicht auf das Urteil des Bundesverfassungsgerichts zu den Schranken der Informationsgewinnung des Bundesnachrichtendienstes eingehen; aber grundsätzlich ist es natürlich so, dass jeder Einsatz missverstanden werden kann. Allein in der Tatsache, dass irgendjemand eine Informationsbeschaffung möglicherweise missversteht, sofort ein Eskalationspotenzial zu erblicken, mit der Folge, dass dann … dem Parlamentsvorbehalt … automatisch … gibt es …[1] Hier müssen wir erst mal klare Kriterien herausarbeiten, die es uns ermöglichen, festzustellen, wann die Notwendigkeit eines Parlamentsbeschlusses gegeben ist.

Siemtje Möller (SPD): Vielen Dank. - Ich habe noch eine Frage an Herrn Herpig. Es klang ja auch an, dass überlegt wird, das Nationale Cyber-Abwehrzentrum zu stärken oder umzubauen. In Gesprächen, beispielsweise auch mit dem Verbindungsoffizier, kam immer mal wieder auch das Nationale Luftabwehrzentrum - so heißt es, glaube ich - zur Sprache. Ist es aus Ihrer Sicht der richtige Weg, das Nationale Cyber-Abwehrzentrum an die Ablauf- und auch Entscheidungsprozesse dieses Zentrums anzupassen, oder sehen Sie einen anderen Weg, die nationale Cyberabwehr zu stärken?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Ich kenne die Ablaufpläne des anderen Zentrums jetzt nicht. Ich würde generell zum Nationalen Cyber-Abwehrzentrum sagen, dass es sehr schwierig zu bewerten ist, wie effektiv und effizient dieses Zentrum überhaupt arbeitet, weil die ganzen Abläufe nicht transparent und öffentlich gemacht werden. Das heißt: Wie die Behörden dort miteinander arbeiten, welche Verpflichtungen es gibt oder möglicherweise auch nicht gibt, um Informationen zu liefern, ist nicht ganz klar. Meines Wissens gibt es hier keine Informationspflichten, das heißt, dass die entsprechenden Behörden Wissen über die Vorfälle und all ihr Wissen nicht jedes Mal einbringen müssen, sondern einbringen können. Das ist natürlich ein relativ großes Problem.

Ich würde aber sagen, dass wir starken Reformbedarf beim Cyber-Sicherheitsrat haben bzw. ein Gremium auf der politisch-strategischen Ebene brauchen, das ebensolche Abwägungen trifft. Ich glaube, auf der taktisch-operativen Ebene, wo das Nationale Cyber-Abwehrzentrum auch tätig ist, wo die Informationen zusammenlaufen, ausge-

[1] Anmerkung Stenografischer Dienst: Störung der Tonübertragung

tauscht werden und auch Vorfälle analysiert werden, sind wir mit den Informationen, die öffentlich verfügbar sind, auf einem guten Wege.

Auf der strategisch-politischen Ebene wird aber eben auch überlegt: Wir haben jetzt einen Vorfall gehabt; er wurde analysiert, und er wurde in diesem Fall vielleicht sogar zugerechnet. Wie gehen wir damit weiter um? Schreiben wir ihn zu, attribuieren wir ihn also öffentlich oder gegenüber Dritten? Welche Beantwortungsmittel nutzen wir? Nutzen wir Cybermittel, nutzen wir Nicht-Cybermittel? - Diesen ganzen Prozess gibt es in Deutschland noch nicht. Da müssen wir einen Prozess aufsetzen, der ebendiese Realitäten widerspiegelt, sodass wir dann auch eine effektive, effiziente und auch irgendwie möglichst zeitnahe Beantwortung solcher Cyberoperationen gewährleisten können.

Ich glaube aber, dass wir in diesem Fall, wenn wir über Reformbedarf reden, eher das Schnittgremium auf strategisch-politischer Ebene betrachten sollten als das auf der taktisch-operativen Ebene, was das Nationale Cyber-Abwehrzentrum wäre.

Siemtje Möller (SPD): Vielen Dank. - Ich würde die restlichen Minuten an meinen Berichterstatter Dirk Vöpel weitergeben.

Dirk Vöpel (SPD): Vielen Dank, auch für die einführenden Vorträge. - Ich hätte erst mal eine Informationsfrage an Herrn Herpig. In Ihren Unterlagen schreiben Sie über die Unterscheidung zwischen Informationsgewinnung, die noch nicht intrusiv ist, und der intrusiven Aufklärung. Können Sie vielleicht noch mal etwas praktischer erläutern, was man sich als Laie konkret darunter vorzustellen hat, wo man die Unterscheidung genau machen kann? Welcher Fall könnte da möglicherweise das eine und welcher Fall das andere sein?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Ja, sehr gerne. - Wenn ich zum Beispiel Passwörter breche, errate oder andere Sicherheitsmechanismen überwinde, sprechen wir von Aufklärung; das ist intrusiv. Dann gehe ich in ein System rein, ich übergehe Sicherheitsmaßnahmen; da können wir von Aufklärung sprechen.

Von Informationsbeschaffung sprechen wir dann, wenn keine Sicherheitsmechanismen übergangen werden. Ich glaube, der Grenzfall ist: Sie sind auf der Suche nach Informationen über den Angreifer, die Angreiferin, und Sie finden einen offenen AWS-Bucket, in dem Daten liegen: vielleicht Blaupausen, vielleicht Zielelisten. Dieser Bucket ist aber nicht über Passwörter geschützt, er ist frei verfügbar und im Internet zugänglich. Wenn Sie dann Informationen runterladen, um sich besser zu informieren, wäre das noch nicht der Schritt zu intrusiven offensiven Maßnahmen, weil keine Sicherheitsmaßnahmen übergangen werden. Das läge noch im Bereich der Informationsbeschaffung.

Dirk Vöpel (SPD): Vielen Dank. - Sie haben, wenn ich das richtig verstanden habe, vorhin gesagt, dass die Bundeswehr im Cyberbereich eigentlich gar keinen Beitrag zur Verteidigung leisten kann; das war für mich schon sehr deutlich so. Dazu die Frage: Wenn man jetzt davon ausgeht, dass die Zuordnung eines Angriffs ja relativ lange dauern kann - das haben wir ja gerade schon diskutiert -, welchen Beitrag könnte denn aus Ihrer Sicht die Bundeswehr dann überhaupt leisten?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Wie gesagt: Ich glaube, dass neben dem Eigenschutz auch die Möglichkeit der Amtshilfe nach Artikel 35 Grundgesetz besteht. Das heißt, wenn wir Großschadensfälle haben, wie zum Beispiel mit den Exchange-Servern, oder wenn viele Universitäten gleichzeitig Ziele von Ransomware-Angriffen werden, dann könnte die Amtshilfe der Bundeswehr beantragt werden, und die Bundeswehr könnte dann eben auch zur Sicherheit beitragen.

Auf der anderen Seite ist es vollkommen richtig, dass das Ganze, wenn sozusagen die Attribuierung unklar ist, eher im Bereich des BMI liegen würde. Fast alle Angriffe, die wir sehen, können nachrichten-/geheimdienstlich oder der OK, der Organisierten Kriminalität, zugeordnet werden.

Sie liegen damit nicht im Bereich der Bundeswehr. Von daher sollte man eigentlich immer davon ausgehen, dass die Reaktionen auf einen Cyberangriff oder einen Vorfall erst mal im Ressort des BMI, namentlich des Bundeskriminalamts, des Verfassungsschutzes und BSI bzw. bei den entsprechenden Länderpendants, liegt.

Dirk Vöpel (SPD): Schönen Dank. - Ich glaube, für die erste Runde haben wir jetzt nicht mehr allzu viel Zeit übrig. Ich würde dann weitergeben. - Danke.

Vorsitzender Wolfgang Hellmich: Vielen Dank. - Dann hat der Kollege Müller für die FDP-Fraktion das Fragerecht. Bitte sehr.

Alexander Müller (FDP): Vielen Dank. - Auch von unserer Seite vielen Dank an die Experten. - Wir hätten eine Frage in Richtung der Zielgerichtetheit von Cyberwirkmitteln. Wir haben ja in der Diskussion jetzt gehört, dass Cyberoffensivmittel oder Cyberwirkmittel Kollateralschäden verursachen könnten und man deswegen natürlich sehr vorsichtig sein muss. Auf der anderen Seite ist es natürlich so: Wenn man eine militärische Auseinandersetzung in erster Linie mit Cyberfähigkeiten führen und damit die Wirkungen unter Verzicht auf kinetische Mittel erzielen kann, dann - das sagt einem der gesunde Menschenverstand - treten deutlich weniger Kollateralschäden ein.

Ich glaube, diese Frage wäre gut für den Praktiker Dr. Koch aufgrund seiner Erfahrung. Dabei geht es mir jetzt nicht um die Wirkmittel von Organisierter Kriminalität - da gibt es ja mit Sicherheit Malware und Viren, die Kollateralschäden verursachen -, sondern um militärische Cyberwirkmittel. Wie zielgerichtet können die wirken, was kann man da aus der Erfahrung heraus sagen? Welche Kollateralschäden kann es geben?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Ich finde, das ist eine sehr gute Frage, Herr Abgeordneter. - Ich würde sagen, der militärische Bereich zeichnet sich dadurch aus, dass wir da tatsächlich eine sehr hohe Zielgerichtetheit generieren können, was schon allein damit begründet ist, dass wir uns ja typischerweise auf entsprechende Hochwertziele ausrichten und diese eine entsprechende Charakteristik haben.

Sie haben Schadsoftware wie Ransomware etc. genannt, die heutzutage stellenweise auch zielgerichteter eingesetzt wird; aber die hat natürlich ein ganz anderes Spektrum. Das betrifft den Rechner X und, sagen wir mal, den und den Server. Der Angreifer versucht eben, weil er in dem Bereich mehr Geld machen kann, auf das Krankenhaus etc. loszugehen. Aber das ist keine Zielgerichtetheit, wie wir sie in dem Sinne eines Cyberwirkmittels im Rahmen des militärischen Umfeldes generieren können.

An praktischen Beispielen, die wir gesehen haben - da gibt es ja nicht so endlos viele -, ist natürlich Stuxnet als Operation auf die Urananreicherungsanlagen im Iran zu nennen. Da hat man ja gesehen, dass, obwohl der Wurm dann letztendlich verbreitet worden ist - über die Gründe kann man diskutieren -, letztendlich nur die eigentliche Anlage betroffen war, das Mittel also sehr, sehr genau zugeschnitten worden ist. Auf allen Rechnern, auf denen es sich weltweit verbreitet hat, was natürlich unschön und ein Stück weit auch unnötig war, ist es nirgends zur Wirkung gekommen, sondern es hat den Effekt tatsächlich nur an der Stelle ausgelöst, wo es ihn generieren sollte. Das ist ein Spezifikum, was wir im Bereich der militärischen Operationen erreichen können.

Alexander Müller (FDP): Vielen Dank. - Die zweite Frage, die ich an Prof. Heintschel von Heinegg und auch an Admiral Daum stellen möchte, ist eine eher rechtliche Frage über völkerrechtliche Verträge zur Regelung oder zur Abrüstung in Bezug auf Cyber. Gibt es bereits erste Diskussionen darüber, dass man versucht, völkerrechtliche Verträge zu erreichen? Gibt es vielleicht sogar auch Vorschläge von Ihnen? An welcher Stelle könnte man dort internationale Verträge schließen, um Einigungen hinsichtlich der militärischen Auseinandersetzungen mit Cybermitteln hinzubekommen?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Es gibt seit Beginn des 21. Jahrhunderts oder - das kann

man sagen - schon seit Ende des 20. Jahrhunderts Vorschläge von verschiedenen Staaten, darunter auch der Russischen Föderation, zu einem sogenannten Rüstungskontrollvertrag im Cyberraum. Die Russische Föderation hat dieses Ansinnen lange verfolgt.

Ich persönlich glaube aber, dass dieses Ansinnen aus unterschiedlichen Gründen nicht von Erfolg gekrönt sein wird.

Erstens ist nicht klar, ob und inwieweit die Russische Föderation sich selber an die Vorgaben eines solchen Abkommens halten würde. Der Begriff der hybriden Kriegsführung oder der hybriden Bedrohung ist ja schon mehrfach genannt worden.

Zweitens ist es so, dass der Entwicklungsstand der Staaten sehr unterschiedlich ist. Ich stimme zwar zu, dass wir in Deutschland viele gute und kluge Köpfe haben und das Know-how da ist, gleichwohl die praktischen Fähigkeiten nicht gegeben sind. Wir müssen einfach erkennen, dass andere Staaten nicht nur das Know-how haben, sondern auch die Fähigkeiten schon generiert haben und wohl nicht bereit sein werden, in irgendeiner Weise die Nutzung dieser Fähigkeiten durch einen völkerrechtlichen Vertrag einzuschränken.

Hinzu käme natürlich noch das weitere Problem der Verifizierung oder etwa der notwendigen vertrauensbildenden Maßnahmen, die im Cyberraum natürlich weitaus schwieriger sind als etwa im Bereich der strategischen oder auch konventionellen Bewaffnung von Staaten.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Ja, vielen Dank. - Mir sind keine Überlegungen bekannt, Aktivitäten zu Rüstungskontrollmaßnahmen im Cyber- und Informationsraum vorzunehmen, so wie man das von Streumunition oder Minen etc. kennt. Vorstellbar ist es natürlich, aber derzeit habe ich keine Erkenntnisse, dass das stattfindet. - Vielen Dank.

Alexander Müller (FDP): Ja, vielen Dank. - Herr Admiral, ich bleibe bei Ihnen. Die Frage ist natürlich in einer öffentlichen Konferenz schwierig, aber vielleicht können Sie trotzdem etwas dazu sagen. Ich frage nach Fähigkeitslücken der Bundeswehr im Cyberraum. Haben Sie Wünsche in Bezug auf Personal, in Bezug auf Ausstattung, wo aus Ihrer Sicht Fähigkeitslücken bestehen, die wir auffüllen müssen?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Ja, vielen Dank. Das ist eine tolle Frage. Dazu nehme ich natürlich gerne Stellung. - Ich will dabei aber natürlich lieber die CIR-Fähigkeiten ansprechen und nicht die Fähigkeiten, die möglicherweise ein Zentrum Cyber-Operationen in meinem Bereich braucht.

Ich habe mehrfach betont, dass Aufklärung in dieser Hinsicht besonders wichtig ist. Sie wissen natürlich, dass wir beispielweise bei luftgestützten Systemen - Stichwort PEGASUS -, bei dem Ersatz der Flottendienstboote, die ja ganz wesentlich der Aufklärung dienen, durchaus einen erheblichen Bedarf haben, die Fähigkeiten zu regenerieren oder auch entsprechend zu erweitern. - Vielen Dank.

Alexander Müller (FDP): Damit dürfte unsere Zeit rum sein. Wir machen in der nächsten Runde weiter.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann hat die Kollegin Brugger für die Fraktion Bündnis 90/Die Grünen das Wort. Bitte sehr.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Das ist sehr nett, aber ich glaube, dass der Kollege Neu von der Linkspartei den Vortritt vor mir hat.

Vorsitzender Wolfgang Hellmich: Ich war zu flott. Das stimmt, Entschuldigung. - Der Kollege Neu. Bitte sehr.

Dr. Alexander S. Neu (DIE LINKE): Ja, vielen Dank, Herr Kollege Hellmich. Noch sind die Grünen gegenüber den Linken nur bei Umfragen führend, aber noch nicht in dem Bundestagswahlergebnis. Insofern vielen Dank, Kollegin Brugger.

Ja, ich möchte zunächst mit dem Parlamentsbeteiligungsgesetz anfangen. Wenn man sich die

Begriffsbestimmung in § 2 und auch in § 1 des Parlamentsbeteiligungsgesetzes anschaut, dann wird ja relativ deutlich, dass es ein Gesetz ist, das sich auf den Schutz der zu entsendenden Soldaten bezieht, und dass der Bundestag erst dann eine Mitbestimmung bekommt, wenn es sozusagen um das Wohl und Wehe der Soldaten im Felde geht, sprich: bewaffnete Einsätze.

Nun wurde das Gesetz 2005 etabliert, also zu einer Zeit, wo die analoge Kriegsführung, noch nicht die digitale, im Mittelpunkt stand. Das hat sich durch die Digitalisierung jetzt ein bisschen geändert; deshalb sitzen wir ja auch hier. Von daher glaube ich, dass das Parlamentsbeteiligungsgesetz an sich überhaupt erst mal generell überholt werden muss, das heißt, den aktuellen Entwicklungen der Cybermöglichkeiten angepasst werden muss. Denn das, was wir bislang vorliegen haben, bezieht den digitalen Bereich noch nicht mit ein. - Das ist meine Vorbemerkung.

Ich habe eine Vielzahl an Fragestellungen, werde aber jetzt erst mal mit einer Frage an Herrn Inspekteur Daum anfangen. Sie haben ja darauf hingewiesen, dass die Bundeswehr im Wesentlichen Eigenschutz betreibe, was ja auch völlig legitim ist; kein Zweifel daran. Ich bin auch immer mal wieder im Gespräch mit dem BSI. Da habe ich schon so ein bisschen den Eindruck bekommen, dass da ein Konkurrenzverhältnis zwischen dem BSI und dem CIR besteht, aber eher ausgehend von der Bundeswehr, die gewissermaßen versucht, dem BSI den Futternapf streitig zu machen, um es mal so auszudrücken, das heißt, auch in den Zuständigkeitsbereich des BSI hinein zu agieren. Was können Sie dazu sagen? Wo gibt es da Überschneidungen? Wo gibt es da vielleicht Kompetenzstreitigkeiten, vielleicht nicht formaler Art, aber in der praktisch-operativen Arbeit?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Ja, vielen Dank, Herr Abgeordneter, für die Frage. - Also, von Kompetenzstreitigkeiten würde ich da natürlich überhaupt nicht sprechen; aber das haben Sie jetzt von mir als Antwort auch nicht erwartet.

Grundsätzlich sind aus meiner Sicht die Rolle des BSI und die Rolle der Bundeswehr klar voneinander abgegrenzt. Wir sind ein enger Partner des BSI, so möchte ich das mal nennen. Wir arbeiten mit dem BSI eng zusammen; denn alles, was wir an Systemen für die Bundeswehr einsetzen, muss natürlich auch den entsprechenden Anforderungen genügen. Das heißt, was die Zertifizierung der IT-Sicherheit unserer Anlagen betrifft: Da gehen wir natürlich ganz wesentlich auf die Vorgaben des BSI ein.

Ich meine auch nicht, dass irgendwo zu erkennen ist, dass die Bundeswehr beim Thema Cybersicherheit oder beim Thema Informationssicherheit glaubt, dem BSI hier irgendwelche, sagen wir, Empfehlungen geben zu können, dass wir da in irgendeiner Weise eine wertigere Stellung hätten oder sogar eine bessere Fähigkeit. Also, ich stehe im regelmäßigen Kontakt mit dem Präsidenten des BSI, und er hätte mir sicherlich gesagt, wenn er mit irgendwelchen Dingen unzufrieden wäre.

Wenn Sie in den Entwurf des neuen IT-Sicherheitsgesetzes 2.0 schauen, dann werden Sie natürlich an irgendeiner Stelle die Formulierung finden, dass die Bundeswehr durchaus die Möglichkeit bekommen soll, für eigene Systeme in gewissen Situationen auch eigene Entscheidungen zu treffen. Das ist dort verankert. Es wird dort aber auf entsprechende Servicelevel, Agreement-Verträge - ich weiß gar nicht, wie der genaue Begriff im Gesetz jetzt lautet - hingewiesen, sodass wir uns also in der Frage eng abstimmen, wo die Bundeswehr von Empfehlungen des BSI abweichen würde.

So muss man klar sehen: Das ist dann in diesem IT-Sicherheitsgesetz sicherlich geregelt. Ich begrüße auch sehr, dass es in dieser Weise drinsteht. Ich kenne aber noch keinen praktischen Fall. Solch ein Regelwerk gibt es ja schon seit vielen Jahren, und mir ist kein einziger Fall bekannt, wo die Bundeswehr gegen eine Empfehlung des BSI Entscheidungen für den Einsatz der eigenen Systeme getroffen hätte. Am Ende ist nämlich sowohl die Empfehlung des BSI wie auch die Bewertung aufseiten der Streitkräfte immer die, eine Risikoabschätzung vorzunehmen.

Diese ist in der Regel unter Technikern recht einvernehmlich.

Wenn Sie dort einen Punkt sehen: In dem IT-Sicherheitsgesetz sehe ich das nicht. Ich erkenne auch bisher keine Zerwürfnisse oder Rivalitäten zwischen diesen beiden Behörden; eher ist das Gegenteil der Fall. - Vielen Dank.

Dr. Alexander S. Neu (DIE LINKE): Vielen Dank für die Aufklärung. - Bei mir ist im Laufe dieser Veranstaltung der Eindruck entstanden, dass offensive Cyberoperationen gutgeheißen werden, gewissermaßen als alternativlos betrachtet werden. Es fiel auch, soweit ich mich zurückerinnere, die Formulierung, dass sie sehr zielgenau stattfinden könnten.

Da habe ich jetzt meine Zweifel, auch mit Blick auf die Attribuierung. Es wurde ja mehrfach gesagt, dass diese Operationen sehr zeitintensiv und arbeitsintensiv seien. Meine Frage an Herrn Thomas Reinhold: Wie genau können Sie die Zielgenauigkeit von Cyberoffensivoperationen beurteilen? Ist das überhaupt machbar?

Sachverständiger Dipl.-Inf. Thomas Reinhold (TU Darmstadt): Danke für die Frage. - Ich glaube, wenn man sich zum Beispiel andere Kräfte, wie die USA, anschaut, die da ein ganz anderes Vorgehen haben, dann sieht man: Sie haben tatsächlich eine zielgenaue Strategie. Sie unterstützen diese Strategie natürlich dadurch, dass sie in Friedenszeiten gefühlt den Fuß in jeder IT-Tür haben und im Zweifelsfall dann bei Bedarf auf die entsprechenden Informationen zugreifen können.

Für die Bundeswehr würde ich das auf jeden Fall nicht so sehen. Wir hatten ja vorhin schon das Beispiel von der Kaltstartfähigkeit. Wenn wir zielgenau agieren wollen, auch gegen unterschiedliche Akteure, gegen unterschiedliche Bedrohungen, müssten wir uns - vielleicht nicht im gleichen Umfang, aber von der Herangehensweise her - an den USA ein Beispiel nehmen.

Wo wir dann Probleme kriegen: Wer soll das machen? Soll es der BND machen? Wie kann so was parlamentarisch kontrolliert werden? Um die Antwort abzukürzen, würde ich sagen: Die offensive Zielgenauigkeit kann ich bei der Bundeswehr einfach nicht sehen.

Dr. Alexander S. Neu (DIE LINKE): Vielen Dank. - Wie viel Zeit habe ich noch?

Vorsitzender Wolfgang Hellmich: Keine mehr.

Dr. Alexander S. Neu (DIE LINKE): Wunderbar.

Vorsitzender Wolfgang Hellmich: Die Kollegin Brugger bekommt das Wort. Bitte sehr.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Ja, vielen Dank, Herr Vorsitzender. Genau, jetzt bin ich auch wirklich dran. - Ich möchte mich erst mal bei allen Expertinnen und Experten für ihre schriftlichen, aber auch mündlichen Stellungnahmen ganz herzlich bedanken, die sehr, sehr, interessant sind.

Ich möchte nur eine kurze Vorbemerkung machen. Es ist ja nicht die erste Anhörung, die wir als Ausschuss zu diesen wichtigen Themen durchführen. Ich würde mir sehr wünschen, dass wir auch im Alltagsgeschäft immer wieder und noch viel häufiger über diese extrem wichtigen Fragen sprechen könnten, was dann auch zur parlamentarischen Kontrolle führt.

Aber ich hätte zuerst noch mal eine andere Frage, nämlich an Frau Schuetze. Sie haben in Ihrer schriftlichen Stellungnahme zwei Fallbeispiele aufgeführt: einmal das Vorgehen der USA - dazu haben Sie ja auch schon einiges ausgeführt - und dann ein ganz anderes Vorgehen vonseiten Japans. Was für Lehren könnten sich eigentlich für die deutsche Cyberpolitik aus dem ergeben, was Japan macht, das sich auch Grenzen auferlegt, aber durchaus auch viel für Schutz und Resilienz tut? Was können Sie uns da für die praktische Politik mitgeben?

Sachverständige Julia Schuetze (SNV e. V.): Ja, vielen Dank. - In Bezug auf Offensivfähigkeiten zur Aufklärung und Wirkung von Angriffen erklärte Japan, dass die Neuinterpretation von Artikel 9 der pazifistischen Verfassung nicht für die Aktivitäten der japanischen Self-Defense Forces

gilt. Dabei hat Japan öffentlich anerkannt - das ist wichtig; das muss auch Deutschland tun -, dass man einordnen muss, wo Offensivfähigkeiten eingesetzt werden und warum. Dadurch schafft man auch Fakten. Dabei muss man natürlich seine eigene Verfassung, bei uns das Grundgesetz, miteinbeziehen.

Die japanische Regierung hat quasi geschlussfolgert, dass sich die zivile Verteidigungsgruppe ständig bereithalten und üben müsste, um weiträumig beständige Aufklärung und Überwachung im Innern zu betreiben. Das bedeutet konkret für die Cyberverteidigung und Cyberabwehr zum Beispiel 24-Stunden-Überwachung von den eigenen Systemen und von Informationssystemen sowie auch erweiterte Maßnahmen gegen Cyberangriffe sowie Malware-Analyse durch die Verteidigungsgruppe.

Im Vergleich zu den USA ist es heute so, dass diese Verteidigungsgruppe dann die Informationsgewinnung nur auf dem eigenen Territorium betreibt - so ähnlich, wie das wahrscheinlich auch die Bundeswehr mit ihrem Lagebericht macht -, aber nicht nach außen geht, weil das mit der pazifistischen Verfassung nicht vereinbar ist.

Von daher sehe ich das Potenzial, dass in Deutschland auch noch mal klarer unterschieden wird: Welche Mittel nutzen wir zur Informationsgewinnung? In Deutschland gibt es wahrscheinlich auch das Potenzial, so wie Herr Herpig ja auch differenziert hat, Möglichkeiten und offensivere Mittel auch außerhalb des Lands zu benutzen. Aber für die Aufklärung und Wirkung von Angriffen, also da, wo man invasiv vorgehen muss, braucht es dann den Parlamentsvorbehalt. Das ist auch zu kommunizieren.

Diese Auslegung macht jetzt Japan. Die USA schaffen entsprechende Fakten. Frankreich hat zum Beispiel eine offensive Doktrin, in der ausgelegt wird, wie weit die Aktivitäten gehen und wo die Grenzen sind. Ich würde der Bundesregierung empfehlen, genau da Fakten zu schaffen und auch das Grundgesetz und den Parlamentsvorhalt usw. anzuwenden.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Vorhin hatten Sie noch mal die Stellungnahme des Auswärtigen Amtes und des Verteidigungsministeriums im Hinblick auf die Doktrin der USA angesprochen, die Netze oder die Infrastruktur, ich würde mal sagen, unbeteiligter Dritter zu nutzen, um militärische Ziele zu verfolgen.

Es wurde in dieser Stellungnahme nicht ausgeführt: „Das ist für uns ein absolutes No-Go“, sondern darin sind gewissen Schwellen festgelegt worden. Sie haben auch gesagt, dass Sie diese nicht für ausreichend halten. Was hätte man also noch präziser formulieren sollen? Ich spitze mal zu: Ist es dann nicht fast schon eine Einladung, verbunden mit der Frage, welche Staaten dann dürfen und welche Staaten nicht dürfen? Muss man da nicht eine viel klarere Grenze ziehen?

Sachverständige Julia Schuetze (SNV e. V.): Ja, auf jeden Fall. Also, hier bewegen wir uns - das gilt erst mal für die USA - unterhalb der Schwelle eines bewaffneten Angriffs. Das kann aber durchaus dazu führen, dass sie in der Theorie unsere Systeme nutzen, um dann einen bewaffneten Angriff vorzunehmen. Da ist es wichtig, dass man das nicht nur völkerrechtlich einordnet, sondern auch die Diskussion der Normen für das Verhalten im Cyberraum mit bedenkt und das auch für sich auslegt und kommuniziert.

Im Fall der USA wäre es zum Beispiel möglich, vielleicht auch auf europäischer Ebene, diesen Prozess im Cyberdialog, der mindestens einmal im Jahr stattfindet, zu erklären und auch anzusprechen. Man könnte zum Beispiel definieren, dass die USA KRITIS-Unternehmen ausnehmen sollten und dass uns die USA im Rahmen des Due-Diligence-Prinzips, das wir ja unterstützen, in Kenntnis setzen müssten, falls solche Angriffe vorbereitet oder ausgetragen werden sollen. Also, da könnte man einfach auch mal das Gespräch suchen und sich klar positionieren - vielleicht auf der europäischen Ebene -, weil Deutschland garantiert nicht das einzige Land ist, das sich mit dieser Frage gerade beschäftigt.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Ich hätte noch viele Fragen, aber

ich glaube, ich darf nicht mehr und muss an den Vorsitzenden zurückgeben. Ich freue mich auf die zweite Runde.

Vorsitzender Wolfgang Hellmich: Ich wollte gerade sagen: Die zweite Runde kommt bestimmt. - Dann kommen wir eben zu dieser zweiten Runde. Als Erste hat die CDU/CSU-Fraktion das Rederecht. Ich habe hier den Namen von Professor Dr. Sensburg stehen. Bitte sehr.

Dr. Patrick Sensburg (CDU/CSU): Wunderbar. Dann fange ich mal an. Ich glaube, mein Kollege Herr Gnodtke wird danach übernehmen.

Ich fange mit einer Frage an Professor Wolff Heintschel von Heinegg zum Völkerrecht an. Wenn ich es eben richtig verstanden habe, hatten Sie gesagt: Das Völkerrecht gibt so viel noch nicht her. - Mich würde schon interessieren, welche Ansätze einer völkerrechtlichen Einordnung es gibt. Mit Blick auf die Aktivitäten des Auswärtigen Amtes möchte ich fragen: Wie kann man Regelungen schaffen? Wie kann man bestimmte Sachen einhegen? Was gibt es da? Ich wäre schon daran interessiert, im Rahmen der Antwort auf meine erste Frage zu erfahren: Wie entwickelt sich das ganze Völkerrecht? Kann uns das irgendeinen Rahmen geben? Oder ist es so: „Alles ist offen, alles kann gemacht werden, und so sollten wir es dann auch machen“?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Vielen Dank, Herr Abgeordneter.

Dr. Patrick Sensburg (CDU/CSU): Ich freue mich übrigens, Sie zu sehen.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Ganz meinerseits. - Ganz so schlimm ist es natürlich nicht. Es ist keineswegs so, dass man im Cyberraum machen könnte, was man will; natürlich nicht. Es besteht aber, wie gesagt, nur dieser Minimalkonsens, von dem ich ja vorhin gesprochen habe, insbesondere soweit Operationen durch den Cyberraum betroffen sind.

Ich glaube, der Versuch, im Rahmen der UN GGE, also der Group of Governmental Experts, einen Konsens in der Frage zu erzielen, ob und inwieweit Völkerrecht, wie es heute besteht, auch bei Cyberoperationen Anwendung finden kann, war durchaus zu begrüßen. Er ist ja letztendlich leider gescheitert, weil die Staaten sich nicht einigen konnten, insbesondere über die Anwendbarkeit des humanitären Völkerrechts, das bei bewaffneten Konflikten angewendet wird. So haben wir auch hier schon erste Ansätze, auf denen wir aufbauen können.

Ich persönlich bin der Meinung, dass wir hier ein wirklich sehr gutes Dokument haben, nämlich das berühmte Tallinn-Handbuch. Es wäre eigentlich mal zu erwarten gewesen, dass auch vonseiten der zuständigen Ministerien mehr kommt als lediglich eine pauschale Ablehnung. Das hat mich sehr geärgert. Augenscheinlich war es so, dass sich das keiner wirklich mal von vorne bis hinten durchgelesen hat. Vielmehr kam nur: Das ist ja nur diese Expertengruppe.

Interessanterweise aber ist es so, dass sich viele andere Regierungen das, was sie im Tallinn-Handbuch finden, durchaus zu Herzen nehmen. Ich sage ja nicht, dass alles, was Sie in diesem Handbuch finden, sozusagen in Marmor gemeißelt ist. Aber es wäre sicherlich eine gute Gesprächsgrundlage und Diskussionsgrundlage, um Klarheit darüber zu schaffen, welche Bestimmungen, welche Kommentierungen in diesem Handbuch etwa seitens des Ministeriums der Verteidigung oder des Auswärtigen Amtes für richtig oder zumindest für begrüßenswert gehalten werden.

Es ist eine Menge da. Es ist keineswegs so, dass wir kein Material, keine Stellungnahmen haben. Dazu gibt es viele. Ich habe ja in meiner Stellungnahme auch die vielen nationalen Cybersicherheitsstrategien bemüht, und das geht ja auch weiter. Wir sollten uns nur mal dazu verhalten.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. - Jetzt kommt die nächste Frage von meinem Kollegen Herrn Gnodtke, vermute ich.

Eckhard Gnodtke (CDU/CSU): Die erste Frage geht an Herrn von Heinegg: Wo sehen Sie Anpassungsbedarf bei bestehenden internationalen und nationalen Regelungen? Die zweite Frage lautet: Wann überschreiten Akte der Cyberspionage, der Cyberüberwachung oder des Datenklaus die Schwelle zu einem Cyberangriff? Ab wann wäre eine offensive Militäroperation als Gegenmaßnahme völkerrechtlich zulässig?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Wenn ich Sie recht verstanden habe, ging die Frage an mich. Fangen wir mit dem Ersten an: Es gibt kein Spionageverbot im Völkerrecht; Spionage ist bestenfalls nach nationalem Recht unzulässig.

Wenn Sie sich erinnern, hat Herr Herpig zwischen intrusiven und nichtintrusiven Operationen unterschieden. Diese Unterscheidung hilft bei der Beurteilung, ob es sich bei einer Cyberoperation bloß um nicht verbotene Spionage oder schon um eine Völkerrechtsverletzung oder gar um einen bewaffneten Angriff handelt, nicht viel weiter; denn Spionage ist per se im Zweifel intrusiv, sodass dieses Element uns wenig weiterhilft.

Wichtig ist, dass wir klar und deutlich zu erkennen geben, ab welchem Schadensmaß wir bereit sind, auch in den Fällen, in denen sich die Wirkungen einer Cyberoperation nicht in der physischen Domäne materialisieren, von einem bewaffneten Angriff auszugehen. Das bedeutet nicht eine Selbstverpflichtung, sondern das ist nur ein Signal an potenzielle Angreifer, dass bei bestimmten schädigenden Cyberoperationen die Bundesrepublik Deutschland durchaus in Erwägung zieht, von ihrem Selbstverteidigungsrecht Gebrauch zu machen.

Im Übrigen sollte ebenfalls deutlich werden, dass die Bundesrepublik Deutschland bereit ist, auch bei maliziösen Cyberoperationen, die unterhalb der Gewalt- oder Angriffsschwelle verbleiben, notfalls in Form von Gegenmaßnahmen zu reagieren, ohne dass sie sich da zu einem bestimmten Verhalten verpflichtet. Sie sollte das klare Signal aussenden, dass sie durchaus bereit ist, hier von dem gesamten Folterinstrument, dass das Völkerrecht zur Verfügung stellt, Gebrauch zu machen. Damit wäre ein erster wichtiger Schritt getan.

Eckhard Gnodtke (CDU/CSU): Eine ergänzende Frage dazu: Wie ist denn die Rechtslage, wenn die Angriffshandlung von sogenannten - in Anführungsstrichen - „patriotischen Hackern“ ohne Staatsauftrag ausgeht, die Angriffshandlung aber im nützlichen Interesse eines fremden Staates liegt? Mit anderen Worten: Reicht die Befürwortung bzw. die nichtöffentliche Zustimmung zu einem Cyberangriff eines nichtstaatlichen Akteurs für die Zurechnung zu einem staatlichen Handeln aus?

Dann, wenn wir noch etwas Zeit haben, die Frage: Wie ist es rechtlich zu beurteilen, wenn ein Cyberangriff vom Server eines unbeteiligten Drittstaates ausgeht? Wäre in einem solchen Fall eine offensive Cyberoperation gegen den Drittstaat als Verteidigungshandlung völkerrechtlich zulässig? - Die Fragen gehen noch einmal an Sie, Herr von Heinegg.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Die Verhaltensweisen privater Akteure sind einem Staat jedenfalls dann zuzurechnen, wenn diese privaten Akteure unter der effektiven Kontrolle eines Staates oder im Auftrag des Staates handeln. Das festzustellen, ist natürlich nicht einfach, sodass ich Ihnen jetzt nur die reine theoretische Rechtslage darlegen kann. Das andere Beispiel hatte ich Ihnen vorhin schon genannt: Es handelt ein privater Akteur, ohne dass dieser private Akteur unter der effektiven Kontrolle eines Staates stünde, aber der Staat anerkennt dieses Verhalten und macht es sich zu eigen. Auch dann ist das Verhalten privater Akteure zurechenbar.

Sind diese Voraussetzungen nicht gegeben, wird dem Zielstaat einer solchen Operation am Ende des Tages nur der Notstand bleiben, dessen Anwendbarkeitsschwelle aber denkbar hoch ist, weil es, wie gesagt, um essenzielle Interessen eines Staates gehen muss und diese essenziellen Interessen, wie vorhin schon bemerkt, nicht mit der kritischen Infrastruktur gleichgesetzt werden dürfen.

Eckhard Gnodtke (CDU/CSU): Vielen Dank. Keine weiteren Fragen.

Dr. Reinhard Brandl (CDU/CSU): Darf ich noch eine Frage vonseiten der Union nachschieben?

Vorsitzender Wolfgang Hellmich: Ja, es ist noch Zeit.

Dr. Reinhard Brandl (CDU/CSU): Ich hätte noch eine Frage an Herrn Vizeadmiral Daum bezüglich des Einsatzes von Cyberkapazitäten in Auslandseinsätzen der Bundeswehr: Spielt das heute bereits eine Rolle? Oder könnte der Einsatz von Cyberkapazitäten aus Ihrer Sicht einen nützlichen Beitrag bezüglich aktueller Fragestellungen in den Einsatzgebieten leisten?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank. - Selbstverständlich spielt das eine Rolle, wobei ich natürlich jetzt hier auf den Anteil „Cyber- und Informationsraum und Aktivitäten“ eingehe im Sinne der Definition, die ich am Anfang genannt habe, nämlich den Cyberraum, das elektromagnetische Umfeld und das Informationsumfeld betreffend. Das spielt natürlich in diesem Kontext eine Rolle; denn wir versuchen mit unserem Beitrag in Auslandseinsätzen, die eigenen Kräfte vor Ort zu unterstützen.

Sie können sich vorstellen, dass bei einem Auslandseinsatz in einer Konfliktregion gleichzeitig Effekte auftreten: a) Ausfälle in den IT-Systemen, b) Störungen im elektromagnetischen Umfeld, also beispielsweise im Bereich Mobilfunk oder Überwachungsradar, c) Informationskampagnen im Einsatzland gegen unsere dort stationierten militärischen Kräfte werden beobachtet. So etwas kann Einfluss auf die Einsatzbereitschaft der Kräfte haben. Wenn es um Informationskampagnen geht, kann das auch Einfluss auf ihre Reputation vor Ort haben.

Auf solche Effekte konzentrieren wir uns im CIR. Wir versuchen, aus räumlichen und zeitlichen Koinzidenzen Zusammenhänge herzustellen. Damit kommen wir letztlich zu der Frage: Sind das zufällige Ausfälle, sind das möglicherweise zusammenhängende Nadelstiche, und steht dahinter möglicherweise eine Kampagne, die sich gegen den Einsatz unserer Kräfte im Ausland richten? Wir agieren zu einem gewissen Teil mit Kräften im Einsatzland vor Ort, aber natürlich ganz wesentlich auch durch Rückgriff auf die Kräfte hier im Inland, im Sinne des Reach-Back.

In diesem Sinne ist die Antwort kurz: Ja, das spielt eine Rolle. - Vielen Dank.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Wir haben jetzt noch nicht oder nur ganz am Rande über die Rolle der NATO gesprochen. Alle Fähigkeiten, die wir anbieten, versuchen wir im NATO-Kontext einzubringen. Haben Sie eigentlich bestimmte Fähigkeiten aus Ihrem Bereich bei der NATO angemeldet?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Die NATO hat vor einigen Jahren begonnen, den Cyberraum als eine militärische Dimension zu definieren; das war auch der Auslöser für viele Staaten. Die NATO betrachtet sich als Verteidigungsbündnis. Insofern ist es nicht Absicht der NATO, eigene Fähigkeiten dazu aufzubauen. Die NATO beschränkt sich in diesem Falle auf den Schutz durch entsprechende Cybersicherheitszentren etc.

Im Rahmen militärischer Operationen ist aber immer die Frage zu stellen: Welche Fähigkeiten helfen auf dem Weg zum Ziel? Insofern schließt auch die NATO nicht aus, dass in militärischen Operationen, insbesondere wenn wir jetzt über das Szenar Landes- und Bündnisverteidigung sprechen - in diesem Fall Bündnisverteidigung -, Cybereffekte eine Rolle spielen. Vor diesem Hintergrund hat die NATO einen Diskussionsprozess mit den Nationen gestartet zu der Frage: Wer sieht sich in der Lage, der NATO entsprechende Beiträge zu stellen? Bei dieser Frage, die an Deutschland gerichtet wurde, hat Deutschland auch erklärt, dass wir bereit wären, der NATO Effekte zur Verfügung zu stellen. - Danke.

Dr. Reinhard Brandl (CDU/CSU): Gibt es in der Diskussion mit der NATO eigentlich eine Organisation im Sinne von „Deutschland stellt Aufklä-

rungskapazitäten oder offensive Kapazitäten, differenziert nach bestimmten Netztypen usw., zur Verfügung“? Wie kann man sich eine Aufgabenteilung im Cyberraum ganz praktisch vorstellen?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Grundsätzlich richtet sich die Frage nach dem Beitrag einzelner Nationen auch an spezielle Fähigkeiten. Das ist in dieser Hinsicht natürlich differenziert. Das hängt immer davon ab, welche Fähigkeiten, welche Effekte relevant sind. Aber dafür gibt es in der NATO einen Prozess, den sogenannten Targeting-Prozess. In dessen Rahmen würde das entsprechend ausgewählt. Das bezieht sich jetzt aber sozusagen auf ein Bündnisszenar, wo man tatsächlich innerhalb eines Konflikts steht.

In Friedenszeiten gibt es gerade im Bereich der elektromagnetischen Aufklärung erhebliche Erkenntnisse. Da gibt es Beiträge, die im Bereich Electronic Warfare der NATO zusammengeführt werden und damit, ich sage jetzt einmal, in den entsprechenden Handbüchern der NATO allen Nationen zur Verfügung stehen. Da gibt es dann vielleicht Aufteilungen nach Regionen. Deutschland ist vielleicht besonders prädestiniert dafür, Informationen über den Ostseeraum mit entsprechenden Sensoren, die sich da bewegen, bereitzustellen.

Noch einmal: Das sage ich im Kontext des CIR, und das bezieht sich nicht konkret auf die Details von CIR-Operationen, also auf die Frage: Was können Nationen zu diesem Lagebild der NATO beitragen? - Vielen Dank.

Dr. Reinhard Brandl (CDU/CSU): Vielen Dank. - Ich hätte jetzt noch eine Frage an Herrn Professor Padilla. Ich möchte Sie bitten, einen internationalen Vergleich zu ziehen. Ich habe in der ersten Runde mit ihm darüber gesprochen, wie die Kapazitäten in Deutschland sind. Er meinte, wir haben ein Umsetzungsproblem, die Kapazitäten wären also durchaus vorhanden. Wir haben vorhin als Beispiel Israel genannt. Wie sieht das zum Beispiel bei Großbritannien oder Frankreich aus, also bei unseren Nachbarländern? Wie setzen die ihre Fähigkeiten, ihre Cyberkapazitäen bei den Streitkräften um?

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Ehrlich gesagt kenne ich mich mit den französischen Streitkräften und den Streitkräften von Großbritannien nicht sonderlich gut aus. Deshalb fällt es mir etwas schwer, Ihre Frage dazu zu beantworten.

Dr. Reinhard Brandl (CDU/CSU): Sie haben vorhin die Kooperation mit Israel angesprochen. Gibt es etwas, was wir von Israel konkret lernen können?

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Na ja, dass Israelis deutlich schneller bei der Umsetzung von Dingen und beim Einbringen von Fähigkeiten in die Truppe sind, liegt an deren extrem engen Vernetzung zwischen Industrie, Universtäten und Streitkräften. Das liegt in Teilen natürlich an ihrer Wehrpflicht und in Teilen auch daran, dass das Land einfach deutlich kleiner ist. Da gibt es also diese extrem enge Vernetzung. Dann gibt es im Wesentlichen eine Handvoll Leute, die sich untereinander kennen oder sogar miteinander gedient haben; das macht die Wege extrem kurz. Das ist bei uns natürlich deutlich anders.

Dr. Reinhard Brandl (CDU/CSU): Die Bundeswehr hat jetzt eine Reihe von Einrichtungen gegründet, im Wesentlichen sind es zwei Einrichtungen, nämlich die Cyberagentur und den Cyber Innovation Hub; darüber haben wir im Bundestag hinlänglich diskutiert. Jetzt Ihr Blick von außen: Nehmen Sie diese Einrichtungen wahr? Was würden Sie uns an Empfehlungen für diese Einrichtungen mitgeben?

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Gerade die Cyberagentur nehme ich als eine riesige Chance wahr; denn ich glaube, dass wir in Deutschland, insbesondere wenn es um Fähigkeiten und Fragestellungen im Bereich einer eher sicherheitskritischen IT-Infrastruktur geht, noch ein gewisses Defizit haben. Deshalb ist die Cyberagentur an sich eine Riesenchance. Meine Empfehlung an Sie wäre: Versuchen Sie nicht, die Cyberagentur mit üblichen Beschaffungsprozessen zu töten; denn dann wird ihr Sinn wieder ad absurdum geführt. Also, wenn wir da wieder die

ganz normalen Prozesse durchlaufen, die wir üblicherweise haben, dann werden wir wieder zu langsam sein, dann werden wir wieder in einem Stau landen und wieder ein Umsetzungsproblem bekommen. Aber die Idee hinter der Cyberagentur ist, glaube ich, eine Riesenchance. Damit würden wir einen blinden Fleck in Deutschland beseitigt bekommen, wenn wir es denn richtig umsetzen.

Dr. Reinhard Brandl (CDU/CSU): Okay. Vielen Dank. Das ist ermutigend. - Das war meine letzte Frage. Vielen Dank.

Vorsitzender Wolfgang Hellmich: Gibt es weitere Fragen aus der CDU/CSU-Fraktion? Zwei Minuten Zeit sind noch. - Das ist nicht der Fall. Dann hat der Kollege Nolte für die AfD-Fraktion das Fragerecht.

Jan Ralf Nolte (AfD): Ich habe keine Fragen mehr. Danke.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann geht das Fragerecht weiter an die SPD-Fraktion. Herr Vöpel.

Dirk Vöpel (SPD): Vielen Dank, Herr Vorsitzender. - Meine nächste Frage geht an den Inspekteur CIR: Wir haben schon bei vielen Fragen herausgehört, dass die Grenzbereiche gerade im Bereich Cyber relativ schwer einzuordnen sind und dass es dort nicht so einfach ist wie im konventionellen Bereich, einen klaren Trennstrich zu ziehen. Jetzt meine Frage im Hinblick auf den Parlamentsvorbehalt: Inwiefern sehen Sie bei Operationen, die Sie vorbereiten, weil Sie reagieren wollen, im Ernstfall reagieren müssen, den Parlamentsvorbehalt in der Form, in der wir ihn heute haben, als Hemmnis, diese Operationen effektiv vorzubereiten? Oder sehen Sie das gar nicht?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Wenn Sie mit „im Ernstfall“ „im Verteidigungsfall“ meinen, wenn wir uns also in einem Konflikt befinden, dann sehe ich gar nicht, dass da ein Parlamentsvorbehalt entsteht. Sofern auf die Auslandseinsätze der Bundeswehr Bezug genommen wird, wird dort letztlich das Parlament ein Mandat erteilen. In diesem Mandat sind derzeit Kräfte und Fähigkeiten angesprochen, „Kräfte“ im Sinne der Kontingentobergrenze, „Fähigkeiten“ mit Blick auf, ich sage einmal, sehr allgemeine Begriffe. Insofern sind die Themen Führungsunterstützung und Aufklärung in der Regel immer eingeschlossen. Damit sind natürlich auch Kräfte aus dem Org.-Bereich CIR in der Lage, dort ihren Einsatz zu sehen.

Bei den Mandaten, die jetzt bestehen - ich habe vorhin ein Szenar skizziert, mit dem wir in den Einsätzen durchaus leben und worauf wir reagieren müssen -, gibt es aus meiner Sicht kein Defizit. Es ist also nicht so, dass mir in dieser Hinsicht entscheidende Fähigkeiten fehlen würden, die ich anbiete, „anbiete“ in dem Sinne, dass das Einsatzführungskommando das in ihrem Kräftedispositiv entsprechend vorsieht. - Vielen Dank.

Dirk Vöpel (SPD): Vielen Dank. - Vielleicht ist es besser, die Frage in Richtung des Völkerrechtlers zu stellen. Der Herr Kollege Neu hat gerade gesagt, wir würden hier starke Diskussionen führen, die darauf zielten, offensive Schläge der Bundeswehr im Bereich Cyber vorzubereiten. Ich habe die ganze Diskussion bis dahin völlig anders verstanden. - Das erst einmal vorab.

Aber das vielleicht als Frage formuliert: Wenn man mit offensiven Maßnahmen reagieren möchte, dann ist es, wenn ich das richtig verstanden habe, notwendig, dass man vorher in verschiedener Form Aufklärung durchführt und da vielleicht schon die Schwelle überschreitet, über die wir vorhin diskutiert haben: Was ist nicht mehr rein defensiv, was ist schon intrusiv? Die Frage ist: Wie schätzt der Völkerrechtler, der Verfassungsrechtler die Frage der Parlamentsbeteiligung ein? Eine Aufklärung, die durchgeführt wird, um einen eventuell vorzunehmenden offensiven Schlag vorzubereiten, liegt immer im Grenzbereich. Wie schätzen Sie das ein, und wie kann man diesen Grenzbereich klarer fassen? Welche Änderungen wären vielleicht nötig, um da mehr Klarheit zu erhalten?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Ich bin

nicht der Meinung, dass es da unbedingt einer notwendigen Klärung bedarf. Wenn eine solche Maßnahme in Vorbereitung einer spezifischen Operation ergriffen wird, dann wird der Parlamentsvorbehalt zum Tragen kommen.

Wenn es aber nur eine allgemeine Generierung von Fähigkeiten ist, um auf einen Eventualfall vorbereitet zu sein, dann, meine ich, ist die Grenze noch nicht überschritten, sodass hier dann auch kein Raum für einen Parlamentsvorbehalt bestünde.

Im Übrigen wäre ich vorsichtig, da zu sehr ins Detail einzusteigen; denn häufig lassen sich diese Operationen gar nicht trennscharf voneinander unterscheiden. Eine Cyberoperation mag integraler Bestandteil einer kinetischen militärischen Operation sein oder umgekehrt, sodass man da einen bestimmten Ermessens- und Handlungsspielraum für die Streitkräfte erhalten muss, um sie in die Lage zu versetzen, dann tatsächlich ihre Aufgabe zu erfüllen.

Vorsitzender Wolfgang Hellmich: Vielen Dank. - Ich würde dann wieder an die Kollegin Möller zurückgeben.

Siemtje Möller (SPD): Moin! Ich würde gerne bei der Frage Parlamentsvorbehalt bleiben. Der Erfolg von Cyberoperationen hängt unmittelbar damit zusammen, dass ein Gegner die eingesetzten Exploits und Vorgehensweisen nun gerade nicht kennt, um vorhandene Schwachstellen in seinem System nicht vorab beseitigen zu können. Das heißt, der Erfolg von Cyberoperationen ist dadurch bedingt, dass sie geheim bleiben.

Nun meine Frage ans BMVg bzw. den militärischen Teil an Herrn Daum und möglicherweise auch an Herrn Koch. Wenn wir von sogenannten Stand-alone-Cyberoperationen sprechen, würde der geltende Parlamentsvorbehalt aus Ihrer Sicht die Effektivität solcher Operationen einschränken? Und falls ja, wie könnte Ihrer Meinung nach die wehrverfassungsrechtlich notwendige Parlamentsbeteiligung hierfür angemessen ausgestaltet werden?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank, Frau Abgeordnete. - Auf die Frage hin, ob man dem Parlamentsvorbehalt mehr Raum einräumen müsste: Mein Verständnis ist, dass das Parlamentsbeteiligungsgesetz einen Antrag bedingt, und zwar hinsichtlich der einzusetzenden Streitkräfte, nicht im Detail der einzelnen Mittel. In diesen Texten wird dann militärisch zwischen vier Fähigkeitsdomänen unterschieden, nämlich Führung, Aufklärung, Wirkung und Unterstützung, und in allen vier dieser Domänen kommt eine Cyberoperation je nach Sachlage und je nach konkretem Ziel zum Einsatz. Wirkung umfasst aber auch Panzer, Schiffe, Flugzeuge, die dort einbezogen werden, und insofern nämlich auch die Dimension Cyber. Solange die Diskussion und letztlich das Mandat auf Basis dieser Fähigkeitsdomänen den Rahmen setzt, ist das für Cyberoperationen gut genug. - Vielen Dank.

Sachverständiger FKpt PH Dr. Dr. habil. Robert Koch (BMVg): Als kleine Ergänzung noch bezüglich des Bedarfs der Geheimhaltung: Das ist bei solchen Operationsarten immer äußerst extrem hilfreich; formulieren wir es einmal so. Aber Sie können, zumindest in der Theorie, auch mit einer öffentlich bekannten Schwachstelle Erfolg haben, die nicht geschlossen wurde oder nicht richtig geschlossen worden ist. Am Beispiel von Microsoft Exchange im Augenblick: Wenn Sie nur den Patch aufspielen und das nicht verifizieren, kann es sein, dass die Schwachstelle nicht wirklich geschlossen worden ist. Dann ist die Geheimhaltung nicht ganz so extrem wichtig.

Aber insgesamt muss man es auf jeden Fall so bewerten, dass die Geheimhaltung von immenser Bedeutung ist, um einfach die Erfolgswahrscheinlichkeit so hoch wie möglich zu machen und eben den Erfolg der Aktion von den Soldatinnen und Soldaten entsprechend zu unterstützen. Aus dieser Perspektive würde ich der Geheimhaltung gerade bei Cyberoperationen schon einen sehr hohen Stellenwert beimessen.

Siemtje Möller (SPD): Vielen Dank. - Das ist, glaube ich, am Ende auch die Frage. - Herr Daum, ich verstehe es so, dass Cyberoperationen möglicherweise in andere Operationsdimensionen

eingebettet sind. Aber nichtsdestotrotz bedeutet eine Parlamentsbeteiligung oder eine Mandatierung durch den Bundestag vorher auch ein Debattieren des Ganzen. Ich sehe auch, dass wir die Zielrichtung, den Operationsraum, zumindest das Operationsgebiet, miteinander diskutieren würden und damit gegebenenfalls auch unterhalb der Schwelle blieben, dass das einfach nicht mehr ganz so geheim sein könnte, wie Sie es möglicherweise brauchen, um eben erfolgreich auch im Cyberinformationsraum wirken zu können. Da betrifft dann eher folgende Fragen: Wie viel Zeit hat man eigentlich? Wie weit muss es geheim gehalten werden?

Wenn wir jetzt darauf zurückkommen, dass wir fast ein Jahr benötigt haben, um klarer attribuieren zu können, woher der Angriff auf den Bundestag gekommen ist, dann ist auch die Frage, ob es überhaupt noch angemessen ist, darauf in irgendeiner Form zu reagieren, weil es eben schon so lange zurückwirkt etc.

Ich würde gerne die Frage noch etwas ausweiten. Wir haben immer noch das Trennungsgebot bezüglich innerer Sicherheit und äußerer Sicherheit. Wir haben in der Anhörung schon länger darüber gesprochen, dass gerade auch die Länderbehörden - darunter fasse ich jetzt einmal alles, was man darunter fassen kann - zuständig sind. An Herrn von Heinegg stelle ich folgende Frage: Welche rechtlichen Anpassungen könnten denn und müssten aus Ihrer Sicht vorgenommen werden, um eine effektive Kooperation zwischen den Sicherheitsbehörden und der Bundeswehr unter Beachtung des Trennungsgebotes rechtssicher zu gestalten?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Wir haben die Lösungsansätze vorhin schon in einigen Redebeiträgen gehört. Wenn und soweit die Rolle der Bundeswehr betroffen ist, ist es in der Tat Artikel 35 des Grundgesetzes, der hier zum Tragen käme.

Das heißt natürlich nicht, dass gerade im Bereich Cyber-Sicherheit nicht ein allgemeiner und integrativer Ansatz ergriffen werden muss; denn Cyber-Sicherheit lässt sich nicht bewerkstelligen, indem man nur eine zuständige Stelle identifiziert, die dann die dafür erforderlichen Maßnahmen ergreifen sollte. Aber Sie müssen sich in diesem Zusammenhang immer auch vor Augen halten, dass diese im kinetischen Bereich mögliche Trennung zwischen Innen und Außen im Cyberraum häufig nicht so ohne Weiteres möglich ist. Man versucht das zwar immer wieder zu tun. Aber wo beginnt der Bereich der äußeren Sicherheit, wenn es sich zum Beispiel um maliziöse Cyberoperationen etwa gegen eine bestimmte kritische Infrastruktur in der Bundesrepublik Deutschland handelt? War zum Beispiel der Angriff auf den Deutschen Bundestag eine Frage der inneren Sicherheit oder eine Frage der äußeren Sicherheit?

Eine solche klare, trennscharfe Unterscheidung lässt sich heute so gar nicht mehr durchführen. Ich warne davor, dies sozusagen zum Anlass zu nehmen, hier Vorfestlegungen vorzunehmen, die dann möglicherweise ein Hindernis dafür darstellen, die effektiven Maßnahmen zu ergreifen, um Sicherheit tatsächlich gewährleisten zu können.

Siemtje Möller (SPD): Wenn Sie so freundlich wären: Wenn ich jetzt zusammenfasse, sehen Sie keine Herstellung einer Rechtssicherheit, weil Sie sagen, man darf keine Trennung vornehmen. Aber irgendwie wird man darauf reagieren müssen, und das muss dann am Ende rechtlich sicher passieren.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Nein, es geht natürlich darum, dass man sich auf alles vorbereiten muss. Dafür ist es erforderlich, dass ein integrativer Ansatz gewählt wird, also ein Whole-of-Government Approach - oder wie immer Sie das nennen wollen - verfolgt wird. Aber es gibt bestimmte Bereiche, wo man nicht mehr sagen kann, das ist eine Angelegenheit rein der inneren Sicherheit, die hier betroffen ist, oder eine Frage rein der äußere Sicherheit, sondern hier muss in der Tat jeder Schritt unternommen werden, um die Bundesrepublik Deutschland in die Lage zu versetzen, auf alle solche Bedrohun-

gen zu reagieren. Da gibt es keinen abstrakt bestimmbaren Königsweg, sondern hier geht es nur in kooperativer Form.

Siemtje Möller (SPD): Herr Herpig, sehen Sie denn eine Möglichkeit zu einer schnelleren Zusammenschaltung der einzelnen Länderbehörden?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Die Länderbehörden sind aktuell schon teilweise im Cyber-Abwehrzentrum vertreten. Ich denke, es macht hier Sinn, dass alle Länderbehörden, die im Cybersicherheitsbereich agieren, also Hessen3C, das Bayerische Landesamt für Sicherheit in der Informationstechnik usw., auch im nationalen Cyber-Abwehrzentrum vertreten sind, um sich da auch direkt austauschen zu können.

Vorsitzender Wolfgang Hellmich: Ich danke Ihnen. - Dann hat Herr Müller für die FDP-Fraktion das Wort.

Alexander Müller (FDP): Vielen Dank. - Ich mache gleich mit dem Thema weiter, wo wir gerade waren, beim Cyber-Abwehrzentrum und den Zuständigkeiten. Die Frage richtet sich an Herrn Professor Heintschel von Heinegg und an Admiral Daum.

Im Cyber-Abwehrzentrum haben wir verschiedene Dienste. Jetzt nehmen wir den klassischen Fall: Es passiert ein Angriff auf kritische Infrastruktur in der Bundesrepublik Deutschland. Wir haben eben erfahren, wie schwer die Attribuierung ist, wie lange das dauert, bis wir es attribuieren. Aber von der Attribuierung hängt ab, wer am Ende zuständig ist. Es müssen sofort Maßnahmen ergriffen werden. Das heißt, es müssen forensische Analysen stattfinden: Von wo kommt es, wer ist es? Vielleicht kennt man schon den Angriffsserver. Gegebenenfalls müssen da Maßnahmen gegen den Angreifer oder die Richtung, aus der es kommt, ergriffen werden; vielleicht kann man schon darauf einwirken. Aber dafür braucht es einen Zuständigen.

Macht es vielleicht Sinn, ein Bundesgesetz in die Wege zu leiten, dass die Bundesregierung für den Anfang, solange die Attribuierung noch nicht erfolgt ist, einer Dienststelle den Hut aufsetzt, dass praktisch einer dieser Dienste - da sitzen die Länderpolizeien, das BSI, die Bundeswehr, der Verfassungsschutz, also etliche Behörden - anfänglich den Hut aufhat, um das Ganze zu koordinieren. Ist das rechtlich sinnvoll?

Eine zweite Frage nur an Herrn Daum in diesem Zusammenhang: Tagt dieses Cyber-Abwehrzentrum eigentlich geheim? Diese Frage stelle ich vor dem Hintergrund, dass wir eben schon die Abgrenzung der Datenschutzaspekte zwischen den einzelnen Diensten angesprochen haben.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Um es noch einmal klarzustellen: Die Zurechenbarkeit ist nicht Voraussetzung für jede Gegenmaßnahme oder Schutzmaßnahme oder Verteidigungsmaßnahme. Allerdings stimme ich Ihnen da zu, Herr Abgeordneter, dass eine Eilfallkompetenz durchaus hilfreich wäre; denn nur so wäre gewährleistet, dass die notwendigen Schritte auch in der erforderlichen Geschwindigkeit getan werden können, um effektive Cybersicherheitsmaßnahmen oder Verteidigungsmaßnahmen dann tatsächlich zu ergreifen.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Herr Abgeordneter, vielen Dank für die Frage. Ich beginne mit dem zweiten Teil: Tagt das NCAZ geheim? Ich will insofern sagen: Es gibt gewisse Themenkreise, Unterarbeitsgruppen in dem Kreis der beteiligten Behörden, und hier gibt es durchaus entsprechende Ausnahmen, wer daran teilnimmt oder nicht. So kann man sich vorstellen, dass dann, wenn Verfassungsschutzbehörde mit BND zu irgendeiner Diskussion zusammenkommt, nicht zwingend alle dabei sind, beispielsweise auch nicht der entsprechende Vertreter des CIR, weil das dann Themen betrifft, die gewissen Zirkeln vorbehalten sind - so will ich das einmal vorsichtig formulieren -, und das respektieren wir auch. Dass wir hinterher Ergebnisse vielleicht für den Schutz unserer eigenen Systeme daraus erfahren, die dann aber, wie man so schön sagt, sanitarisiert sind, auf-

grund derer also der Rückschluss auf die Information gar nicht möglich ist, ist davon natürlich unbenommen.

Es gibt derzeit sehr wohl einen Koordinator im Cyber-Abwehrzentrum. Der wird von einer der teilnehmenden Behörden gestellt, und der koordiniert in der Tat die Arbeit, die Themenfelder und die Prioritäten und versucht, sicherzustellen, dass die Informationen entsprechend fließen. Das ist aber sozusagen in der Rolle des Koordinators ein Unabhängiger; er vertritt dort nicht irgendeine Behörde. Er stellt sich bei den Themen, um die es dort geht, wenn es zur Abwehr eines Angriffs kommt, natürlich auch die Frage: Wer sollte das dann sein? Das könnte man jetzt einfach einmal festlegen und beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik eine federführende Rolle geben. Dagegen hätte ich jetzt gar keine Bedenken. Aber da sprechen dann auch soundso viele Präsidenten ein Wort mit.

Das für mich in diesem Kontext wesentliche Thema ist die tatsächliche Reaktionsfähigkeit. Derzeit ist das Cyber-Abwehrzentrum noch nicht mit einem Auftrag versehen, beispielsweise 24/7, jederzeit reaktionsfähig zu sein und dann Maßnahmen zu koordinieren. Das findet derzeit in dieser Qualität noch nicht statt. Da sehe ich die besondere Herausforderung, wenn uns nämlich ein möglicherweise massiverer Angriff - ich nenne ihn gerne „digitalen Gau“ - erfasst und massiv Ausfälle festzustellen sind, wenn man darüber nachdenken müsste - ich bin jetzt ganz vorsichtig in der Formulierung -, ob die Telekom, wenn Bayern virenverseucht ist, es dann vom Internet abkapselt, um der Verbreitung dieses Virus Einhalt zu gebieten. Inwieweit das überhaupt rechtlich vorstellbar ist, sei einmal dahingestellt.

Aber diese schnelle Reaktionsfähigkeit, diese Entscheidungsfindung bedingt wirklich, dass alle um den Tisch herum sitzen, also auch, wie von Herrn Herpig angesprochen, die entsprechenden Länderbehörden. Dann müsste man dort möglicherweise auch noch ein Mandat an das Cyber-Abwehrzentrum geben, dort Entscheidungen zu treffen, die dann einen gewissen Verbindlichkeitscharakter haben und nicht erst beispielsweise eine Ministerpräsidentenkonferenz benötigen. Wenn es denn sozusagen um akute Reaktionen zur akuten Abwehr geht, dann sind da sicherlich mehr Reaktionsfähigkeit, mehr Handlungsfähigkeit und möglicherweise auch mehr Mandat erforderlich. - Das wäre meine Antwort. Herzlichen Dank.

Alexander Müller (FDP): Vielen Dank. - Eine zweite Frage noch zum Thema der defensiven und offensiven Maßnahmen und Operationen - darüber haben wir heute schon öfter gesprochen - vielleicht an den Praktiker, Dr. Koch: Kann man defensive und offensive Maßnahmen voneinander abgrenzen? Es ist heute schon angeklungen, dass der eine oder andere vielleicht beabsichtigt, den Auftrag der Bundeswehr möglichst auf defensive Maßnahmen zu begrenzen. Wo würden wir uns denn selbst einschränken? Ich frage danach, damit man sich das an einem praktischen Beispiel einmal klarmachen kann. Was würde das bedeuten, und wie würden wir uns mit einem solchen Gesetz selbst einschränken?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Eine Unterscheidung ist prinzipiell eher wenig hilfreich, um das so zu sagen, weil die Toolbox, die Maßnahmen etc. überall das Gleiche sind. Da kann man an die damalige Diskussion um den Hacker-Paragrafen erinnern, bei der wir das gleiche Themenfeld hatten und gesagt wurde, ja, wir brauchen die gleichen Tools jetzt sozusagen auf der Whitehead- und der Blackhead-Seite. Bei den Fähigkeiten, die man aufbaut, haben wird das strukturell gut unterschieden. Wir haben die Informationssicherheitsorganisation. Wir haben den CNO-Bereich, der für die aktiven Maßnahmen erforderlich ist. Aber die Fähigkeiten, wie wir die Leute ausbilden müssen, was sie letztendlich können und anwenden müssen, umfassen die gleiche Basis, das gleiche Wissen.

Wenn wir jetzt hergehen und sagen, okay, wir setzen es nur noch im Bereich der Defensive ein, dann habe ich da schon erhebliche Sorgen, was die Durchsetzungsfähigkeit im entsprechenden Einsatzraum anbelangt; denn wir müssen jederzeit damit rechnen, dass ein guter Gegner - wir haben ja gesagt, die einen oder anderen sind, was

das Technologische anbelangt, deutlich weiter als wir - zum Beispiel auf dem Gefechtsfeld auf unsere Waffensysteme einwirken kann. Wenn ich Best Practice aus dem zivilen Bereich heranziehe und dann sage, okay, ich habe mein Risiko soundso weit abgedeckt und habe jetzt noch den Notfallplan, mein System wieder anzufahren, die Daten wiederherzustellen, sodass ich im Beispiel eines Ransomware-Vorfalls keine Probleme habe, mein Geschäftsprozesse wieder anlaufen usw., dann habe ich zwar einen zeitlichen Verzug, aber alles richtig gemacht.

Das greift halt nicht im Rahmen einer militärischen Cyberoperation, weil ich nicht die Zeit habe, um anzufangen, meine militärischen Systeme im Einsatzgebiet, auf dem Gefechtsfeld mit solchen Notfallplänen wieder fit zu machen, sondern ich muss auf die Maßnahmen, die auftreten, direkt reagieren können, mit sämtlichen Voraussetzungen, die wir heute schon diskutiert haben. Dafür brauche ich auch die offensiven Fähigkeiten, um dann in diesem Rahmen mit den jeweiligen rechtlichen Möglichkeiten wirken zu können, wenn ich einen solchen Angriff sehe, und ich kann mich eben nicht darauf verlassen, dass da irgendwie ein Notfallplan greift. - Danke.

Vorsitzender Wolfgang Hellmich: Vielen Dank. - Herr Dr. Neu hat jetzt das Wort.

Dr. Alexander S. Neu (DIE LINKE): Ich bin überrascht, dass zum Thema Aktualisierungsbedarf und Erfassungsbedarf des Parlamentsbeteiligungsgesetzes eher schwache Hinweise kamen, dass es also - so zumindest meine Interpretation - da keine Notwendigkeit gebe. In §§ 1 und 2 des Parlamentsbeteiligungsgesetzesanschaut wird bei der Begriffsbestimmung usw. usf. durchaus von bewaffneten Streitkräften gesprochen, die sich außerhalb des Gebietes des Grundgesetzes bewegen, also außerhalb der Bundesrepublik Deutschland. Nun ist es so, dass sich die Soldatinnen und Soldaten, wenn sie an einer Cyberoperation teilnehmen, nicht unbedingt im Ausland befinden müssen. Ich möchte jetzt zwei Szenarien ansprechen und hoffe dann auf eine Antwort.

Das eine Szenario ist: Der UN-Sicherheitsrat beschließt eine Maßnahme gegen Land X, und die Bundesregierung signalisiert ihre Beteiligung ausschließlich in Form von Cyberfähigkeiten. - Dann wäre das in meinen Augen ein Gegenstand, der im Parlament beraten werden müsste, weil die Bundeswehr gewissermaßen aktiv wird. Aber zugleich ist es nicht so, dass die Soldatinnen und Soldaten der Bundeswehr dafür im Ausland sein müssten. Das könnten sie auch vom Inland her machen. Also, wäre es dann ein Fall für das Parlamentsbeteiligungsgesetz, so wie es jetzt geschrieben ist, oder müsste man es - wie zumindest meine Meinung ist - entsprechend an die digitalen Herausforderungen anpassen?

Das zweite Szenario ist: Der Bundestag wird angegriffen, was wir vor einigen Jahren hatten. Es dauert mehr als ein Jahr bis zur Attribuierung. Mehr als ein Jahr bedeutet, man reagiert nicht unmittelbar, sondern zeitlich verzögert. - Hier würde dann die Frage sein: Wäre ein Vergeltungsschlag seitens Deutschlands, ein Vergeltungsschlag durch die Bundeswehr ein Fall für das Parlamentsbeteiligungsgesetz, ja oder nein, auch vor dem Hintergrund eines reinen Cybervergeltungsschlags, vor dem Hintergrund, dass die Soldaten nicht unbedingt im Ausland tätig werden müssten, sondern diesen Vergeltungsschlag vom deutschen Staatsgebiet aus betreiben könnten?

Das sind doch gewissermaßen Szenarien, die eine Aktualisierung, eine Anpassung des Parlamentsbeteiligungsgesetzes, so wie es jetzt geschrieben ist, erforderlich machen würden.

Diese Frage geht einmal an Herrn Thomas Reinhold und zum anderen an Herrn Professor Heinegg. - Danke.

Sachverständiger Dipl.-Inf. Thomas Reinhold (TU Darmstadt): Danke für die Frage. Die rechtliche Komponente maße ich mir an dieser Stelle nicht an zu bewerten. Das, denke ich, kann Herr Heinegg auf jeden Fall viel besser.

Ich glaube, es ist einfach nur entscheidend, auf Folgendes hinzuweisen, weil das in den Stellungnahmen der Kolleginnen und Kollegen zum

Teil anders dargestellt wurde: Aus der technischen Perspektive - so würde ich als ein Techniker sagen - ist ein Einwirken auf ein System immer eine Gefährdung eines Systems. Dabei wird oft unter den Tisch fallen gelassen, dass man nicht sofort das Zielsystem zur Hand hat, das man angreifen möchte, wo man vielleicht wirken möchte, vielleicht auch mit berechtigtem Hintergrund usw., sondern dass man sich da erst einmal hinarbeiten muss.

Das kann man im Vorfeld eines Konfliktes tun, vorbereitend. Man kann es vielleicht erst, wenn sozusagen das Parlament sagt: Ja, ihr dürft. - Trotzdem muss man sich immer überlegen, dass auf dem Weg dahin einfach viele unbeteiligte Systeme liegen, die man im Zweifelsfall mit gefährdet, die Dienste haben, die zivilen Zwecken nutzen. Und wenn man einen geschickten Angreifer hat, dann wird er sich auch genau hinter solchen Systemen verstecken. - Das zum technischen Hintergrund. An dieser Stelle möchte ich an Herrn Heinegg übergeben. - Danke.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Fangen wir mit dem zweiten Punkt an, Herr Abgeordneter: Vergeltung. Das vergessen Sie mal! Also, Rache, Vergeltung, das ist etwas, was jedenfalls vom geltenden Völkerrecht nicht gedeckt wäre. Das Einzige, was gedeckt wäre, wäre eine Selbstverteidigung. Selbstverteidigung ist nur zulässig, wenn wir eine Selbstverteidigungssituation haben. Wir „brauchen“ also einen bewaffneten Angriff. Sonstige Gegenmaßnahmen setzen einen andauernden Völkerrechtsbruch voraus, auf den man reagiert. Und wenn ein Jahr ins Land gegangen ist und keine weiteren Bedrohungen hinzugekommen sind - oder Cyberoperationen -, dann ist der Raum für Gegenmaßnahmen, ich würde mal sagen, denkbar klein.

Nun zum Parlamentsbeteiligungsgesetz. Wenn Sie sich die Genese des Parlamentsbeteiligungsgesetzes noch einmal vor Augen halten: Es war ja diese berühmt-berüchtigte Entscheidung des Bundesverfassungsgerichts, wonach die Bundeswehr ein Parlamentsheer sei. Wenn wir davon ausgehen, dann würde natürlich auch eine Cyberoperation, selbst wenn sie im Rahmen und nach Maßgabe der Regeln eines Systems kollektiver Sicherheit wie der Vereinten Nationen erfolgt, grundsätzlich eine Parlamentsbeteiligung oder ein Mandat des Deutschen Bundestages erfordern, wenn und soweit die Cyberoperation über das hinausgeht, was bloße Aufklärung zum Beispiel wäre. Wenn die Cyberoperation tatsächlich physische Wirkungen oder Wirkungen in der physischen Domäne zeitigen würde, dann wäre das ein Einsatz, der - jedenfalls nach Sinn und Zweck und im Lichte der Genese des Parlamentsbeteiligungsgesetzes - ebenfalls dem Parlamentsvorbehalt unterläge. Jede Beteiligung an Feindseligkeiten oder an einer Anwendung bewaffneter Gewalt in diesem Sinne wäre damit vom Parlamentsbeteiligungsgesetz gedeckt.

Wenn wir das aber noch klarstellen wollen, bitte: Das wäre natürlich eine Möglichkeit. Aber auch hier kann ich das wiederholen, was ich vorhin schon gesagt habe: Gehen Sie da um Gottes Willen nicht zu sehr ins Detail! Denn wie wollen Sie das alles noch auseinanderhalten? Das dürfte äußerst schwierig sein.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann hat Frau Brugger das Wort.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Ich hätte Fragen an Herrn Herpig und möchte einmal damit starten, was Sie als erste These benannt haben. Sie schreiben ja auch in Ihrer Stellungnahme, dass wir bei einer laufenden Cyberoperation nicht irgendwie abschrecken oder sie nicht abwehren könnten mit einer Gegencybermaßnahme - wenn ich das einmal so ein bisschen umschreiben darf - und dass die Experten sich an der Stelle auch einig seien. Jetzt haben wir hier manchmal ein bisschen andere Auffassungen gehört. Können Sie noch einmal erläutern, warum Sie glauben, dass das nicht zu mehr Sicherheit beiträgt, und warum es diesen Abschreckungs- oder Abwehreffekt vielleicht gar nicht geben kann?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Ja. Vielen Dank. - Also, was Sie machen, wenn ein Angriff detektiert ist: Sie versuchen, zu gucken, wo der Angriff stattgefunden hat, welcher

Schaden eventuell schon angerichtet wurde. Dann ist zu entscheiden, ob man den Angriff - vielleicht eingedämmt - weiterlaufen lässt, um zu gucken, ob man Informationen für die Attribuierung findet oder weitere Hintertüren. Man versucht, den Schaden dann abzuwenden, das System oder die Systeme so schnell wie möglich wieder ans Laufen zu bringen. Es gibt natürlich auch andere, passive Maßnahmen, wie die Umleitung von DDoS-Angriffen zum Beispiel; das würde man dann bei den Internetserviceprovidern wie der Telekom oder Vodafone beantragen. Es gibt ein unglaublich großes Set an passiven Maßnahmen. - Das ist normalerweise das, was man macht, wenn da nichts anderes detektiert wird.

Mir ist kein realistisches Szenario bekannt - gucken Sie sich Exchange an, gucken Sie sich Solar-Flare an -, wo offensive intrusive Maßnahmen irgendetwas dazu beigetragen hätten, dass eine Cyberoperation eines Gegners gestoppt wird. Es gibt - das weiß ich - in Sicherheitsbehörden ganz tolle hypothetische Szenarios, wo sich jemand ausgedacht hat: So, wenn man das und das annimmt - was noch nie in der Welt vorgekommen ist -, dann könnte man mit offensiven, intrusiven Cybermaßnahmen einen Angriff irgendwie stoppen. - Das halte ich für komplett verfehlt; das ist in vielleicht 0,1 Prozent oder noch weniger der Fälle irgendwann einmal sinnvoll. Von daher sollte man sich hier auf die Stärken der anderen Maßnahmen verlegen, die wirklich den Schaden eindämmen, das Leben wieder ans Laufen bringen und den Angriff entsprechend abwehren.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): „Schwachstellen“ ist ein Stichwort, das hier in der Debatte immer wieder fällt. Sie haben in Ihrer Stellungnahme für ein Schwachstellenmanagementmodell plädiert, das ein bisschen auch so eine Abwägung macht. Wenn eine Sicherheitsbehörde eine Schwachstelle nutzen möchte, hat sie natürlich gar kein Interesse daran, dass andere darüber Bescheid wissen. Das ist für die Bürgerinnen und Bürger im Land möglicherweise ein Sicherheitsrisiko. Wie könnte denn so ein Schwachstellenmanagementmodell aussehen, und welche Rolle hat da aus Ihrer Sicht die Bundeswehr?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Vielen Dank für die Frage. - Herr Koch hat vorhin ja auch schon ein wenig erläutert, was bei Schwachstellen zu tun ist. Wir haben eine komplette Veröffentlichung dazu geschrieben. Aber in Kürze: Zuallererst muss die Analyse stattfinden, ob die Behörde - in diesem Fall die Bundeswehr - überhaupt für irgendwelche Einsätze, die sie bisher geplant hat oder zukünftig planen kann, unbekannte Schwachstellen braucht oder sich auf bekannte Schwachstellen - die, die sich im Disclosure-Prozess befinden, die, die noch nicht gepatcht sind, usw. - zurückziehen kann. Herr Koch hat vorhin angeführt: Manche Sachen werden überhaupt nicht gepatcht, weil es den Hersteller, den Maintainer gar nicht mehr gibt usw. usf.

Wenn man sagt: „Wir brauchen in ganz wenigen Fällen - die können wir auch ganz klar darlegen - unbekannte Schwachstellen, wie auch immer wir die beschaffen; hoffentlich auf einem moralisch, ethisch und rechtlichen korrekten Wege“, ist zu analysieren, ob diese Schwachstelle, wenn wir sie für eine gewisse Zeit zurückhalten, eventuell mehr Schaden an deutschen Systemen und den Systemen von Verbündeten anrichtet als das, was wir mit ihr an Wirkung erreichen können. Hier sollten alle deutschen Behörden, die mit Schwachstellen hantieren, einbezogen werden. Es macht keinen Sinn, wenn irgendeine Behörde, die mit Schwachstellen agiert, aus diesem Prozess rausgelassen wird; das führt den Prozess ad absurdum. Das heißt, auch die Bundeswehr müsste hier dabei sein und dementsprechend diese Informationen austauschen.

Dann gibt es eine Bewertung, die natürlich dafür sorgen muss, dass hauptsächlich und immer im Zweifelsfall die IT-Sicherheit und die Cybersicherheit in Deutschland Vorrang haben vor irgendwelchen offensiven intrusiven Maßnahmen. Und dann wird beurteilt, mit verschiedenen Kategorien, was geschehen soll.

Das ist ein Modell, was in vielen anderen Ländern - in den USA, in den Niederlanden, im Vereinigten Königreich, in Australien - bereits etabliert ist.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Dann hätte ich noch eine Frage an Frau Schuetze - Sie hatten vorhin schon darauf Bezug genommen, auch in Ihrer Stellungnahme -: Was dürfte aus Ihrer Sicht die Bundeswehr ohne Mandat tun, und wo setzt die Mandatspflicht ein? Was heißt das aus Ihrer Sicht für die Frage der parlamentarischen Kontrolle, und wie können wir diese stärken und ausbauen?

Sachverständige Julia Schuetze (SNV e. V.): Ja, also, technisch gesehen, finde ich, hat Herr Herpig das ja gut aufgeteilt in Informationsgewinnung und alles, was danach stattfindet. Aufklärung - intrusiv quasi - und Wirkung wäre nur unter parlamentarischer Beteiligung machbar. Ich finde, die Diskussion heute hat gezeigt, dass da schon noch Potenzial ist für eine erweiterte Kontrolle und eine genaue Ausdifferenzierung dieser offensiven Maßnahmen und wofür die dann eingesetzt werden. Ich glaube, das ist gerade im Hinblick darauf sehr wichtig, dass der Zielstaat natürlich, falls es entdeckt wird, einfach auch die Kontrolle hat, zu reagieren. Und dann muss man auch darlegen können, ob das jetzt eine nachrichtendienstliche Tätigkeit war oder doch zur Vorbereitung eines Angriffs diente. Da möchte ich nur meine Kollegen Herrn Wetzling und Herrn Vieth von SNV zitieren; die haben die Stellungnahme zum BND-Gesetz gemacht und dort auch noch mehr Kontrolle gefordert. Gerade weil die Bundeswehr ja auch keine … - jetzt ist der Ton mal wieder an - nachrichtendienstliche Tätigkeit … und dass da alle in der Kontroll- -…[1] Nachrichtendienst, auch nach Artikel 45d. Genau, das könnte man noch mal ausdifferenzieren.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank.

Vorsitzender Wolfgang Hellmich: Ja, auch meinerseits danke sehr. - Dann gehen wir jetzt in die dritte Runde. Die CDU/CSU-Fraktion ist dran.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. - Ich fange einfach mal an mit einer Frage, die vielleicht so ein bisschen ins Technische zurückgeht, einer Frage an Admiral Daum: Was wären denn Cyberhandlungen, wo man sagt - mal ganz konkrete Beispiele -: „Aus rechtlichen Gesichtspunkten sind wir einwandfrei im grünen Bereich“? Vielleicht kann man das auch mal mit EloKa vergleichen. Ich stelle mir so vor, EloKa ist nur passiv unterwegs, defensiv. - Ich hatte EloKa immer anders verstanden. Aber wo sind Bereiche - mal so ein paar Beispiele -, wo Sie sagen: „Da sind wir bei Cyber völlig safe“, und wo wäre so ein Grenzbereich, den man diskutieren müsste?

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank, Herr Abgeordneter. Ich bin noch da, musste nur die richtige Taste finden; Entschuldigung. - Also, wo sind wir rechtlich im grünen Bereich? Vielleicht darf ich, weil insbesondere von Herrn Herpig und Frau Schuetze unterschieden wird zwischen Informationsgewinnung und Aufklärung, hier voranstellen: Im militärischen Sprachgebrauch ist Aufklärung der gesamte Prozess und nicht erst der Prozess, wo beispielsweise intrusiv gearbeitet wird, wo die Passwortschwelle überwunden wird. Das muss man in dem Kontext verstehen, damit, wenn ich von Aufklärung spreche, nicht gleich jeder an Herrn Herpig denkt und dann sagt: Da tut er ja etwas, was er gar nicht darf. - Selbstverständlich steht vor dem Überwinden dieser Grenze die passive Erfassung, also das, was wir mit Elektronic Support Measures, Herr Abgeordneter, im Bereich EloKa verfolgen. Das ist natürlich alles im grünen Bereich. Natürlich ist auch alles, was beispielsweise ein Flottendienstboot vor einer Küste außerhalb der Hoheitsgewässer zufällig im elektromagnetischen Spektrum auffängt, alles im grünen Bereich. Und auch, das entsprechend auszuwerten, zu versuchen, dort Erkenntnisse zu ziehen, ist natürlich alles in Ordnung.

Im Themenfeld Wirkung, dort, wo es - und das muss man jetzt sicherlich differenzieren - im Bereich der elektronischen Kampfführung dazu

[1] Anmerkung Stenografischer Dienst: Störung der Tonübertragung

führen würde, dass man ein gegnerisches Radargerät mit elektronischen Gegenmaßnahmen stört, muss natürlich ein besonderer Umstand bestehen, der das entsprechend zulässt, also rechtlich abgesichert - oder natürlich in einem Konfliktfall. Das sage ich jetzt ganz vorsichtig: Im Frieden ist ja alles verboten, was nicht ausdrücklich erlaubt ist. Im Krieg ist aber alles erlaubt, was nicht ausdrücklich verboten ist. - Das aber ganz vorsichtig; vielleicht kommt hinterher Herr Heintschel von Heinegg und sagt, ich habe bei ihm in den Rechtsvorlesungen nicht aufgepasst. Aber im Grunde genommen geht es ja um diesen Aspekt.

Und dann natürlich der Bereich der Informationsoperation. Die Analyse des Informationsumfeldes „Wie ist dort Meinungsbildung vielleicht in eine andere Richtung zu bewegen? Wie sind Informationen an die Bevölkerung im Einsatzland abzugeben, die dort positiv zugunsten deutscher Streitkräfte wirken?“, begleitende Prozesse, das ist natürlich auch alles zulässig.

Was wir - Sie haben ja nach Beispielen gefragt - beispielsweise im Bereich der operativen Kommunikation ausschließen, ist sozusagen, dass wir mit False News, mit Fake News, mit falscher Propaganda vorgehen. Das würden wir explizit nicht tun. Das liegt natürlich im Kontext der Kriseneinsätze auch sehr nahe; denn dort wollen wir ja in der Regel vor Ort helfen, wollen Frieden stiften etc. Deshalb wollen wir uns da natürlich nicht dem Risiko aussetzen, mit falschen Botschaften unsere eigene Reputation infrage zu stellen. Dort würden wir sofort in einen Bereich kommen, wo es dann nicht nur rechtlich bedenklich wird, sondern im Grunde genommen auch ethisch-moralisch bedenklich wird.

Wenn wir es konkret auf den Cyberraum konzentrieren, dann erfolgt die Aufklärung eben bis zu der Tür, die passwortgesichert oder durch einen Schlüssel gesichert ist; das ist die natürliche Grenze, bis zu der wir gehen können. Alles, was dahinter ist, wäre dann rechtlich weiter abzusichern.

Das war jetzt unter meinem Anspruch CIR, Innendimension Cyberraum, Informationsumfeld, elektronische Kampfführung, für jedes, glaube ich, ein Beispiel, wo es möglich ist, und eines, wo wir dann aufhören würden und nicht agieren würden. Ich hoffe, das beantwortet Ihre Frage. - Herzlichen Dank.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. Das ging schon absolut in die richtige Richtung, hat ganz viel von dem beantwortet, was ich gefragt habe.

Ich möchte noch einmal nachsetzen. Das war so ein bisschen die Perspektive „aus Deutschland in die Welt“, sage ich mal. Was ist im Einsatzland? Ich bewege mich in Afghanistan und sehe eine Drohne, die auf deutsche Einheiten zukommt, und die könnte ich möglicherweise entschlüsseln. Machen wir so was? Können wir so was? Ich fände es gut, wenn wir das könnten. Oder machen wir uns da so lange Gedanken, ob das rechtlich geht, und verlieren die Kompetenz?

Sie brauchen hier im ungeschützten digitalen Bereich keine detaillierte Antwort zu geben. Aber es geht mir um die Wirkmächtigkeit auch hinterher. Oder diskutieren wir über das, was wir im Inneren auch diskutieren, über Einfallstore usw.? Das sind Diskussionen, die wir auch in der Innenpolitik haben. Ich denke, wir sollten schauen, dass wir nicht hinter das, was bei EloKa seit Jahrzehnten klar ist, jetzt im Cyberraum total zurückfallen. Also, ich bin immer davon ausgegangen, wir können auch wirken, wenn es die Notwendigkeit erfordert.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Grundsätzlich ist es erst einmal so: Wenn im Einsatzland eine Drohne auf Kräfte zufliegt und das in der Hinsicht eine Gefährdung bedeutet, dann gibt es das Gebot der Selbstverteidigung, und dann könnte man die theoretisch - Mandat etc. vorausgesetzt - natürlich abschießen. Insofern: Wenn wir uns darüber einig werden, dass das Abschießen in einem Szenar zulässig wäre, dann wäre möglicherweise auch das Blenden, das Stören dieser Drohne mit Kräften, die wir auf dem Gefechtsfeld bereitstellen, rechtlich zulässig. Inwieweit wir das schon können und inwieweit wir da noch Verbesserungsbedarf sehen, das will ich hier mal kürzer halten. Ich will es aber so formulieren: Ich denke, wir haben von

Bergkarabach gelernt, dass Drohnen in der Wirkung eine ganz neue Qualität auf dem Gefechtsfeld einnehmen, und das beschäftigt natürlich alle unsere Kameraden des Heeres, der Luftwaffe und der Marine, sich dort zu wappnen und sich dagegen zu wehren, und das interessiert natürlich auch den Inspekteur CIR hinsichtlich der Frage: Mit welchen elektronischen Gegenmaßnahmen können wir dort operieren?

Der Cyberangriff im klassischen Cyberraum ist da wahrscheinlich eher weniger hilfreich. Da müssten Sie schon wissen, wo der Pilot sitzt, und ihn dann in seiner Führungskapazität dort einschränken; das halte ich eher für unwahrscheinlich. Aber das Thema „EloKa gegen Drohnen“ ist natürlich ein spannendes Thema und aus meiner Sicht auch neu betont worden. Deshalb wird bei uns jetzt neu untersucht: Welche Fähigkeitslücken haben wir dort? - Vielen Dank.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. Das beantwortet meine Frage. - Vielleicht könnte ich Ihnen bilateral einige Beispiele nennen, wo man auch an den Container für den Drohnenpiloten herankäme. Wir gucken ja nicht nur nach Amerika. Wir gucken ja auch in andere Staaten, die kleiner sind, wo es vielleicht auch interessant wäre, die Kommunikation zu stören.

Ich will eine letzte Frage - weil ich glaube, meine Kollegen haben auch noch Fragen - an Professor Heintschel von Heinegg stellen. Mal gucken, ob *ich* seine Vorlesung gut verstanden habe. Ich habe Herrn Admiral Daum so interpretiert: Alles, was konventionell möglich ist, ist rechtlich auch per Cyber möglich, also: Wenn ich die Drohne abschießen kann, kann ich sie auch digital erfassen, stören usw. - Ist das die Grundregel?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Ja, wenn Sie so wollen, kann man das genau auf diesen Punkt bringen. Lediglich in Ergänzung zu dem, was Admiral Daum gesagt hat: Im Einsatzgebiet - Afghanistan oder wo immer es sein mag, meinetwegen auch Mali - ist man nicht darauf beschränkt, nur Selbstverteidigung durchzuführen, sondern man kann so eine Drohne, auch ohne dass sie eine konkrete Bedrohung darstellt, ohne Weiteres neutralisieren, und das natürlich auch mittels einer Cyberoperation.

Dr. Patrick Sensburg (CDU/CSU): Gut. - Ich hätte jetzt zwar noch Fragen, aber ich sehe: Die Kollegen haben auch Fragen. - Daher würde ich erst mal weitergeben und nur eingrätschen, wenn keiner mehr Fragen hat; dann würde ich mit meinen Fragen kommen. Ich sehe nämlich den Kollegen Lehmann und andere.

Vorsitzender Wolfgang Hellmich: Wer seitens der CDU/CSU-Fraktion meldet sich? Der muss mal kurz ein Signal geben.

Dr. Patrick Sensburg (CDU/CSU): Sonst mache ich weiter.

Vorsitzender Wolfgang Hellmich: Herr Kollege Sensburg, Sie dürfen weitermachen.

Dr. Patrick Sensburg (CDU/CSU): Okay. Super. - Dann würde ich nämlich noch einmal Fregattenkapitän Koch eine Frage stellen. Wenn jetzt gilt, was Vizeadmiral Daum und Professor Heintschel von Heinegg gesagt haben, dass im Grunde - ich sage es ganz platt - digital das rechtlich geht, was konventionell geht, wo sehen Sie dann für das Ministerium die Fragebereiche? Es ist ja gut, dass wir die Anhörung machen, und wir haben ja auch offene Fragen, die in der ganzen Zeit gestellt worden sind. Aber was ist das Kernproblem? Bei der Frage des Mandats bzw. der Rules of Engagement ist das Digitale, der Bereich Cyber ein anderes Wirkmittel. Aber ist es zulässig? Nur weil es um Cyber geht, wirft es keine neuen rechtlichen Fragen auf; so habe ich die Vorredner verstanden. Wo sind dann aus Ihrer Sicht die Knackpunkte?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Ich will nur kurz auf diese Fragestellungen eingehen, weil ich nicht in der Rolle des BMVg-Vertreters da bin. Allerdings mache ich im BMVg auch Cyberpolitik. Die interessanten Fragestellungen in dem Bereich wurden ja angerissen, insbesondere international unterschiedliche Interpretationen und das sehr kleine gemeinsame Set, das man hier im Augenblick zur Verfügung hat. Ich denke, dass insbesondere, wie

man da vorwärtskommt, eine wichtige Fragestellung ist; die entsprechenden Gremien mit ihren Herausforderungen wurden erwähnt. Da ist das Auswärtige Amt, das für uns in diesen Angelegenheiten federführend tätig ist, sehr aktiv. Es hat auch wieder jüngst entsprechende Papiere vorgelegt. Da müssen wir einfach gucken, wie wir international weiterkommen. - Ich fasse mich an der Stelle kurz.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. - Jetzt frage ich mal umgekehrt Herrn Dr. Herpig, um vielleicht mal diesen anderen Blick zu kriegen. Nehmen wir an, es ist so wie bei meiner gerade formulierten Grundthese - ich spitze bewusst zu -: All das, was konventionell rechtlich einwandfrei ist, darf man auch digital cybermäßig tun, sage ich mal flapsig. - Unterschreiben Sie das auch? Das würde unsere Problemstellung dramatisch reduzieren. Oder wie bewerten Sie das?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Ja, aber.

Dr. Patrick Sensburg (CDU/CSU): Das „aber“ ist das, worauf ich hinauswill.

Sachverständiger Dr. Sven Herpig (SNV e. V.): Aber der Cyberraum gestaltet sich eben anders als der konventionelle Raum. Vorhin kam das Beispiel Stuxnet; mit Stuxnet hätte es einen zielgerichteten Angriff gegeben, den es natürlich mitnichten so gab. Stuxnet war eigentlich mit vielen, vielen Hundert Millionen US-Dollar designt und beinhaltete einen Nachbau der kompletten Fazilität in Natans, die nachher angegriffen werden sollte, um nicht außerhalb des Irans und auch nicht außerhalb dieser Fazilität irgendwo auf der Welt auffindbar zu sein. Es ist korrekt, dass Stuxnet nur in Natans Wirkung entfaltet hat. Aber Stuxnet wurde am Ende auf der ganzen Welt gefunden. Deswegen wurde ja auch herausgefunden, was mit ihm passiert. Er wurde zum Beispiel auch in Netzwerken von Alliierten gefunden. Ich frage mich, wie wir es betrachten würden, wenn wir auf einmal in unseren kritischen Infrastrukturen eine Schadsoftware, die industrielle Steueranlagen manipulieren kann, von amerikanischer Seite oder von israelischer Seite fänden.

Gleichzeitig muss man dazu natürlich auch sagen - Herr Koch hat es vorhin gesagt -: Wenn jemand diese Schadsoftware, die ja nicht wirklich zielgenau war, obwohl sie mit einem riesigen Budget so geplant war, in seinen eigenen Netzen findet, kann er sie auch reverse engineeren und dadurch die Schwachstellen weiterverwenden. Das heißt, wenn Feinde der USA bei dieser Cyberwaffe - ich mag den Ausdruck nicht - die Schwachstelle, die in Stuxnet drin war, reverse engineert hätten, hätten sie sie gegen Deutschland und die USA einsetzen können. Mir ist nicht bekannt, dass es ein konventionelles Wirkmittel gibt, das sich genauso gestaltet. Deswegen macht es natürlich zwar irgendwie Sinn, dass das, was für konventionelle Wirkmittel gilt, auch im Cyberraum für Cyberwirkmittel gilt. Aber der Cyberraum ist anders gestaltet, und die Cyberwirkmittel funktionieren teilweise ganz anders als die konventionellen Wirkmittel. Diese Spezifitäten müssen wir betrachten, und für diese Fälle müssen wir diskutieren, bis wohin es gehen kann.

Dr. Patrick Sensburg (CDU/CSU): Es ist ja die Frage, wenn ich es richtig sehe: Wann liegt ein Cyberangriff vor? Wann hat er eine bestimmte Schwelle erreicht, dass ich seine Intensität bewerten kann, wo es militärisch relevant wird? Jetzt stelle ich mir das Ganze in der folgenden Situation vor: In Afghanistan setzt einer der beteiligten Staaten Stuxnet ein. Er soll irgendwelche Zentrifugen dazu bringen, sich zu schnell zu drehen. Darf ich darauf konventionell antworten, darf ich digital antworten, oder muss ich es hinnehmen?

Sachverständiger Dr. Sven Herpig (SNV e. V.): Ich denke, in dem Fall würde man, je nachdem welche Wirkung ausgelöst wird, entsprechend den konventionellen Antwortmöglichkeiten auch die Cybermöglichkeiten miteinbeziehen.

Dr. Patrick Sensburg (CDU/CSU): Wenn ich das dann richtig wahrnehme, besteht gerade im Bereich des Angriffs, wenn ich keine Konfliktsituation irgendwelcher Art habe, das Problem des

Bewertens. Wenn ich, sage ich mal, im Kriegsvölkerrecht etc. bin - ich will jetzt den Satz nicht wiederholen -, ist alles möglich, was nicht verboten ist; in Cyberangelegenheiten haben wir noch nicht die völkerrechtlichen linken und rechten Grenzen. Aber das Problem besteht immer dann, wenn ich im Frieden bin. Wenn ich dann so einen Cyberangriff feststelle, habe ich eine Vielzahl von Problemen: Welche Wirkmächtigkeit besteht? Wie hoch ist die Anzahl der Angriffe? Geschieht es einmal alleine? Welches Zerstörungspotenzial besteht? Und so weiter. Da habe ich das Problem. Wenn ich in einem militärischen Konflikt bin, habe ich die Probleme erst mal grundsätzlich nicht - rechtlich, meine ich jetzt; faktisch habe ich die ganzen Fragen natürlich auch, aber rechtlich nicht. Sehe ich das richtig? Dann kann man das Problem ein bisschen reduzieren.

Sachverständiger Dr. Sven Herpig (SNV e. V.): Da ich kein Rechtswissenschaftler bin, würde ich dem erst mal so zustimmen, wie das vorhin gesagt worden ist, und noch mal darauf verweisen, dass es dann aber auch den gleichen Effekt, die gleiche Wirkung haben muss wie ein entsprechendes konventionelles Medium. Es ist ja auch im Konflikt, im Verteidigungsfall, wie auch immer, nicht alles erlaubt.

Dr. Patrick Sensburg (CDU/CSU): Gott sei Dank. Ich bin ein großer Freund davon, diese Möglichkeiten einzuhegen und dafür zu sorgen, dass man sich an Regeln hält. Darüber müsste man sowieso mal wieder reden. - Ganz herzlichen Dank.

Die vielleicht letzte Frage meinerseits.

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Herr Abgeordneter, dürfte ich noch ganz kurz wegen dieser Zielgerichtetheit eine Antwort auf Herrn Herpig geben?

Dr. Patrick Sensburg (CDU/CSU): Gerne.

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Im Rahmen von militärischen Cyberaktionen hat das ja doch eine entsprechende Bedeutung. Stuxnet ist durchaus zielgerichtet. Die Diskussion, die immer besagt, dass er es nicht ist, betrachtet nur eine von den Schadsoftwarevarianten oder Wirkmittelvarianten, wie immer man das in dem Kontext nennen will, die sich letztendlich verbreitet hat. Es betrifft aber nicht die ursprünglichen Versionen, die anfangs eingesetzt worden sind und sich sehr klar nur in einem sehr geringen Bereich verbreitet haben. Ob der spätere Verbreitungseffekt gewollt war oder nicht gewollt war, ist eine Diskussion, die wir irgendwann mal am Rande ausführlicher führen sollten, weil die einheitliche Interpretation, die relativ oft gefunden wird, dass das eben ein Unfall war und das aggressivere Vorgehen von der israelischen Seite gewünscht war, nur eine mögliche Interpretation in dem Bereich ist. Also, wir können das schon entsprechend zielgerichtet bauen.

Dr. Patrick Sensburg (CDU/CSU): Ganz herzlichen Dank. - Jetzt sehe ich keine Uhr mehr. „Heißt das: Ende?“, frage ich den Vorsitzenden. - Drei Minuten noch. Dann stelle ich eine ganz, ganz kurze Frage. Ich meine, Frau Schuetze wäre da die geeignete Expertin; denn Sie hatten eben schon was dazu gesagt. Deswegen würde ich einfach noch mal fragen: Wo stehen wir eigentlich in Deutschland bei der Cyberkompetenz? Welche Länder sind da richtig pfiffig? Welche sind da nicht pfiffig? Sind wir da auf Platz 3 nach China und den USA, sind wir da auf Platz 193, oder wo sind wir da? Ich weiß: Das ist eine ganz offene Frage, die Sie jetzt vor das Problem stellt: Was meint er überhaupt? - Aber ich will mal gucken, was Sie sagen.

Sachverständige Julia Schuetze (SNV e. V.): Ja, okay. Es kommt halt darauf an, was für Kompetenzen gemeint sind, worum es geht. Ich bin generell nicht so ein Freund davon, irgendwelche KPIs zu nehmen und dazu zu sagen, wo wir im Vergleich zu anderen stehen; denn dann muss man ja zugleich die Defensivfähigkeiten auch im Bereich Policy usw. betrachten. Da gibt es verschiedene Modelle. Von daher kann ich Deutschland jetzt nicht im Vergleich zu anderen einordnen und würde es auch nicht gerne tun. Innerhalb Deutschlands sollte man sich aber vielleicht schon auch überlegen: Was haben wir für ein Ziel? Was wollen wir erreichen?

Dr. Patrick Sensburg (CDU/CSU): Ja, die Frage war aber schon anders. Die Frage betraf den Vergleich international. Das andere hatten wir heute schon ganz lange gehört.

Sachverständige Julia Schuetze (SNV e. V.): Ich kenne keine sehr gute Statistik, die ich jetzt zitieren würde, die, wie ich finde, sehr gut gemacht ist und über die man sagen kann, dass es einen Vergleich gibt, vielleicht höchstens noch das Cybersecurity Maturity Model von Oxford. Ich weiß aber auch nicht, wo wir da gerade stehen. Das ist so ein bisschen ein kohärenter Überblick über Fähigkeiten sowohl im Technischen als auch im Politischen. Da kann man sich mal den Report für Deutschland angucken und auch die Reports für die anderen. Die geben auch zum Beispiel Empfehlungen, wo man noch Potenzial hat.

Dr. Patrick Sensburg (CDU/CSU): Super, ganz lieben Dank. - Damit sind meine Fragen beendet.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann geht das Fragerecht an Herrn Nolte von der AfD-Fraktion.

Jan Ralf Nolte (AfD): Kein Bedarf.

Vorsitzender Wolfgang Hellmich: Kein Bedarf. - Seitens der SPD-Fraktion, habe ich mir sagen lassen, gibt es auch keinen Bedarf. - Da würde ich mal die Möglichkeit nutzen, eine Frage an Herrn Padilla zu richten: Wie weit sind eigentlich die technologischen Entwicklungen, die es möglich machen, jeden technischen Pfad innerhalb des Netzes so zu verwischen, ich sage mal: falsche Spuren zu legen, dass man am Ende die Herkunft einer bestimmten übersandten Information überhaupt gar nicht mehr nachvollziehen kann oder dass vielmehr, wie gesagt, falsche Spuren gelegt werden?

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): So gesehen sehr weit. Was Sie aber üblicherweise haben: Sie kriegen es nicht hin, komplett zu verschleiern, wo die Informationen herkommen. Was üblicherweise gemacht wird, ist, dass sehr lange Perlenketten gebaut werden; ich nenne das immer „Perlenketten“. Das heißt, Sie haben viele verschiedene Systeme, über die das Ganze geschleust wird und die Sie auch nicht so furchtbar einfach deanonymisiert kriegen. Es gibt ja verschiedene Anonymisierungsnetzwerke, die Sie nehmen können; es gibt verschiedene VPN-Anbieter, die für so was genutzt werden. Es ist schon nicht ganz unaufwendig, da eine Deanonymisierung herbeizuführen. Das bringt uns dann wieder zu den offensiven Mitteln; denn wenn Sie so was schaffen wollen, benötigen Sie häufig irgendeine Art von offensiven Wirkmitteln, um so eine Deanonymisierung durchführen zu können.

Vorsitzender Wolfgang Hellmich: Das hat letztlich erhebliche Konsequenzen für die Frage der Attribuierbarkeit, -

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Korrekt.

Vorsitzender Wolfgang Hellmich: - die sich zeitlich wie faktisch dann sehr schwierig darstellt.

Sachverständiger Prof. Dr. Elmar Padilla (FKIE): Korrekt. Unter anderem deshalb brauchen wir ja so lange. Das beste Modell, das ich da kenne, ist dieses MICTIC-Modell, das beim BSI unter anderem genutzt wird. Es besagt, dass man sich die Malware, also die Schadmittel, anguckt, dass man sich die Infrastruktur für den Angriff anguckt, dass man sich die C&C-Server anguckt, die Telemetrie, das, was man an Intelligence-Informationen über potenzielle Tätergruppierungen schon hat, aber dass man sich auch dieses „Cui bono?“ anguckt. Das heißt, dass man es nicht rein mit technischen Maßnahmen versucht, sondern dass man versucht, so einen Maßnahmenmix zu finden.

Die Problematik an der Stelle ist aber, dass wir in meinen Augen so eine Art Indizienbeweis führen. Das heißt, wir kommen darüber nicht zu dem, was ich in meinem Eingangsstatement meinte, zu einer unbestreitbaren, eindeutigen Attribuierung, sondern eigentlich ist das eine Art Indizienbeweis, und der ist auch noch relativ aufwendig. Ich glaube, das führt zu vielen der Problematiken, was ich ja vorhin schon mal versucht habe zu erläutern.

Vorsitzender Wolfgang Hellmich: Danke sehr. - Dann hat der Herr Müller das Fragerecht.

Alexander Müller (FDP): Vielen Dank. - Wir haben noch eine Frage, die die Cybersicherheit unserer Kommunikationsinfrastruktur in Deutschland betrifft. Wir diskutieren ja seit einigen Monaten, ob wir es erlauben oder verbieten sollen, dass bestimmte Hersteller Komponenten in unsere Mobilfunkinfrastruktur einbauen, und wie groß das Schädigungspotenzial oder das Spionagepotenzial von solchen Geräten ist. Da wir heute Fachleute dabei haben, würde mich mal interessieren - das richtet sich zunächst an Dr. Koch -, inwieweit man das mitigieren kann, inwieweit man solche Geräte kontrollieren kann. Unser Interesse muss es ja sein, dass wir möglichst viel Wettbewerb für unsere Telekommunikationsausrüster haben, damit die die Auswahl aus verschiedenen Geräten haben. Aber wie groß ist denn die reale Gefahr? Kann man diese Geräte nicht vorher einmal analysieren und zertifizieren und sagen: „Okay, davon geht keine Gefahr aus“? Wie groß ist die reale Gefahr? Wie schätzen Sie das ein? Was würden Sie empfehlen? Würden Sie aus Ihrer fachlichen Sicht eher sagen, dass die Gefahr zu groß ist?

Dann noch eine rechtliche Frage an Professor Heintschel von Heinegg: Auf welcher Rechtsgrundlage kann denn die Bundesregierung überhaupt unsere Infrastruktur schützen, indem sie den Telekommunikationsprovidern Vorgaben macht nach dem Motto: „Aus diesen Ländern dürft ihr Hardware kaufen, aus solchen Ländern dürft ihr keine Hardware kaufen“? Wie ist das rechtlich überhaupt möglich?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Die Fragestellung ist natürlich hoch spannend; im Rahmen der 5-G-Diskussion gab es dazu zahlreiche Statements. Oft wird ja gesagt: Okay, wir schauen uns jetzt die Geräte an, aber wir haben noch nichts gefunden. - Das ist dieses maßgebliche „Wie finde ich was?“.

Ich habe einen Bereich Penetrationstest in der Bundeswehr aufgebaut, in dem wir auch tief in die Systeme reinschauen. Man hat immer dieses letztendliche Problem: Wie lange suche ich, und wie hoch ist die Wahrscheinlichkeit, dass ich irgendwas finde? Wenn man so ein bisschen in die Historie schaut, dann finden wir beispielsweise um 2012 herum die Diskussion um den Prozessor Microsemi ProASIC3, bei dem man eine Hintertür gefunden hat. In der Diskussion mit den Herstellern wird dann eben dargestellt: Ja, das sind die Debugging-Funktionalitäten. - Das ist eine ganz große Herausforderung in dem Bereich. Wenn ich so was vernünftig mache, dann kann ich es auch glaubhaft abstreiten.

Sehen wir uns einmal den Kommunikationsbereich an. Wenn ich beispielsweise einen Informationskanal verstecken und einbauen will, dann kann ich schon rein die validen Standards nutzen. Das sind maßgeblich RFCs, Requests for Comments, anhand deren quasi die Geräte mit Internet gebaut werden, die die Industrie heranzieht, in denen die technischen Vorgaben hinterlegt sind. Da sind Spielräume drin, und die sind auch erforderlich, dass die Produkte letztendlich kompatibel und interoperabel sind und da draußen miteinander funktionieren. Wenn ich die als Hersteller aber geschickt ausnutze, kann ich da beispielsweise einen Informationskanal, den zurzeit kein Sicherheitssystem findet, implementieren. Deshalb ist es immer gut, wenn man tief in die Geräte reinschaut, den Source Code zur Verfügung hat, den vernünftig analysiert. Nur den Source Code zu haben, reicht nicht; ich muss ihn natürlich auch auswerten, bewerten können. Man kann mathematische Testverfahren drüberlaufen lassen, den Code verifizieren. Das ist alles noch sehr aufwendig und führt zu Forschungsbedarf; aber das wären so die Ansätze, wo man in dem Bereich weitergehen kann.

Etwas kann natürlich auch sinnvoll sein. Sagen wir mal, ich bin Hersteller X. Ich habe jetzt irgendwas Fieses in mein Gerät eingebaut und baue einen Informationskanal zwischen verschiedenen Komponenten auf. Ich kann natürlich versuchen, irgendwo im Perimeter, an irgendwelchen Netzübergängen einfach einen anderen Hersteller, eine andere Komponente, wo ich höhere Sicherheitsstandards habe oder so, einzubringen und hier mögliche Kanäle abzuschneiden.

Letztendlich aber ist die Gesamtnachricht: Die Möglichkeiten von bewusst eingebrachten Schwachstellen in dem Bereich sind extrem vielfältig. Es gibt viele Forschungsarbeiten in dem Bereich, aber es ist sehr, sehr herausfordernd. Wenn es vernünftig gemacht ist, dann ist es kaum aufzufinden, oder ich habe auf jeden Fall „plausible deniability“: eine gute Bewertung oder eine gute Begründung, warum ich das nicht absichtlich gemacht habe. Das ist natürlich bei dem einen oder anderen Hersteller dann durchaus ein Risiko, das man in der Praxis mitberücksichtigen muss.

Alexander Müller (FDP): Und Ihre persönliche Empfehlung, Ihre persönliche Einstellung dazu noch?

Sachverständiger FKpt Dr. Dr. habil. Robert Koch (BMVg): Auch in dem Bereich gibt es ja im Open-Source-Bereich verschiedene Sachen und Projekte, die man heranziehen kann, natürlich nicht mit der gleichen Leistungsfähigkeit. Wir sind auch in diesen Bereichen durchaus nicht Weltmarktführer, sagen wir es so. Wir haben die entsprechenden Abhängigkeiten. Da muss man eben gucken, dass man hier die eigenen Kompetenzen wieder stärkt - Stichwort: digitale Souveränität - und die ganzen Maßnahmen, die da avisiert sind. Und ja, letztendlich ist es eine Risikobetrachtung. Also: In welchen Bereichen will ich was einsetzen? Und man muss eben vertrauenswürdig mit den Herstellern umgehen und sagen: Er stellt mir den Source Code zur Verfügung, auch wenn es ein proprietäres System ist; wir können untersuchen; wir haben einen Ansprechpartner.

Inwieweit das in der Praxis ausreichend ist, ist fraglich. Wir haben das beispielsweise bei dem Kompetenzzentrum von Microsoft, wo wir, der Staat, den Code einsehen können. Inwieweit hilft Ihnen das? Es ist trotzdem unendlich viel Code, Sie brauchen die Experten, die es bewerten können, etc. etc. Also: Es ist ein Start, aber der Weg zu einer echten Sicherheit ist dann immer noch sehr weit.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Wenn ich kurz noch etwas zur Ergänzung sagen darf: Ende der 90er-Jahre hat die chinesische Führung bekannt gemacht, sie würde bis zu 4 000 Cyberkrieger ausbilden, und deren Aufgabe sei es natürlich, nationale chinesische Interessen zu vertreten. Zu glauben, dass in diesem sehr sensiblen Bereich die chinesische Regierung sich zurückhalten wird und das Ganze sozusagen als rein wirtschaftliche Betätigung akzeptieren wird, wäre meines Erachtens etwas naiv. Jeder von Ihnen, der ein iPhone hat, stellt ein Sicherheitsrisiko dar, und sei es auch nur aus dem Grunde, dass das iPhone in China produziert worden ist.

Zu der Frage aber, die Sie gestellt haben, ist die Rechtsgrundlage relativ einfach. Sie haben sowohl im nationalen Recht als auch im Völkerrecht als auch im Europarecht natürlich die nationale Sicherheit als Ausnahmetatbestand. Es ist keineswegs so, dass Sie hier gerichtsfeste Beweise vorzulegen hätten, sondern es reicht aus, wenn vernunftmäßige Verdachtsmomente bestehen, dass hier eine Gefahr für die nationale Sicherheit besteht.

Vorsitzender Wolfgang Hellmich: Das Gute ist: Ich habe kein iPhone. - Ich glaube, es sind inzwischen auch eher 10 000 denn 4 000 Cyberkrieger in China, wenn ich das richtig sehe.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Das war Ende der 90er-Jahre, Herr Vorsitzender, also vor über 20 Jahren, als sie das ankündigten. Dass es jetzt weit mehr sind, ist natürlich völlig klar.

Vorsitzender Wolfgang Hellmich: Gut. - Dann hat Herr Dr. Neu das Wort.

Dr. Alexander S. Neu (DIE LINKE): Vielen Dank, Herr Hellmich. - Ich habe noch eine Frage an Herrn Professor von Heinegg. In Ihrem Eingangsstatement hatten Sie ausgeführt, dass Deutschland unter keinen Umständen eine Souveränitätsverletzung mit Blick auf Cyberoperationen akzeptieren solle. Da bin ich vollkommen bei Ihnen; das ist völlig inakzeptabel. Zugleich debattieren wir hier immer wieder über offensive Wirkmittel als unterstützende Maßnahmen neben Defensivmaßnahmen. Also, man muss offensiv agieren,

um überhaupt ein Defensivpotenzial aufbauen zu können, soweit ich das richtig verstanden habe.

Nun ist die Nichtakzeptanz einer Souveränitätsverletzung natürlich keine Einbahnstraße und nicht nur zugunsten der Bundesrepublik Deutschland oder des Westens zu sehen, sondern zugunsten aller Staaten - so zumindest die UN-Charta. Da wir ja Teil der UN sind, sollten wir das, denke ich, auch akzeptieren. Das heißt mit anderen Worten: Das Sicherheitsbedürfnis anderer Staaten muss genauso respektiert werden wie unser Sicherheitsbedürfnis. Wie ist das denn mit den Argumenten für offensive Wirkmittel in Einklang zu bringen? Das habe ich noch nicht so ganz verstanden.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Die Tatsache, dass die Souveränität für alle Staaten gleichermaßen gilt, bedeutet ja nicht, dass damit von vornherein offensive Operationen oder, wie Sie es nennen, „offensive Wirkmittel“ ausgeschlossen wären. Wir haben schon auf die vielen Ausnahmen verwiesen - sei es Selbstverteidigung, seien es Gegenmaßnahmen usw. usf. -, sodass ich der Meinung bin, dass jede Souveränitätsverletzung jedenfalls rechtfertigungsbedürftig ist. Wenn wir als Bundesrepublik Deutschland bei der Souveränitätsverletzung eines anderen Staates keinen hinreichenden Rechtfertigungsgrund vorzubringen berechtigt wären, dann wäre das natürlich weiterhin eine Völkerrechtsverletzung.

Wenn ich also sage: „Wir müssen auf unsere Souveränität mehr Wert legen und Souveränitätsverletzungen auch beim Namen nennen“, dann schließe ich damit natürlich nicht aus, dass andere Staaten das Gleiche tun könnten, wenn und soweit sie von einer ähnlichen Operation betroffen wären.

Dr. Alexander S. Neu (DIE LINKE): Nachfrage: Das heißt, Sie konditionieren Souveränität? Souveränität ist sozusagen nicht absolut zu betrachten, sondern einer Konditionalität unterworfen: Wenn Staat X ein berechtigtes Interesse hat, dann kann er die Souveränität eines anderen Staates aushebeln.

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Nicht „berechtigtes Interesse“ - das wäre mir etwas zu weitreichend -, sondern einen echten Rechtfertigungsgrund, der eine Souveränitätsverletzung eines anderen Staates ausnahmsweise rechtfertigt. Das ist ganz wichtig im Hinterkopf zu behalten. Es geht nicht um eine Interessenverfolgung, sondern es geht um einen Rechtfertigungsgrund. Das heißt, ich muss nach völkerrechtlichen Vorschriften suchen, die es ausnahmsweise erlauben, die Souveränität eines anderen Staates zu verletzen.

Dr. Alexander S. Neu (DIE LINKE): Okay. - Danke.

Vorsitzender Wolfgang Hellmich: Ich sehe keine weiteren Fragen. - Dann geht das Fragerecht an Frau Brugger.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. - Ich würde da gerne gleich weitermachen, Herr Professor von Heinegg. Und zwar: Frau Schuetze hatte ja vorhin die Reaktion oder Stellungnahme der Bundesregierung mit Blick auf die Politik der USA angesprochen. Da reden wir, wenn ich das richtig verstehe, durchaus von einer Souveränitätsverletzung, wenn für eine militärische Operation, deren Ziel vielleicht gar nicht ein deutscher Akteur sein mag, deutsche Infrastruktur oder Netze genutzt werden könnten. Sie hatten vorhin sehr pointiert gesagt, so etwas sollte man nicht unbeantwortet lassen. Was würden Sie da empfehlen, und wie klar ist das rechtlich geregelt, wenn es sich sozusagen nur um eine Art Mitnutzung der Infrastruktur handelt und nicht um einen expliziten Angriff, der sich dann auch gegen einen Akteur hierzulande richtet?

Sachverständiger Prof. Dr. Wolff Heintschel von Heinegg (Europa-Universität Viadrina): Frau Abgeordnete, da bringen Sie genau das auf den Punkt, was im Augenblick umstritten ist. Wenn ich die bloße, wie Sie es nennen, „Mitnutzung“ in den Blick nehme, dann gibt es hier keinen echten Konsens. Staaten wie die USA stellen sich auf den Standpunkt, das sei überhaupt rechtlich irrelevant; denn es sei ja letztlich nur, wenn Sie

so wollen, das Transferieren von Daten über bestimmte Netzwerke usw., und das sei völkerrechtlich irrelevant.

Andere Staaten sehen das sehr viel enger. Da gilt es dann eben, die berühmten Like-minded States zu finden, um mit ihnen erst mal zu einem gemeinsamen Standpunkt zu kommen, der dann möglicherweise sich auf die Sicht anderer Staaten positiv oder natürlich auch negativ auszuwirken geeignet ist.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Total spannend. - Dann würde ich nämlich den Ball aufnehmen und an Herrn Reinhold zurückspielen. Wenn Sie uns noch mal etwas zu den Möglichkeiten, Grenzen und Erfordernissen der Rüstungskontrolle in dem Bereich sagen könnten, würde das, glaube ich, genau diese Frage noch mal aufnehmen.

Sachverständiger Dipl.-Inf. Thomas Reinhold (TU Darmstadt): Vielen Dank für die Frage. Vielen Dank, dass Sie das Thema noch mal anschneiden. - Grundsätzlich ist die Idee von Rüstungskontrollen in der Vergangenheit immer gewesen, dass man das gegenseitige Misstrauen zwischen Staaten abbaut. Zwei Staaten beobachten sich irgendwie; beide haben Sorge, dass der andere etwas plant, mehr Fähigkeiten hat als man selbst und entsprechend reagiert.

Ich muss ehrlich sagen, dass ich in den Debatten, wie ich sie heute gehört habe, eine ähnliche Tendenz wahrnehme, weil wir ganz viel über Offensive reden. Das mag in einem gewissen Rahmen begründet sein, sollte aber zumindest von Maßnahmen begleitet werden, die das Ganze sozusagen wieder „runterkochen“. Das kann damit beginnen, dass man Doktrinen austauscht; das passiert schon in einem gewissen Rahmen. Es gibt internationale Gremien, es gibt die UNGGE, es gab die Open-ended Working Group, die gerade einen wichtigen Durchbruch erreicht hat, es gibt die OSZE, in deren Rahmen Gespräche geführt werden.

Ich glaube aber, dass man im Cyberspace tatsächlich noch ganz andere Maßnahmen durchführen kann. Wichtig ist, hier zu betonen, dass bei der Rüstungskontrolle das Problem besteht, dass ganz viele von den etablierten Maßnahmen im Cyberspace schlichtweg nicht funktionieren, weil dieser als Domäne anders funktioniert.

Trotzdem könnte man tatsächlich über eine defensive Ausrichtung der Bundeswehr diskutieren, indem man sagt, man nutzt die ganze Palette an Werkzeugen, um die eigenen Netze sicher zu machen, um stark zu sein und um eine gute Verteidigung zu haben; man nutzt sie aber nicht offensiv oder, wenn man sie offensiv nutzt, dann wirklich nur in extrem genau definierten Bereichen. Man nimmt vielleicht die ganzen offensiven Operationen, die jetzt der BND als Zuträger von Informationen durchführt, einfach doch zurück, oder man begrenzt sich, indem man sagt, man greift gewisse Systeme nicht an oder schaut noch nicht mal auf gewisse Systeme wie kritische Infrastrukturen, weil da einfach immer die Gefahr besteht, dass das bloße Draufschauen doch mal schiefgeht.

Wie ich in meinem Eingangsstatement gesagt habe, ist es nicht so einfach möglich, zu sagen, man guckt sich ein System nur an; denn in dem Moment, wo ich in einem System drin bin und schaue: „Was passiert hier?“, habe ich es in einem gewissen Rahmen schon kaputtgemacht. Andere, die das wahrnehmen - vielleicht der Staat, in dem diese KRITIS steht -, sehen erst mal nur eine schadhafte Operation. Die wissen noch nicht unbedingt: Ist es „nur“ - in Anführungszeichen - Spionage, oder wird wirklich etwas vorbereitet, wo am Ende irgendwie auch eine Malware platziert wird? Da steckt ganz viel Eskalationspotenzial drin. Das heißt sozusagen, Maßnahmen wie der Verzicht auf den Einsatz bestimmter Waffen wären sehr, sehr hilfreich, wenn man dies als deutsche Regierung klar formuliert. Das Auswärtige Amt hat da ja gerade einen sehr wichtigen Vorstoß unternommen.

Man kann auch noch weiter gehen, indem man sagt: Okay, wenn alle Staaten Informationen über Sicherheitslücken horten, die in dem Moment, wo sie zurückgehalten werden, natürlich die zivile Sicherheit - auch die eigene nationale zivile Sicherheit - gefährden, müsste man sich darüber austauschen: Wie kann man dafür sorgen, diese

Stockpiles, wie man sie nennt, abzubauen? Gibt es vielleicht Mechanismen, gibt es vielleicht technische Verfahren, gibt es im Rahmen des Vulnerabilities Equities Process vielleicht Möglichkeiten, Sicherheitslücken zu schließen bzw. die reine Quantität ein bisschen zu reduzieren, um die allgemeine Bedrohung im Cyberspace, die das letztlich bedeutet, irgendwie einzugrenzen?

Dann gibt es natürlich noch weitere Verfahren im Bereich der Rüstungskontrolle. Wie kann man das ganze Thema Verifikation weiterdenken? Da sind wir jetzt aber im Bereich des Spekulativen. Ich kann nur immer wieder dafür plädieren, was ich im Eingangsstatement gesagt und in der Stellungnahme geschrieben habe: Da brauchen wir einfach die naturwissenschaftliche Friedensforschung - gerade im Bereich der Informatik -, die aus meiner Sicht noch völlig unzureichend ausgeprägt ist. - Danke schön.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. - Dann hätte ich noch eine Frage an Herrn Vizeadmiral Daum. Und zwar: Sie haben selber vorhin schon die Parallele zur Coronakrise gezogen; ich will das mal auf einer anderen Ebene tun. Wir haben ja gesehen, dass in der Coronakrise von Landesregierungen Amtshilfe der Bundeswehr angefordert wurde, woraufhin die Bundeswehr zum Glück gesagt hat: „Moment, rechtlich ist das so nicht erlaubt“, und die Landesregierungen so ein bisschen in ihre Schranken gewiesen hat.

Wenn wir jetzt über Fälle von Amtshilfe im Bereich Cyber, aber auch über einen absoluten Notfall, der den Einsatz der Bundeswehr im Inneren verfassungsrechtlich erlauben würde, sprechen: Ist das ausreichend diskutiert? Ist das ausreichend vorgeplant? Und muss das nicht auch - zum Beispiel mit Blick auf die Amtshilfe, jetzt nicht auf den Einsatz der Bundeswehr im Inneren - ein Stück weit geübt werden? Sie wissen: Wir als Grüne sind da sehr skeptisch. - Das würde mich noch interessieren.

Sachverständiger VAdm Dr. Thomas Daum (Inspekteur CIR): Vielen Dank, Frau Abgeordnete, für die Frage. - Die Bundeswehr kann natürlich im Zuge der Amtshilfe einbringen, was die Bundeswehr an Fähigkeiten hat. Das ist erst mal das Grundprinzip. Wir können ja im Falle, dass wir um Amtshilfe gebeten werden, nicht mit irgendwelchen anderen Fähigkeiten, die wir gar nicht besitzen, antreten; das ist keine Frage. Dann gilt es natürlich immer, zu prüfen, ob der Amtshilfeantrag in dieser Hinsicht rechtmäßig ist oder ob es bei der Amtshilfe möglicherweise darum geht, wir mögen in irgendein System einbrechen, was uns normalerweise gar nicht möglich wäre. Das muss man natürlich differenzieren.

Dass man das trainieren muss, ist keine Frage. Es gibt ja beispielsweise die LÜKEX, die länderübergreifenden Übungen. Da ist das BBK derzeit in der Federführung für das Jahr 2021. Dort will man beispielsweise ein Szenario durchspielen, in dem die Bundesrepublik Deutschland durch Cyberangriffe in irgendeiner Weise geschwächt ist, unter der für mich natürlich unglücklichen Annahme, dass es das Cyber-Abwehrzentrum nicht geschafft hat, dieser Schadenslage Herr zu werden, und deshalb dann sozusagen der andere Apparat - Katastrophenhilfe etc. - anlaufen muss.

Also: In dieser Situation spielt die Bundeswehr sicherlich eine Rolle. Es ist vorstellbar, dort zur Amtshilfe gerufen zu werden wie in jedem anderen Fall auch. Etwas zu üben, ist immer gut, damit man über die verschiedenen Rollen, die dort wahrgenommen werden können, überhaupt Bescheid weiß. Deshalb sind wir beispielsweise bei LÜKEX natürlich dabei. - Herzlichen Dank.

Agnieszka Brugger (BÜNDNIS 90/DIE GRÜNEN): Danke schön.

Vorsitzender Wolfgang Hellmich: Vielen Dank. - Wir sind jetzt am Ende der dritten Runde angekommen. Deshalb ist meine Frage, ob es für eine weitere Runde Gesprächs- oder Fragebedarf gibt. Mein Eindruck ist: Wir haben eine sehr intensive Diskussion geführt, die viele Fragen beantwortet hat, aber auch viele Fragen aufgeworfen hat, die noch nicht beantwortet sind.

Ich fand in der letzten Runde den Hinweis darauf, dass Verfassungsrealität auch geübt werden muss, spannend, da man bei Übungen, wenn es

sie gibt - ich halte sie für sehr wichtig -, glaube ich, unter dem Gesichtspunkt „Beteiligung des Parlamentes“ mal die Frage mit einbeziehen müsste: Wie sieht eigentlich eine solche Lage aus, in der das Parlament beteiligt sein müsste bzw. beteiligt wäre?

Wir hatten so etwas mit dem niederländischen Verteidigungsausschuss vor - das hat wegen Corona nicht stattfinden können -, nämlich in einer Art politischen Übung die Frage zu klären: Was passiert eigentlich unter dem Gesichtspunkt der Parlamentsbeteiligung, wenn eine deutsch-niederländische Einheit in einen Einsatz gehen sollte? Dazu gibt es viele offene Fragen. Ich glaube, an dieser Stelle ist es wichtig, eine politisch-parlamentarische Übung durchzuführen, in der eine solche Situation unter den Bedingungen und im Rahmen des Parlamentsbeteiligungsgesetzes einfach mal durchgespielt wird. Ein solches Szenario durchzuspielen, fände ich sehr spannend.

Ich glaube, die Diskussion heute hat für die Arbeit des Verteidigungsausschusses - aber nicht nur des Verteidigungsausschusses, sondern auch des Innenausschusses und vieler anderer Ausschüsse - eine Menge Fragen zutage gefördert, weil die einzelnen Sektionen der Parlamentsorganisation eben nicht zu trennen sind, sondern das Thema querschnittlich mehrere Bereiche betrifft und im politischen Raum auch entsprechend querschnittlich angegangen werden muss.

Auch wenn es im Moment keine weiteren Fragen und keinen Bedarf für eine nächste Runde gibt, gibt es mit Sicherheit Bedarf für eine weitere Expertenanhörung, wann auch immer die sein mag. Wir müssen konsequent an dem Thema weiterarbeiten; das ist, glaube ich, sehr richtig.

Ich will an dieser Stelle als Allererstes dem Ausschusssekretariat für die Vorbereitungsarbeit und für die Organisation des Ganzen danken. Wir haben das jetzt das zweite Mal innerhalb kürzester Zeit gemacht, und die Kolleginnen und Kollegen haben, glaube ich, viele Schweißperlen auf der Stirn gehabt, die sie jetzt alle abwischen können; denn sie wussten nicht, ob das auch alles gut geht. Es ist gut gegangen.

Ich danke auch im Namen aller meiner Kolleginnen und Kollegen im Verteidigungsausschuss den beteiligten Sachverständigen für ihre Teilnahme und für ihre fundierten Beiträge. Ich fand, es war eine sehr gute und sehr tiefgehende Diskussion, die auch deutlich gemacht hat, dass das Interesse des gesamten Verteidigungsausschusses an diesem Thema sehr groß ist.

Ich komme an dieser Stelle meiner letzten hohen Aufgabe nach und schließe diese Ausschusssitzung. Ich wünsche Ihnen noch einen schönen Tag. Vielen Dank noch mal. „Bis die Tage!“, wie man hier so schön sagt. Tschüss!

(Schluss: 16.36 Uhr)

Anlagen

Schriftliche Stellungnahme von
Prof. Dr. Wolff Heintschel von Heinegg
Europa-Universität Viadrina

Schriftliche Stellungnahme von
Dr. Sven Herpig
Stiftung Neue Verantwortung e. V.

Schriftliche Stellungnahme von
FKpt Dr. Dr. habil. Robert Koch
Bundesministerium der Verteidigung

Schriftliche Stellungnahme von
Dipl.-Inf. Thomas Reinhold
Technische Universität Darmstadt

Schriftliche Stellungnahme von
Julia Schuetze
Stiftung Neue Verantwortung e. V.

VÖLKERRECHTLICHE FRAGEN IM CYBER- UND INFORMATIONSRAUM

Verteidigungsausschuss des Deutschen Bundestages,
Öffentliche Anhörung, 14. Dezember 2020

Prof. Dr. iur. Wolff Heintschel von Heinegg,
Europa-Universität Viadrina, Frankfurt (Oder)

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)941
08.12.2020 - 19/3494
5410

Vorbemerkung

Zum Begriff des Cyberraums

Die besonderen Charakteristika des Cyberraums – Interkonnektivität und Ubiquität – verleiten mitunter dazu, den Cyberraum als virtuellen Raum zu verstehen, der sich scheinbar einer Anwendung traditioneller (völker-)rechtlicher Regeln und Prinzipien entzieht. Die damit einhergehende Mystifizierung des Cyberraums sollte jedoch unbedingt vermieden werden. Zu diesem Zweck bietet es sich an, auf allgemeine Definitionsversuche zu verzichten und sich stattdessen der auch von den U.S. Joint Chiefs of Staff verwendeten Beschreibung nach Maßgabe des – vereinfachenden, gleichwohl hilfreichen – sog. 3-Ebenen-Modells zu bedienen, wonach der Cyberraum aus einem physikalischen Netzwerk (unterseeische Kommunikationskabel, Leitungen, Server etc.), einem logischen Netzwerk (u.a. Protokolle) sowie einer personalen Ebene (Nutzer und Cyber-persona, z.B. IP-Adresse) besteht, wobei diese drei Ebenen sich gegenseitig bedingen.[1]

Zum Begriff der Cyber-Operation

Nicht jeder Rechnereinsatz oder jede Nutzung des Cyberraums ist als völkerrechtlich relevante Cyber-Operation einzuordnen. Vielmehr sollte der Fokus auf Operationen liegen ‚that involve the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace'.[2] Als Beispiel einer solchen Cyber-Operation, mit der Ziele im oder durch den Cyberraum erreicht werden sollen, kann genannt werden: ‚use of computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'[3] Folglich sollen allein solcher Cyber-Operationen in den Blick genommen werden, die Wirkungen im oder durch den Cyberraum zeitigen oder zu zeitigen bestimmt sind. Operationen durch den Cyberraum zeichnen sich dadurch aus, dass sich ihre Wirkungen in der physischen Domäne materialisieren. Demgegenüber verbleiben die Wirkungen von Cyber-Operationen im Cyberraum innerhalb des Cyberraums.

[1] Chairman of the Joint Chiefs of Staff, *Cyberspace Operations*, S. I-2 ff. (Joint Publication 3-12, 8 June 2018), abrufbar unter: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
[2] U.S. Department of Defense, Law of War Manual (June 2015, updated December 2016), Abs. 16.1.1, abrufbar unter: https://www.hsdl.org/?view&did=797480.
[3] Ebd.

Es sei jedoch darauf hingewiesen, dass mit der Einordnung als Cyber-Operation weder eine völkerrechtliche Wertung noch eine Einordnung als Angriff im völkerrechtlichen Sinne einhergeht.

I. Cyber-Operationen als Anwendung von Gewalt oder bewaffneter Angriff

In den verschiedenen nationalen Cyber-Sicherheitsstrategien wird der Begriff des ‚Cyber-Angriffs' in einem denkbar weiten Sinne verwendet. Davon erfasst werden sollen etwa 'deliberate acts that seriously compromise national security, stability or prosperity by manipulating, denying access to, degrading or destroying computers or networks or the information resident on them'.[4] Während mitunter zwischen Cyber-Angriffen und anderen maliziösen Cyber-Operationen unterschieden wird[5], darf mit Blick auf dieses weite Verständnis nicht unberücksichtigt bleiben, dass die nationalen Cyber-Sicherheitsstrategien alle erdenklichen Bedrohungen im oder durch den Cyberraum zu erfassen versuchen, einschließlich der organisierten Kriminalität, Cyber-Spionage und schädigende Cyber-Operationen, wie den STUXNET-Angriff gegen die iranische Anreicherungsanlage. Folglich rechtfertigen sie nicht die Schlussfolgerung, alle von ihnen behandelten maliziösen Cyber-Operationen stellten eine Anwendung von Gewalt i.S. von Art. 2 Abs. 4 UN-Charta oder gar einen das Selbstverteidigungsrecht auslösenden bewaffneten Angriff i.S. von Art. 51 UN-Charta dar.

Allerdings kann festgehalten werden, dass sich die Staaten der durch die zunehmende Abhängigkeit zahlreicher Bereiche vom Cyberraum selbst geschaffenen Schadenanfälligkeit hinreichend bewusst sind, so dass sie heute bereit sind, Cyber-Operationen, die signifikante Wirkungen[6] zeitigen, als Anwendung von Gewalt und, soweit diese mit Blick auf ihr Ausmaß und Effekte hinreichend gravierend sind, als das Selbstverteidigungsrecht auslösende bewaffnete Angriffe anzusehen. Diese – recht allgemeine – Einordnung steht insoweit in grundsätzlichem Einklang mit der Rechtsprechung des Internationalen Gerichtshofs (IGH), als das Gewaltverbot und das Selbstverteidigungsrecht nicht auf bestimmte Einsatzmittel begrenzt werden können, sondern Anwendung finden auf ‚any use of force, regardless of the

---

[4] Australian Government, *Australia's Cyber Security Strategy* (2016), S. 15 (2016), abrufbar unter: https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf (last visited on 11 October 2019). Siehe auch Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (2016), abrufbar untert: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile, in der auf S. 14 ein Cyber-Angriffe definiert wird als 'IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised.' Vgl. ferner further Public Safety Canada, *National Cyber Security Strategy* (2018), abrufbar unter: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf, in der auf S. 33 ein Cyber-Angriff definiert wird als 'an attack that involves the unauthorized use, manipulation or destruction of, or access to, via electronic means, electronic information or the electronic devices or computer systems and networks used to process, transmit or store that information.'

[5] Cyber Security Agency of Singapore, *Singapore's Cybersecurity Strategy* (2016), S. 25, abrufbar unter: https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf.

[6] U.S. Department of Defense, *The DoD Cyber Strategy* (April 2015), S. 5, abrufbar unter: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

weapons employed.'[7] Entscheidend kommt es darauf an, ob eine Cyber-Operation dazu bestimmt ist, Tod, Verletzung, Schaden oder Zerstörung zu verursachen, oder diese Wirkungen tatsächlich zeitigt. Das ist zweifellos zu bejahen, wenn die Wirkungen denen eines Einsatzes konventioneller Mittel und Methoden der Kriegführung gleichen, was dann der Fall sein wird, wenn sie sich außerhalb des Cyberraums, mithin in der physischen Domäne, materialisieren. Schwieriger einzuordnen sind Cyber-Operationen, deren Wirkungen auf den Cyberraum beschränkt bleiben.

1. Cyber-Operationen mit Wirkungen außerhalb des Cyberraums (Operationen durch den Cyberraum) und Selbstverteidigungsrecht

a) Cyber-Operationen als Bestandteil einer traditionellen Gewaltanwendung

Eine Cyber-Operation durch den Cyberraum kann sich als Teil einer zusammengesetzten Handlung darstellt, die darauf gerichtet ist, schädigende kinetische Wirkungen zu verursachen. Beispielsweise kann eine Cyber-Operation Teil eines traditionellen militärischen Angriffs sein, wie etwa der israelische Angriff auf eine syrische Nukleareinrichtung im Jahr 2007, dem angeblich eine Cyber-Operation gegen die syrische Luftabwehr vorausging. [8] Derartige Cyber-Operationen können daher als Teile einer zusammengesetzten Handlung angesehen werden, die zusammengenommen mit dem Einsatz traditioneller Mittel der Kriegführung als Gewaltanwendung oder bewaffneter Angriff eingeordnet werden kann oder aber als bloße Vorbereitungshandlung. Insoweit bestehen folglich keine nennenswerten völkerrechtlichen Einordnungsschwierigkeiten.

b) Eigenständige Cyber-Operationen

Cyber-Operationen durch den Cyberraum, die nicht (notwendige) Bestandteile einer traditionellen Gewaltanwendung sind, können darauf gerichtet sein, dem Einsatz traditioneller Schädigungsmittel vergleichbare Wirkungen zu zeitigen, indem sie Objekte außerhalb des Cyberraums (oder die physikalische Infrastruktur des Cyberraums) beschädigen oder zerstören. Auch Personen können durch Cyber-Operationen verletzt oder getötet werden, wenn etwa die Cyber-Infrastruktur eines Krankenhauses angegriffen wird und dadurch lebenserhaltende Maßnahmen nicht mehr durchgeführt werden können. In nationalen Cyber-Sicherheitsstrategien werden auch derartige Cyber-Operationen behandelt, ohne sie jedoch als das Selbstverteidigungsrecht auslösende bewaffnete Angriffe einzuordnen. So betont beispielsweise das U.S. Department of Defense seine Bereitschaft, ‚to defend the nation against cyberattacks of significant consequence'[9], jedoch erlaubt die Verwendung des Verbs ‚to defend' nicht notwendigerweise die Schlussfolgerung, derartige Cyber-Operationen würden stets als bewaffnete Angriffe angesehen. Auch das Handbuch des U.S. Department of Defense begnügt sich mit einer recht allgemeinen und daher wenig hilfreichen Feststellung:

---

[7] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion of 8 July 1998, ICJ Reports 1998, 226-267, 224, Abs. 39.

[8] Vgl. D.E. Sanger / M. Mazzetti, 'Israel Struck Syrian Nuclear Project, Analysts Say', The New York Times, October 14, 2007, abrufbar unter: https://www.nytimes.com/2007/10/14/washington/14weapons.html.

[9] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 6), S. 3.

> ‘A State’s inherent right of self-defense, recognized in Article 51 of the Charter of the United Nations, may be triggered by cyber operations that amount to an armed attack or imminent threat thereof.’[10]

Weitere Stellungnahmen erlauben aber eine deutlichere Einordnung. Die U.S. Joint Chiefs of Staff weisen darauf hin, dass Cyber-Operationen ‚are often employed with little or no associated physical destruction‘, betonen aber auch, dass ‚modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domain.’[11] Der damalige Rechtsberater des U.S. Department of State stellte 2012 fest, dass ‚cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force’[12], so dass u.a. die folgenden Cyber-Operationen als Anwendung von Gewalt und, bei hinreichender Schwere, bewaffnete Angriffe eingeordnet warden könnten:

> ‘(1) operations that trigger a nuclear plant meltdown, (2) operations that open a dam above a populated area causing destruction, or (3) operations that disable air traffic control resulting in airplane crashes.’[13]

Für Koh entspricht es gesundem Menschenverstand, Cyber-Operationen, deren physische Wirkungen denen traditioneller Mittel der Kriegführung gleichkommen als Gewaltanwendung einzuordnen, so dass das Selbstverteidigungsrecht eines Staates durch ‚computer network activities that amount to an armed attack or imminent threat thereof’[14] ausgelöst werden kann.

Eine vergleichbare Position hat der britische General-Anwalt vertreten:

> ‘[…]. the UK considers it is clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to an inherent right to take action in self-defence, as recognised in Article 51 of the UN Charter.
> If a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us. If it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects.

[10] U.S. Department of Defense, *Law of War Manual* (Fn. 2) Abs. 16.3.
[11] Joint Chiefs of Staff, Cyberspace Operations (Fn. 1), S. II-11.
[12] Harold H. Koh,’ International Law in Cyberspace’, 54 Harvard International Law Journal – Online (December 2012), 1-12, 4, abrufbar unter: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=5858&context=fss_papers.
[13] Ebd.
[14] Ebd.

> Acts like the targeting of essential medical services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means.'[15]

Schließlich wird auch in der südkoreanischen Cyber-Sicherheitsstrategie ausdrücklich die Möglichkeit betont, dass bestimmte Cyber-Operationen Wirkungen zeitigen können, die denen traditioneller bewaffneter Angriffe gleichstehen.[16]

Diese und vergleichbare Stellungnahmen eignen sich nicht notwendigerweise zum Nachweis einer allgemeinen Staatenpraxis oder einer Rechtsüberzeugung, die für die Geltung einer entsprechenden Gewohnheitsrechtsnorm (oder allgemein anerkannten Interpretation) erforderlich sind. In diesem Zusammenhang sind die folgenden Faktoren zu berücksichtigen: (1) Nationale Cyber-Sicherheitsstrategien beruhen auf einem integrierten Ansatz, der die Staaten in die Lage versetzen soll, auf das gesamte Spektrum von Cyber-Bedrohungen zu reagieren, so dass das Selbstverteidigungsrecht lediglich eine unter mehreren Optionen darstellt. (2) Einige Staaten scheuen sich, das Selbstverteidigungsrecht ausdrücklich in Bezug zu nehmen. Dies mag innenpolitischen Erwägungen geschuldet sein (wie etwa im Falle Deutschlands) oder dem starken Fokus auf den Schutz der eigenen Volkswirtschaft und der öffentlichen Ordnung (wie im Falle Singapurs). Gleichwohl ist davon auszugehen, dass solche und auch andere Staaten eine Gewaltanwendung oder – bei hinreichender Schwere – einen bewaffneten Angriffs bejahen würden, wenn sie Ziel einer maliziösen Cyber-Operation werden, deren Wirkungen in der physischen Domäne denen des Einsatzes traditioneller Mittel und Methoden der Kriegführung gleichkommen.

Bei bewaffneten Angriffen mit traditionellen Mitteln und Methoden der Kriegführung besteht mittlerweile weitgehende Einigkeit, dass eine Ausübung des Selbstverteidigungsrechts nicht erst dann zulässig ist, wenn sich die Schäden materialisieren. Ausreichend ist es, wenn dies unmittelbar bevorsteht, weil der Angreifer aller erforderlichen Schritte unternommen hat. In diesem Zusammenhang bestehen zwar insoweit einige semantische Verwirrungen, als die Einordnung der Selbstverteidigung als ‚präventiv', ‚präemptiv', ‚antizipatorisch', oder ‚interzeptiv' mehr Fragen aufwirft als zur Klärung beiträgt. Gleichwohl kann festgehalten werden, dass ein Staat nicht bis zum Schadenseintritt abwarten muss. Angesichts der hohen Geschwindigkeit des Datentransfers ist es jedoch durchaus schwierig, einen unmittelbar bevorstehenden Cyber-Angriff festzustellen, ohne dass es bereits zu Schäden gekommen ist. Auch die bloße Implementierung einer maliziösen Software ist nicht unbedingt ausreichend, um von einem unmittelbar bevorstehenden bewaffneten Angriff ausgehen zu können. Anders verhält es sich jedoch im Falle von Angriffszielen, die der kritischen Infrastruktur – z.B. Energieversorgung, Gesundheitssystem – zugerechnet werden können, da ein Abwarten des Schadenseintritts zu weitreichenden, nicht zumutbaren Konsequenzen führen würde. Darauf wird unter I. 2. Zurückzukommen sein.

---

[15] Attorney General Jeremy Wright, Cyber and International Law in the 21st Century, Speech delivered on 23 May 2018, available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (last visited on October 7, 2019).

[16] National Security Office (South Korea), National Cybersecurity Strategy, S. 6. Diese ist unmittelbar als pdf-Datei abrufbar.

c) Zusammengesetzte Handlung

Schließlich sei nochmals auf das auch von der Völkerrechtskommission der Vereinten Nationen anerkannte Konzept der zusammengesetzten Handlung (‚composite act') eingegangen.[17] Es ist durchaus möglich, dass eine Reihe von Cyber-Operationen nicht einzeln, aber in ihrer Gesamtheit Wirkungen zeitigen, die denen des Einsatzes traditioneller Schädigungsmittel gleichkommen. Beispielsweise kann durch eine Cyber-Operation eine sog. Hintertür im Zielsystem geschaffen werden, die es dem Angreifer erlaubt, sich jederzeit Zugang zu verschaffen, etwa um zu einem späteren Zeitpunkt eine Schadsoftware zu installieren, die dann Schäden oder Zerstörungen in der physischen Domäne verursacht, wie etwa Flugzeugabstürze, weil die Flugzeuge nicht mehr von einem Luftverkehrsleitsystem geführt werden können. In diesem Fall ist das Installieren der Hintertür Teil einer zusammengesetzten Handlung, die in ihrer Gesamtheit eine Anwendung von Gewalt bzw. einen bewaffneten Angriff darstellen kann.

d) Zwischenergebnis

Cyber-Operationen, deren Wirkungen sich außerhalb des Cyberraums materialisieren und die Tod, Verletzung, Schäden oder Zerstörungen zeitigen oder zu zeitigen geeignet sind, können als gegen den Zielstaat gerichtete Gewaltanwendung angesehen werden. Sind die Konsequenzen mit Blick auf ihre Wirkungen und ihr Ausmaß von hinreichender Schwere, sind diese Cyber-Operationen bewaffnete Angriffe, die das Selbstverteidigungsrecht des Opfers auszulösen geeignet sind. Das Opfer derartiger Angriffe ist nicht zu einer gleichartigen Reaktion verpflichtet, sondern kann sich auch für den Einsatz traditioneller Wirkmittel entschließen, solange die Schranken des Selbstverteidigungsrechts – Erforderlichkeit, Verhältnismäßigkeit, Unmittelbarkeit – gewahrt bleiben.

2. Cyber-Operationen, deren Wirkungen auf den Cyberraum beschränkt bleiben (Cyber-Operationen im Cyberraum)

Es besteht noch keine allgemeine Einigkeit, ob und unter welchen Voraussetzungen Cyber-Operationen im Cyberraum als Anwendung von Gewalt oder bewaffneter Angriff eingeordnet werden können. Erinnert sei in diesem Zusammenhang an die im Jahr 2007 gegen Estland gerichteten DDoS-Angriffe, die trotz ihrer weitreichenden Auswirkungen auf den öffentlichen und Finanzsektor nicht als bewaffnete Angriffe i.S. von Art. 5 des NATO-Vertrags angesehen wurden. Zu berücksichtigen ist zudem, dass Daten bislang noch nicht Objekten gleichgestellt werden können, so dass das Löschen von Daten als solches nicht als Zufügung eines materiellen Schadens eingeordnet werden kann. In diesem Zusammenhang ist auch zu berücksichtigen, dass dem Völkerrecht ein Verbot der Cyberspionage fremd ist – da wohl alle

[17] Vgl. International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83 vom 28. Januar 2002. Art. 15 der Entwurfsartikel lautet:

(1) The breach of an international obligation by a State through a series of actions or omissions defined in aggregate as wrongful occurs when the action or omission occurs which, taken with the other actions or omissions, is sufficient to constitute the wrongful act.

(2) In such a case, the breach extends over the entire period starting with the first of the actions or omissions of the series and lasts for as long as these actions or omissions are repeated and remain not in conformity with the international obligation.

Staaten verdeckt im und durch den Cyberraum Informationen sammeln. Das nicht-autorisierte Eindringen in ein fremdes System geht aber häufig mit einer Modifikation oder einem Löschen bestimmter, im Zielsystem residenter Daten einher. Würde mithin das bloße Löschen von Daten als Zufügung eines Schadens gewertet, würden sich die Staaten der Möglichkeit der Cyberspionage begeben. Eine dahingehende Bereitschaft oder gar Rechtsüberzeugung ist jedoch nicht feststellbar. Schließlich ist in diesem Zusammenhang auch in Erinnerung zu rufen, das wirtschaftliche oder finanzielle ‚Schäden' vom Anwendungsbereich des Gewaltverbots und des Selbstverteidigungsrechts ausgeschlossen werden.

Trotz dieses Befundes ist ein langsames Umdenken zu verzeichnen, da sich die Staaten ihrer – selbst geschaffenen – Verwundbarkeit gegenüber maliziösen Cyber-Operationen zunehmend bewusstwerden. So hat der Beirat für auswärtige Angelegenheiten des Königreichs der Niederlande die Ansicht vertreten, Cyber-Operationen als bewaffnete Angriffe einzuordnen, wenn sie die Funktionsweise des Staates nachhaltig beeinträchtigen:

> 'It is more difficult to conclude whether this is the case if there are no actual or potential fatalities, casualties or physical damage. A serious, organised cyber attack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state. In such cases, there must be a disruption of the state and/or society, or a sustained attempt thereto, and not merely an impediment to or delay in the normal performance of tasks for it to be qualified as an armed attack. A disruption of banking transactions or the hindrance of government activity would not qualify as an armed attack. However, a cyber attack that targets the entire financial system or prevents the government from carrying out essential tasks, for example an attack on the entire military communication and command network that makes it impossible to deploy the armed forces, could well be equated with an armed attack.'[18]

Auch das U.S. Verteidigungsministerium wertet gegen militärische Befehls- und Führungsstrukturen gerichtete Cyber-Operationen als bewaffnete Angriffe, wenn festgestellt wird, dass , DoD networks and key resources on which DoD relies for its operations and attacks that could impact the U.S. military's ability to operate in a contingency.'[19] Das U.S. Verteidigungsministerium geht für Konfliktzeiten davon aus, dass that 'apotential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage.'[20] Auch in der britischen Cyber-Sicherheitsstrategie werden ‚vulnerabilities in cyberspace [that] could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home'[21] im Kontext des Selbstverteidigungsrechts thematisiert.

Die weiteren vom niederländischen Beirat angeführten Cyber-Operationen, die zu einer erheblichen Beeinträchtigungen öffentlicher oder gesellschaftlicher Funktionen führen, sind

---

[18] Advisory Council on International Affairs, Cyber Warfare, S. 21 (No 77, AIV/No 22, CAVV December 2011).
[19] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 3), S. 10.
[20] Ebd., S. 2.
[21] The UK Cyber Security Strategy, S. 15 (November 2011), abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

eng mit der zunehmenden Sorge der Staaten hinsichtlich ihrer verwundbaren kritischen Infrastrukturen verbunden.

In der nationalen Cyber-Sicherheitsstrategie der USA aus dem Jahr 2018 wird nachdrücklich auf die Notwendigkeit zum Schutz von ‚networks, systems, functions, and data'[22], der , domestic critical infrastructure and global supply chains'[23] ebenso hingewiesen wie auf die Verwundbarkeit der USA gegenüber ‚peacetime cyber attacks against critical infrastructure'.[24] Sorgen bereiten dem U.S. Verteidigungsministerium ‚a cyberattack of significant consequence on the U.S. homeland and U.S. interests'[25] sowie ‚a sophisticated actor [who] could target an industrial control system (ICS) on a public utility to affect public safety, or enter a network to manipulate health records to affects an individual's well-being. A disruptive, manipulative, or destructive cyberattack could present a significant risk to U.S. economic and national security if lives are lost, property destroyed, policy objectives harmed, or economic interests affected.'[26] Die U.S. Joint Chiefs of Staff befassen sich mit ‚methods producing WMD-like effects' and the 'catastrophic effects […] possible in cyberspace because of the existing linkage of cyberspace to critical infrastructure SCADA systems.'[27] Schließlich wird in einer weiteren U.S. Strategie Die Bedeutung nationaler Sicherheitsinteressen betont, zu denen ‚the survival of the Nation; the prevention of catastrophic attack against U.S. territory; the security of the global economic system; the security, confidence, and reliability of our allies; the protection of American citizens abroad; and the preservation of universal values.'[28] gezählt werden.

Auch andere Staaten haben die Notwendigkeit des Schutzes ihrer kritischen Infrastrukturen erkannt. Deutschland fasst unter den Begriff der kritischen Infrastruktur ‚organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences.'[29] Genannt werden die folgenden Sektoren: ‚energy, information technology and telecommunication, transport, health, water, food, finance and insurance, State and public administration, media and culture.'[30] Singapur verweist auf ‚essential services such as energy, banking, healthcare and transport [that] are powered by infocomm technology.'[31] Kanada definiert kritische Infrastruktur als , processes, systems, facilities, technologies, networks, assets and services essential to health, safety, security or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.'[32]

---

[22] President of the United States of America, National Cyber Security Strategy of the United States of America, S. 3 (September 2018), available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[23] Ebd., S. 26.
[24] Ebd. S. 3.
[25] U.S. Department of Defense, The DoD Cyber Strategy (Fn. 6), S. 14.
[26] Ebd., S. 2.
[27] Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Fn. 1), S. C1
[28] Chairman of the Joint Chiefs of Staff, The National Military Strategy of the United States of America 2015, S. 5 abrufbar unter: https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
[29] German Cyber Security Strategy (Fn. 4), S. 15.
[30] *Ibid*.
[31] *Singapore's Cybersecurity Strategy* (Fn. 5), S. 8.
[32] Canadian Cyber Security Strategy (*supra* Fn. 4), S. 33.

Die NATO-Staaten haben erkannt, dass , cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.'[33]

Den nationalen Cyber-Sicherheitsstrategien und weiteren Stellungnahmen ist gemein, dass sie gegen die kritische Infrastruktur gerichteten Cyber-Operationen ein dem Einsatz traditioneller Mittel und Methoden der Kriegführung gleichkommendes Schädigungspotential zuerkennen. Sie rechtfertigen aber nicht die Schlussfolgerung, die Staaten würden jede gegen die kritische Infrastruktur gerichtete Cyber-Operation als einen das Selbstverteidigungsrecht auslösenden bewaffneten Angriff einordnen. Die Bandbreitet derartiger Cyber-Operationen ist derart groß, dass ihre Wirkungen im besten Fall lediglich Unannehmlichkeiten bereiten, im schlimmsten Fall aber das Funktionieren des Staates schwer beeinträchtigen können. Angesichts dessen ist es schwerlich möglich, eine allgemeine Rechtsüberzeugung nachzuweisen, die zu einer anerkannten Klassifizierung solcher Cyber-Operationen führt ‚that do not have a clear kinetic parallel'.[34]

Gleichwohl ist es vertretbar, bestimmte Cyber-Operationen als Anwendungen von Gewalt oder bewaffnete Angriffe anzusehen. Dies gilt für (1.) Cyber-Operationen gegen die für die nationale oder Bündnisverteidigung wesentlichen Infrastrukturen; (2.) Cyber-Operationen die die Staatsfunktionen nachhaltig erschüttern; (3) Cyber-Operationen gegen die Energieversorgung, das Gesundheitswesen oder lebensnotwendige Versorgungsketten. Wohl nicht gefolgt werden kann der Auffassung, nach der Cyber-Operationen gegen das gesamte Finanzsystem unter Art. 2 Abs. 4 und Art. 51 UN-Charta fallen.

3. Herausforderungen

Wenngleich es möglich ist, bestimmte Cyber-Operationen als Anwendungen von Gewalt oder gar bewaffnete Angriffe einzuordnen, sehen sich Staaten vergleichsweise großen Schwierigkeiten gegenüber.

Erstens besteht das Problem der **Zurechenbarkeit** einer Cyber-Operation zu einem bestimmten Staat fort. Die Handlungen, die einem Staat nach Maßgabe des Völkerrechts zugeordnet werden können, beschränken sich zwar nicht auf Organverhalten, sondern auch auf das Verhalten von Privatpersonen.[35] Gleichwohl steht die dem Cyberraum eigene Anonymität, aber auch die Möglichkeit, dass ein sog. Botnet zum Einsatz kommen kann, einer hinreichend sicheren Zurechnung häufig entgegen. Obgleich es mitunter gelungen ist,

[33] NATO, Wales Summit Declaration, Abs. 72 (5. September 2014), abrufbar unter: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf.

[34] Harold H. Koh, International Law in Cyberspace (*supra* note 9), p. 7.

[35] Vgl. dazu die Art. 4 ff. der Entwurfsartikel der Völkerrechtskommission zur Staatenverantwortlichkeit (Fn. 17).

maliziöse Cyber-Operationen einem bestimmten Staat zuzurechnen[36], bedarf es immer noch einer erheblichen Verbesserung cyber-forensischer Fähigkeiten, ohne die eine wirksame Reaktion nur unter engen Voraussetzungen möglich wäre. Daher hat der Befund der U.S. Joint Chiefs of Staff immer noch Gültigkeit:

> 'To initiate an appropriate defensive response, attribution of threats in cyberspace is crucial for any actions external to the defended cyberspace beyond that authorized as authorized self-defense. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state, with sufficient confidence and verifiability to hold them accountable.'[37]

Zweitens ist es, wie bereits erwähnt, äußerst schwierig, einen **unmittelbar bevorstehenden** oder bereits begonnenen **Angriff** im oder durch den Cyberraum hinreichend sicher festzustellen. Daher mögen die Konzepte der ‚antizipatorischen', ‚präventiven', ‚präemptiven' oder ‚interzeptiven' Selbstverteidigung im Cyberraum wenig ergiebig sein. Soweit ein unmittelbar bevorstehender Angriff im oder durch den Cyberraum in Frage steht, sind die im Tallinn-Handbuch 2.0 gegebenen Beispiele durchaus hilfreich:[38] (1) die Implementierung einer ‚logischen Bombe', wenn es hinreichend wahrscheinlich ist, dass zur Aktivierung notwendigen Bedingungen erfüllt werden; (2) die Implementierung einer maliziösen, aus der Ferne auszulösenden Software, wenn und soweit der Auslösende sich tatsächlich zum Angriff entschlossen hat.

Drittens besteht ein letztes praktisches Problem, wenn für das Vorliegen einer Gewaltanwendung oder eines bewaffneten Angriffs ein **subjektives Element** in Form von Vorsatz oder Absicht gefordert wird. Dies lässt sich weder in der physischen Domäne noch im Cyberraum feststellen. Zudem ist Art. 2 Abs. 4 und Art. 51 UN-Charta ein dahingehendes Erfordernis nicht zu entnehmen. Im Übrigen besteht stets die Möglichkeit, dass eine Cyber-Operation unbeabsichtigte Wirkungen bzw. Sekundärwirkungen zeitigt, die objektiv geeignet sind, eine Gewaltanwendung oder einen bewaffneten Angriff zu indizieren.

II. Weitere völkerrechtliche Fragestellungen

1. Due diligence

Der IGH hat im Korfu-Kanal-Fall festgestellt, ‚it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[39] Angewendet auf maliziöse Cyber-Operationen, die auf dem Territorium eines Staates vorgenommen, ohne dass sie diesem Staat zugerechnet werden können, und gegen einen anderen Staat gerichtet sind, ist der Ausgangsstaat verpflichtet, diese Cyber-Operationen zu beenden, sobald er davon

[36] Verwiesen sei lediglich auf den Mandiant Report aus dem Jahr 2013, in dem der Nachweis erbracht wurde, dass gegen die USA gerichtete maliziöse Cyber-Operationen der Volksrepublik China zurechenbar waren. Vgl. https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html. Joint Chiefs of Staff, Cyberspace Operations (Fn. 1), S. I-12. Vgl. auch die deutsche Cyber-Sicherheitsstrategie (Fn. 4), S. 3

[38] Michael N. Schmitt (gen. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge 2017), Kommentierung zur Regel 73, Abs. 7 f..

[39] International Court of Justice, Corfu Channel Case (United v. Albania), ICJ Rep. 1949, 4, 22.

Kenntnis erlangt hat oder hätte erlangen können. Dabei macht es keinen Unterschied, ob Ziele der Cyber-Operationen staatliche Einrichtungen oder private Infrastrukturen sind, da es um den Schutz der territorialen Integrität des Zielstaates geht. Allerdings impliziert dies keine Pflicht zur Prävention oder gar zu einer umfassenden Überwachung der sich auf dem Territorium ereignenden Cyber-Operationen.

2. Abwehr von maliziösen Cyber-Operationen, die unterhalb der Gewalt- bzw. Angriffsschwelle verbleiben

Selbst wenn maliziöse Cyber-Operationen unterhalb der Gewalt- oder Angriffsschwelle verbleiben, können sie wegen der mit ihnen einhergehenden Verletzungen der Souveränität des Zielstaates als völkerrechtwidrig eingeordnet werden.[40] Der Opferstaat bleibt dann nicht auf Proteste oder andere diplomatische Reaktionen beschränkt, sondern darf seinerseits mit einer verhältnismäßigen Gegenmaßnahme, also einem völkerrechtswidrigen Akt, reagieren, um den betreffenden Staat zu veranlassen, von seinem völkerrechtswidrigen Handeln abzulassen.[41] Freilich setzt dies die Zurechenbarkeit zu dem anderen Staat voraus.

Zudem besteht unter engen Voraussetzungen die Möglichkeit zur Verfügung, einen Notstand geltend zu machen, wenn eine nicht zurechenbare maliziöse Cyber-Operation eine schwere und unmittelbar drohende Gefahr für ein wesentliches Interesse (‚essential interest') des Staates verursacht.[42] Dann darf, soweit die weiteren Schranken beachtet werden, diese Gefahr abgewehrt werden, selbst wenn dadurch die Rechte anderer (unbeteiligter) Staaten beeinträchtigt werden.

3. Unterscheidung zwischen defensiven und offensiven Cyber-Operationen

Schließlich sollte erwogen werden, die gängige Unterscheidung zwischen defensiven und offensiven Cyber-Operationen insoweit aufzubrechen, als es um effektive Gegenmaßnahmen gegen maliziöse Cyber-Operationen geht. Gegenmaßnahmen im und durch den Cyberraum können nur dann hinreichend wirksam sein, wenn sie nicht allein auf die Abwehr beschränkt sind und wenn die Verantwortlichen mit Blick auf offensive Cyber-Operationen nicht allein über theoretische Kenntnis, sondern auch über hinreichende praktische Fähigkeiten verfügen.

---

[40] Vgl. dazu Tallinn Manual 2.0 (Fn. 38), Rules 1 ff.

[41] Vgl. dazu allein die Art. 22, 49 ff. der Entwurfsartikel der Völkerrechtskommission zur Staatenverantwortlichkeit (Fn. 17).

[42] Vgl. ebd., Art. 25:

‘1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:

(*a*) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and

(*b*) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.

2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:

(*a*) the international obligation in question excludes the possibility of invoking necessity; or

(*b*) the State has contributed to the situation of necessity.’

Stellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die öffentliche Anhörung des Verteidigungsausschusses am 15. März 2021 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".

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)985
25.02.2021 - 19/3727
5410

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

Der Sachverständige bedankt sich bei Dr. Matthias Schulze[2] für die wertvolle Grundlagenarbeit in diesem Bereich.

Kontakt

Dr. Sven Herpig
sherpig@stiftung-nv.de
@z_edian (Twitter)
Leiter für Internationale Cybersicherheitspolitik
Stiftung Neue Verantwortung

[1] Stiftung Neue Verantwortung (2020): Experten-Profil von Dr. Sven Herpig
[2] Stiftung Wissenschaft und Politik (2020): Experten-Profil von Dr. Matthias Schulze

1. Die Rolle der Bundeswehr in der deutschen Cybersicherheitsarchitektur

Der erste Grundstein für die deutsche Cybersicherheitsarchitektur wurde bereits 1986 gelegt. In diesem Jahr wurde in der Vorgängerorganisation des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Zentralstelle für das Chiffrierwesen (ZfCh), „[...] eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte“[3]. Am 1. Januar 1991 nahm das Bundesamt für Sicherheit in der Informationstechnik nach Ausgründung aus dem Bundesnachrichtendienst (BND) seine Arbeit auf. In den öffentlichen Fokus geriet die Cybersicherheitsarchitektur dann insbesondere im Jahr 2011 durch die Veröffentlichung der Cyber-Sicherheitsstrategie für Deutschland.[4] Seitdem hat sich einiges getan. Zum Einen wurde die Architektur um viele neue Akteure – wie zum Beispiel das Kommando Cyber- und Informationsraum der Bundeswehr – ergänzt.[5] Zum Anderen ist Cybersicherheitspolitik ein elementarer Bestandteil der deutschen Innen-, Außen- und Sicherheitspolitik geworden.

Cybersicherheit wird in Deutschland auf Bundes- und Länderebene seit je her von zivilen Behörden hergestellt.[6] Hierbei laufen alle Fäden beim Bundesamt für Sicherheit in der Informationstechnik zusammen. Diese Nationale Cybersicherheitsbehörde[7] ist unter anderem für den Schutz der Regierungsnetze, die Kooperation mit der Wirtschaft und die Bereitstellung von Informationen für die Gesellschaft verantwortlich. Hinzu kommen das Bundeskriminalamt zur Bekämpfung von Cyberkriminalität und des Bundesamt für Verfassungsschutz zur nachrichtendienstlichen Aufklärung. Auf Länderebene werden diese Funktionen analog übernommen, unter anderem vom Landesamt für Sicherheit in der Informationstechnik, dem Hessen3C, den Landesämtern für Verfassungsschutz und den Landeskriminalämtern. Nachrichtendienstliche Erkenntnisse aus dem Ausland zur Cybersicherheitslage fließen zusätzlich durch den Bundesnachrichtendienst in die Arbeit der Behörden ein.[8] Das Nationale Cyber-Abwehrzentrum – in dem auch das Bundesamt für den Militärischen Abschirmdienst und das Kommando Cyber- und Informationsraum der Bundeswehr vertreten sind – bietet für all diese Erkenntnisse eine Kooperationsplattform.[9]

Die Rolle des Bundeswehr bei der gesamtstaatlichen Sicherheitsvorsorge im Bereich Cybersicherheit im Frieden ist verfassungsrechtlich in der Praxis bisher hauptsächlich auf den Eigenschutz, also defensive Aktivitäten, begrenzt. Auf Basis der Anzahl und Heterogenität der eigenen IT-Systeme ist dies eine sinnvolle Nutzung der vorhandenen Ressourcen zur Steigerung der Resilienz der

[3] Bundesamt für Sicherheit in der Informationstechnik (2003): Jahresbericht 2003
[4] Bundesministerium des Innern (2011): Cyber-Sicherheitsstrategie für Deutschland 2011
[5] Sven Herpig und Rebecca Beigel (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten
[6] Sven Herpig und Rebecca Beigel (2020): Deutsche Cybersicherheits- und Cyberverteidigungspolitik: Staatliche Akteure und Zuständigkeiten
[7] Offiziell “Cybersicherheitsbehörde des Bundes”, vgl.: Sven Herpig (2020): Die „Unabhängigkeit“ des Bundesamtes für Sicherheit in der Informationstechnik
[8] Bundesnachrichtendienst (2020): Cybersicherheit
[9] Bundeskriminalamt (2020): Nationales Cyber-Abwehrzentrum

Bundeswehr-IT, vor allem wenn zukünftig vermehrt auf den Einsatz von Maschinellem Lernen gesetzt werden soll.[10] Zukünftig könnte die Möglichkeit der Amtshilfe gem. § 35 GG durch die Bundeswehr bei schweren Cybervorfällen noch weiter beleuchtet werden, zum Beispiel durch konkrete Einsatzszenarios. In bisheriger Ermangelung eines zivilen Katastrophenschutzes für den Cyberraum[11], könnte die Bundeswehr möglicherweise öffentliche Einrichtungen wie Universitäten bei der Wiederherstellung ihrer Systeme nach einem "Großschadensfall" – z. B. einem Ransomware-Angriff – unterstützen.

2. Die Grenze von Defensiv und Offensiv im Cyberraum

Die Grenze zwischen defensiv und offensiv wird im Cyberraum in der Regel dann überschritten, wenn die getätigten Maßnahmen nicht mehr die eigenen Systeme, sondern Systeme von Dritten und / oder Systeme des intendierten Ziels betreffen (vgl. Abbildung 1).

Innerhalb offensiver Maßnahmen wäre eine trennscharfe Grenze zwischen Informationsgewinnung – im Sinne einer technischen Sondierung ohne intrusive Maßnahmen – und Aufklärung/ Wirkung dann erreicht, wenn die IT-Schutzziele[12] – Vertraulichkeit, Integrität und Verfügbarkeit – der Zielsysteme beeinträchtigt werden.[13] Solange sie nicht beeinträchtigt werden, zum Beispiel durch Aktivitäten wie Portscans, sind die Maßnahmen nicht intrusiv und es kann von Informationsgewinnung gesprochen werden.[14] Dies kann auch der Fall sein, wenn zwar das Schutzziel Vertraulichkeit verletzt wird, aber das Zielsystem über keinerlei Sicherheitsfunktionen verfügt, die umgangen werden müssen, z. B. bei falsch konfigurierten Cloudstorage-Systemen.[15] Es handelt sich hierbei aufgrund der bereits genannten Herausforderungen seitens des Ziels – Informationsgewinnung (nicht intrusiv) von Aufklärung und Wirkung (beides intrusiv) zu unterscheiden – um eine bewusst konservative Auslegung von Informationsgewinnung.

Informationsgewinnung dient zur Identifikation von möglichen Zielsystemen (Bürosysteme aber auch Wehrtechnik) und ihren Schwachstellen. Das daraus resultierende Wissen bildet die Grundlage, um eigene intrusive offensive Maßnahmen vorzubereiten. Hierfür müssen zum Beispiel Exploits

[10] Sven Herpig (2019): Securing Artificial Intelligence und Sven Herpig (2020): Understanding the Security Implications of the Machine-Learning Supply Chain
[11] Wie ein ziviler Katastrophenschutz für den Cyberraum aussehen kann, wie z. B. hier skizziert: AG KRITIS (2020): Das Cyber-Hilfswerk
[12] Bundesamt für Sicherheit in der Informationstechnik (2020): IT-Grundschutz Kompendium
[13] Oft wird in der Unterscheidung zwischen Maßnahmen der Informationsgewinnung und der Aufklärung angeführt, dass Informationsgewinnung passiv ist, während Aufklärung aktiv ist. Jedoch ist zum Beispiel ein Portscan, eine Maßnahme der Informationsgewinnung, durchaus eine vorsätzliche Aktivität. Eine wirklich passive Maßnahme zur Informationsgewinnung wäre im Gegensatz hierzu ein Honeypot, der vom Gegner ausgelöst wird und damit ausschließlich reagiert. Aus diesem Grund wird hier die Unterscheidung zwischen nicht-intrusiv/intrusive und defensiv/offensiv gewählt.
[14] Matthias Schulze (2020): Militärische Cyberoperationen. Nutzen, Limitierungen und Lehren für Deutschland
[15] Vgl. z. B. UpGuard Team (2017): Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online

entwickelt oder beschafft und in Offensivwerkzeuge und -plattformen integriert werden. Darüber hinaus gilt es auch, detaillierte Einsatzgrundsätze zu formulieren, die, wie die Wahl der Offensivwerkzeuge und -plattformen, von den Informationen aus der Informationsgewinnung profitieren[16]. Auf Basis dieser Definition sollte Informationsgewinnung nicht notwendigerweise dem Parlamentsvorbehalt unterliegen.

3. Cyberverteidigung durch die Bundeswehr

Über die Aufgaben beim Eigenschutz, der Amtshilfe und der Informationsgewinnung hinaus besitzt die Bundeswehr aber auch intrusive offensive Cyberfähigkeiten. Diese können im Spannungs-, und Verteidigungsfall, also im Rahmen der Landes- und Bündnisverteidigung, sowie bei (robusten) Auslandsmandaten zum Einsatz kommen.[17] Sie unterliegen dabei denselben Beschränkungen wie die Fähigkeiten in anderen Domänen. Der Rolle von IT-Systemen Dritter, vor allem von Drittstaaten und deren Interdependenzen, wird allerdings noch zu wenig Beachtung geschenkt. Weiterhin sollte auch beim Mandats-, Spannungs-, und Verteidigungsfall die Aufmerksamkeit der Bundeswehr im Cyberraum auf dem Eigenschutz und der Amtshilfe gerichtet sein. Behörden im Ressort des Bundesministeriums des Innern, für Bau und Heimat – wie das Bundesamt für Sicherheit in der Informationstechnik – sollten ihrer ursprünglichen Aufgabe zur Erhaltung der Cybersicherheit in Deutschland nachkommen.

Für die Ausweitung der Befugnisse zum Einsatz offensiver intrusiver Cyberfähigkeiten der Bundeswehr außerhalb von Mandats-, Spannungs-, und Verteidigungsfall werden vor allem zwei Aspekte ins Feld geführt: Aktive Cyberabwehr und Aufklärung.

Aktive Cyberabwehr, die im verteidigungspolitischen Bereich auch als “digitaler Verteidigungsfall” traurige Berühmtheit erlangte, wirft noch einige Fragen auf.[18] Wann genau dieser aktiviert werden soll, ist im Kontext hybrider Bedrohungen, sowie der geringen Trennschärfe von Cyberkriminalität, aktiven Maßnahmen (Desinformation) und Aufklärung/ Wirkung fremder Staaten bisher weitestgehend unklar.[19] Expert:innen sind sich darüber hinaus nahezu gänzlich einig, dass die Durchführung von offensiven Maßnahmen im Cyberraum nicht dazu geeignet ist, anhaltende und laufende Cyberoperationen abzuschrecken[20] oder gar abzuwehren[21]. Hinzu kommt, dass die aktuellen gesetzlichen Regelungen hier die Zuständigkeit für Gefahrenabwehr auf Länderebene sehen. Eine Änderung dieser Regelungen hat vor dem Hintergrund fehlender Effektivität und weiteren Herausforderungen wie fristgerechter Zurechnung (Attribution), vor allem in zeitkritischen Situationen, keinen Sinn. Die Zurechnung von gegnerischen offensiven intrusiven Maßnahmen ist in der Regel ein

[16] Jack Rhysider (2020): Darknet Diaries - Ep 50: Operation Glowing Symphony
[17] Matthias Schulze (2020): German military cyber operations are in a legal gray zone
[18] Sven Herpig (2018): Aktive Cyber-Abwehr / Hackback
[19] Matthias Schulze (2020): German military cyber operations are in a legal gray zone
[20] Matthias Schulze (2019): Überschätzte Cyber-Abschreckung
[21] Sven Herpig et al. (2020): Aktive Cyberabwehr/ Hackback in Deutschland – Leseliste 2017-2020 –

langwieriger, komplexer Prozess (lies: Wochen oder Monate statt Stunden oder Tage), der vor allem technische, aber auch nachrichtendienstliche und politische Erkenntnisse umfasst.

Die Aufklärung ähnelt in Ziel und Funktion der Informationsgewinnung, ist jedoch im Gegensatz zu ihr intrusiv. Das heißt es werden hierbei die IT-Schutzziele der Zielsysteme verletzt. Hierdurch können zusätzliche Informationen erworben werden, die für die Vorbereitung im Rahmen von Wirkungsmaßnahmen genutzt werden können. Weiterhin können Veränderungen in den Zielsystemen (z. B. unautorisierter Einbau von “Hintertüren”) vorgenommen werden, damit in einem späteren Bedarfsfall zeitnah gehandelt werden kann. Die Herausforderung hierbei ist, dass bei intrusiven offensiven Maßnahmen das Ziel kaum zwischen Aufklärung und Wirkung unterscheiden kann.[22] Offensive intrusive Maßnahmen der Bundeswehr im Cyberraum benötigen daher einen Mandats-, Spannungs-, Verteidigungs- und Bündnisfall als Rechtsgrundlage, auch wenn das einen gewissen Vorlauf zur Durchführung offensiver Maßnahmen benötigt. Nur so kann eine unabsichtliche Eskalation verhindert und internationales Recht (z. B. Artikel 2 Absatz 4 und Artikel 51, Charta der Vereinten Nationen)[23] geachtet werden.

<table>
<tr><th colspan="2">Defensiv</th><th colspan="3">Offensiv</th></tr>
<tr><th colspan="3">Nicht-Intrusiv</th><th colspan="2">Intrusiv</th></tr>
<tr><td>Eigenschutz</td><td>Amtshilfe</td><td>Informationsgewinnung</td><td>Aufklärung</td><td>Wirkung</td></tr>
</table>

Abbildung 1: Maßnahmen der Bundeswehr im Cyberraum (nicht abschließend)

4. Zurechnung (Attribution) von Aufklärungs- und Wirkungsmaßnahmen

Die Zurechnung von Aufklärungs- und Wirkungsmaßnahmen ist relevant für die Lagebilderstellung und mittel- bis langfristige strategisch-politische Beantwortung von Cyberaktivitäten. Diese können auch die öffentliche Zuschreibung (engl. ebenfalls Attribution) eines Vorfalls zu seinen Urheber:innen umfassen. Aktuell gibt es jedoch noch eine Vielzahl an ungelösten Herausforderungen bei der strategischen Beantwortung von Cyberaktivitäten in der deutschen Cybersicherheitspolitik., wie z. B. ein fragmentiertes Zurechnungsberichtswesen.[24]

[22] Bruce Schneier (2014): Computer Network Exploitation vs. Computer Network Attack
[23] United Nations Regional Information Centre for Western Europe (1973): Charta der Vereinten Nationen und Statut des Internationalen Gerichtshofs
[24] 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.

5. Voraussetzung für den Einsatz offensiver intrusiver Cyberfähigkeiten durch die Bundeswehr

Grundlagen für Aufklärungs- und Wirkungsmaßnahmen sind die Kenntnis von Schwachstellen und Exploits, sowie Offensivwerkzeuge und -Plattformen. Die Beschaffung dieser Mittel muss genauer betrachtet werden. Beim Einsatz von Offensivwerkzeugen und -Plattformen sollten ethische Grundsätze berücksichtigt werden, da die entsprechenden Hersteller immer öfter mit suspekten Geschäftspraktiken[25] und daraus resultierenden Menschenrechtsverletztungen bis hin zur gezielten Tötung[26] in Verbindung gebracht werden. Aus Ermangelung eines nationalen staatlichen Schwachstellenmanagementmodells[27] sollte die Bundeswehr ausschließlich Exploits verwenden, die auf bereits bekannten Schwachstellen beruhen.[28] Es fehlt bisher an der behördenübergreifenden Analysefähigkeit, ob die Zurückhaltung einer spezifischen unbekannten Schwachstelle Deutschland mehr schadet (u.a. durch Kollateralschäden) als nutzt. Damit dies für die Bundeswehr und andere Akteure wie Nachrichtendienste ressortübergreifend sichergestellt werden kann, sollte von allen beteiligten Ressorts das Vorhaben des Bundesministeriums des Innern, für Bau und Heimat, ein staatliches Schwachstellenmanagement aufzubauen, aktiv unterstützt werden. Als Grundlage hierzu kann das SNV-Modell[29] dienen.

6. Schlussbemerkung

Während es im Rahmen von (robusten) Auslandsmandaten und – was hoffentlich nicht vorkommen wird – im Verteidigungs-, Spannungs- oder Bündnisfall durchaus Anwendungsfelder für den Einsatz offensiver intrusiver Cyberfähigkeiten geben kann, so müssen die rechtlichen, technischen und politischen Rahmenbedingungen von der Beschaffung bis zur Einbettung der Missionen in eine gesamtstaatliche Strategie detailliert und transparent ausgearbeitet werden.

Es ist jedoch wichtig anzuerkennen, dass die bisherige und aktuelle Cybergefährdungslage in Deutschland fast ausschließlich von organisierter Kriminalität und Nachrichtendiensten geprägt ist. Um diesen Aktivitäten entgegenzuwirken, muss die Bundesregierung gesamtstaatlich IT-Sicherheit und Resilienz fördern. Da der Bundeswehr als Teil dieses Ansatzes vor allem die Rolle des Eigenschutzes und ggf. der Amtshilfe zukommt sollte hier auch der politische und organisatorische Fokus liegen und nicht auf der Entwicklung offensiver intrusiver Cyberfähigkeiten. Der Satz: “Offensive ist die beste Defensive” gilt nicht im Cyberraum.

---

[25] Vgl. z.B. ZEIT ONLINE, dpa, msk (2020): Razzia bei Münchner BKA-Trojanerlieferant
[26] Vgl. z.B. David D. Kirkpatrick (2018): Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says
[27] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit
[28] Als bekannt wird hier eine Schwachstelle angesehen, wenn sie entweder öffentlich ist, dem Hersteller gemeldet wurde oder dem Bundesamt für Sicherheit in der Informationstechnik mit der Zielsetzung gemeldet wurde, diese dem Hersteller zu melden oder öffentlich vor ihr zu warnen.
[29] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit

Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen

Stellungnahme zur öffentlichen Anhörung im Verteidigungsausschuss am 15. März 2021

PD Dr. Dr. habil. Robert Koch

Robert.Koch@UniBw.de

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)997

09.03.2021 - 19/3781

5410

Vorbemerkung

Die vorliegende Stellungnahme ist keine offizielle Position des Bundesministeriums der Verteidigung, sondern die Sichtweise des Autors vor dem Hintergrund seiner wissenschaftlichen und fachlichen Expertise. Der Autor ist kein Jurist oder Völkerrechtler, sondern promovierter und habilitierter Informatiker mit fachlichem Schwerpunkt IT- und Cybersicherheit. Entsprechend werden nicht alle Fragestellungen des Fragenkatalogs adressiert, sondern es erfolgt insbesondere eine technische Analyse und Bewertung.

Zusammenfassung

Chancen und Risiken des Cyber- und Informationsraums Staat, Wirtschaft und Gesellschaft stehen in einer weiter zunehmend digitalisierten und vernetzten Welt wachsenden Herausforderungen im Cyber- und Informationsraum gegenüber. Während die Digitalisierung zahlreiche Chancen bietet, generiert sie aufgrund der dahinterliegenden Daten, Werte und Einflussmöglichkeiten in Verbindung mit den charakteristischen Eigenschaften des Cyber- und Informationsraums wie einer hohen Wirkasymmetrie, herausfordernder Attribuierung und globaler Konnektionsfähigkeit in Nahe-Echtzeit ein lukratives Ziel für Angreifer, von Script Kiddies über Hacktivisten und private Organisationen, der Organisierten Kriminalität (OK), bis hin zu staatlichen Akteuren. Das Spektrum der Angriffe kann dabei von einem Defacement von öffentlichen Webauftritten, einer Diensteverhinderung, bspw. durch eine Systemüberlastung mittels einer (D)DoS-Attacke[1] oder der erpresserischen Verschlüsselung von Systemen, der Exfiltration oder Manipulation von Daten bis hin zur physikalischen Zerstörung von Infrastruktur gehen.

Notwendigkeit und Grenzen von resilienten Systemen Mit der zunehmenden Professionalisierung von Cyberangriffen und einer steigenden Anzahl von Akteuren muss die staatliche Handlungsfähigkeit sichergestellt werden. Um die Risiken im Cyber- und Informationsraum auf ein tragbares Maß zu reduzieren, ist insbesondere eine effektive Zusammenarbeit im gesamtstaatlichen Ansatz und eine leistungsfähige, gesamtstaatliche Cyber-Sicherheitsarchitektur sowie die Erhöhung der Systemresilienz bspw. durch Nutzung gehärteter und hochsicherer Systeme insbesondere auch im Bereich der Kritischen Infrastrukturen (KRITIS) erforderlich. Da hochwertige Angriffsvektoren jedoch insbesondere auch bei hochsicheren und eigentlich resilient konzipierten System vorhanden sein können und in der Praxis wiederholt vorzufinden waren, ist durch defensive Maßnahmen alleine kein ausreichendes Sicherheitsniveau zu generieren. Das Vorhalten offensiver Fähigkeiten kann zur Gewährleistung der Cybersicherheit beitragen und ist insbesondere für den Erhalt der militärischen Handlungsfähigkeit zwingend erforderlich.

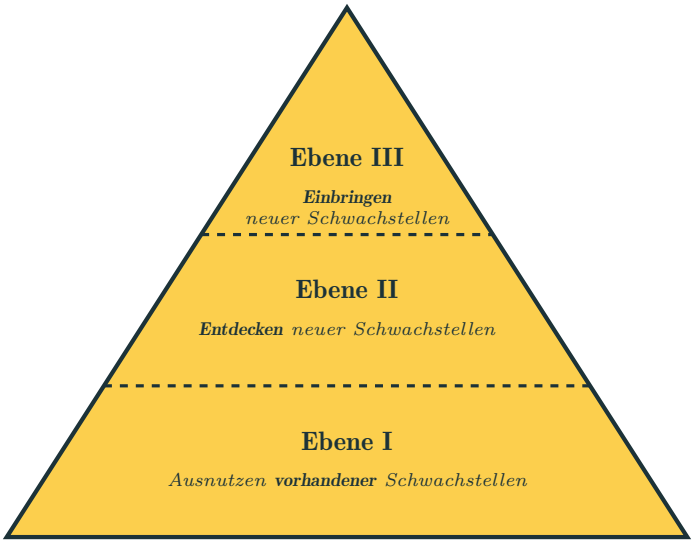
[1] (Distributed) Denial of Service

Was sind die Möglichkeiten und Grenzen von Cyberoperationen?

Für eine Diskussion der Möglichkeiten und Grenzen von Cyberoperationen kann die Fragestellung, welche Effekte auf welcher Basis generiert werden können, als Ausgangspunkt genutzt werden. Effekte können insbesondere in den Kategorien „Diensteverhinderung“ und „Daten“ generiert werden. Diensteverhinderung kann sowohl temporärer als auch permanenter Natur sein und direkt auf verschiedenen Ebenen, von Applikationen bis zur Hardware, oder indirekt bspw. durch die Störung von Kommunikationskanälen, erfolgen. Bzgl. Daten können insbesondere Aufklärung, Manipulation oder Zerstörung avisiert werden.

Herausforderungen der Cybersicherheit Um entsprechende Effekte zu erzielen, stehen eine Vielzahl von potentiellen Vektoren zur Verfügung; die weitverbreitete Ausnutzung von Schwachstellen in Software stellt hierbei lediglich einen kleinen Teilbereich dar. Vielmehr ist es erforderlich, eine holistische Betrachtung der Angriffsvektoren vorzunehmen; hier spiegelt sich insbesondere auch der Unterschied zwischen IT-Sicherheit und Cybersicherheit wider: Während IT-Sicherheit den „Zustand [beschreibt], in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind“[2], wird bei Cybersicherheit das Aktionsfeld der Informationssicherheit auf den gesamten Cyberraum ausgeweitet[3]. Cybersicherheit überschreitet daher insbesondere die Grenzen der eigenen Firma und beinhaltet Aspekte wie Stromversorgung, Telekommunikation und Versorgungsketten, welche regelmäßig *nicht* unter eigener Kontrolle stehen.

Um die unterschiedlichen Fähigkeiten und Möglichkeiten verschiedener Interessensgruppen, staatlicher als auch nichtstaatlicher Organisationen und Institutionen sowie von Streitkräften verstehen und einordnen zu können, bietet sich die Nutzung eines Bedrohungsmodells mit drei grundsätzlichen Ebenen an[4]:



Dreistufiges Bedrohungsmodell zu Schwachstellen im Cyberraum.

[2] Vgl. Definition „IT-Sicherheit“ im Glossar der Cyber-Sicherheit des BSI.
[3] Vgl. Definition „Cyber-Sicherheit“, ebd.
[4] Vgl. Defense Science Board, Task Force Report „Resilient Military Systems and the Advanced Cyber Threat“, 2012.

Ausnutzen vorhandener Schwachstellen In der unteren Ebene werden Bedrohungen eingeordnet, welche bereits öffentlich bekannte Schwachstellen ausnutzen. Solche finden sich bspw. in der CVE-Datenbank der MITRE Corporation[5], während andere Datenbanken wie bspw. die Exploit Database von Offensive Security[6] öffentlich verfügbare Exploits und fehlerhafte Programme sammeln und archivieren. Aufgrund der öffentlichen Verfügbarkeit der Informationen sollte gegen Angriffe dieser Ebene prinzipiell ein guter Schutz etablierbar sein. In der Praxis stößt dies aber aus einer Vielzahl von Gründen immer wieder an Grenzen. Ursachen können mangelhafte oder gar ausbleibende Bereitstellungen von Patches für fehlerhafte Produkte durch die betroffenen Unternehmen bis hin zur per se fehlenden Möglichkeit des Patchens eines Systems sein. Letzteres kann bspw. durch nicht ausreichende Systemressourcen bedingt sein, zum Beispiel bei IoT-Geräten[7], durch das Supportende eines Produkts oder gar, weil die entsprechende Herstellerfirma nicht mehr existiert. Gerade IT-Systeme in KRITIS und Steuerungsanlagen können hiervon betroffen sein, da dort regelmäßig eine besonders lange Nutzungsdauer vorliegt.

Die erhebliche Alltagsrelevanz dieser Ebene zeigt sich in der Praxis durch Vorfälle wie im Rahmen der Ransomware „WannaCry“, welche im Mai 2017 zahlreiche Systeme weltweit, insbesondere auch im Bereich der KRITIS und von Industrieanlagen, infizierte. Die ausgenutzte Schwachstelle war bereits bekannt und Patche verfügbar, betroffen waren aber insbesondere Systeme, welche vom Hersteller Microsoft nicht mehr unterstützt wurden, bspw. Windows XP und Server 2008[8].

Entdecken neuer Schwachstellen Auf der mittleren Ebene des Bedrohungsmodells finden sich Angriffe, welche auf Basis neu entdeckter und öffentlich noch unbekannter Schwachstellen, sog. Zero-Days (0days) ausgeführt werden. Zum Auffinden von 0day-Schwachstellen ist typischerweise ein entsprechend höherer Ressourcenaufwand erforderlich, insbesondere bzgl. Fachwissen, Systemkenntnis und Programmiererfahrung. Allerdings werden in den letzten Jahren neue Schwachstellen zunehmend durch automatisierte Softwaretests, bspw. Fuzzing, gefunden[9]. Hierbei werden die Fuzzingtechnologien stetig weiterentwickelt und u.a. auch mit Verfahren des maschinellen Lernens[10] kombiniert. Beachtet werden muss hierbei, dass Wert und Nutzen einer 0day-Schwachstelle für eine Cyberoperation sehr unterschiedlich sein können, da die Effekte von einfacher Diensteverhinderung bis hin zu entfernter Codeausführung mit administrativen Rechten[11] reichen können. Dies spiegelt sich bspw. in der Bewertung von Schwachstellen im Common Vulnerability Scoring System (CVSS)[12] wider. Stuxnet[13], der Angriff auf die iranische Urananreicherungsanlage in Natanz, ist von programmiertechnischer Perspektive dieser Ebene zuzurechnen.

Schwachstellen dieser Ebene müssen aber nicht zwangsläufig die Soft- oder Firmware betreffen, sondern können auch in Hardware vorliegen. Bspw. waren von der einfach angreifbaren Implementierung des pro-

[5] Common Vulnerabilities and Exposures, The MITRE Corporation
[6] The Exploit Database, Offensive Security
[7] Internet-of-Things
[8] Die Gruppe „The Shadow Brokers“ veröffentlichte den der NSA zugerechneten Exploit ETERNALBLUE (Schwachstelle CVE 2017-0144) am 14. April 2017, die Schadsoftware WannaCry verschlüsselte vom 12. bis 15. Mai 2017 zahlreiche Systeme weltweit. Ein Patch (MS17-010) wurde bereits im März 2017 herausgegeben, allerdings ursprünglich nicht für die von Microsoft nicht mehr unterstützten Betriebssysteme.
[9] Vgl. bspw. „Fuzzing ImageIO“ oder „5 CVEs found with Feedback-based Fuzzing“.
[10] Machine Learning (ML)
[11] Remote Code Execution with Privilege Escalation
[12] Vgl. Forum of Incident Response and Security Teams CVSS Special Interest Group (SIG), FiRST CVSS-SIG.
[13] Operation „Olympic Games“

prietären CRYPTO1-Algorithmus der weitverbreiteten „MIFARE Classic“[14] RFID[15]-Karten über 200 Millionen Exemplare betroffen[16,17]. Die Schwachstellen Spectre[18] und Meltdown[19], auf deren Basis unbefugt Speicherbereiche in modernen Prozessoren ausgelesen werden konnten, sind ebenfalls prominente Beispiele in diesem Bereich.

Einbringen neuer Schwachstellen Bedrohungen der oberen Ebene zeichnen Schwachstellen aus, welche *bewusst* in ein (typischerweise sicherheitsrelevantes) System eingeführt werden. Diese sind so angelegt, dass sie möglichst unauffällig sind und die originale Funktionsweise nicht beeinflussen. Neben einer Abbildung in Software, Firmware oder Hardware, können entsprechende Angriffsvektoren auch in mathematischen Verfahren (Algorithmik oder Zahlen) versteckt werden. Im Falle der Einbringung einer entsprechenden Schwachstelle in Hardware kann eine Aktivierung bzw. Ausnutzung entweder von außen in Form einer Hintertür (Backdoor) erfolgen, oder autark durch die Aktivierung bei bestimmten System- oder Umgebungsparametern[20]. Daraus ergibt sich eine sehr schwierige und ggf. nicht mögliche Detektierbarkeit, bei derzeit in der Praxis sehr eingeschränkten und oftmals nicht zerstörungsfreien Untersuchungsverfahren.

Aufgrund der hohen Komplexität und weltweiten Verzweigung der Versorgungsketten mit einer Vielzahl von beteiligten Akteuren in zahlreichen Ländern[21], gerade auch bei IT-Produkten, steigt das Risiko entsprechender Manipulationen in allen Bereichen, von der Design- bis zur Auslieferungsphase, erheblich an. Der Angriff auf die SolarWinds Orion Plattform, welcher im Dezember 2020 öffentlich bekannt wurde, unterstreicht die mögliche Tragweite solcher Operationen[22].

Weiterhin ergibt sich, insbesondere bei geeigneter Ausführung im Rahmen von Hardwaremanipulationen, ein hoher Grad an Abstreitbarkeit[23]. Beispiele hierfür sind die Diskussion aus dem Jahre 2012 um das Vorhandensein einer Hardware-Hintertür in einem auch in verschiedenen militärischen Anwendungen eingesetzten Mikrochip[24] oder der Bloomberg Businessweek-Artikel „The Big Hack“[25]. Auch wenn es stark umstritten ist, ob eine wie im Bloomberg-Artikel dargestellte Manipulation tatsächlich stattgefunden hat, ist die technische Realisierbarkeit gegeben[26]. Auch im Bereich der Algorithmik liegen öffentlich bekannte

[14] Hersteller NXP Semiconductors N.V.
[15] Radio Frequency Identification
[16] Vgl. bspw. Gerhard de Koning Gans, Jaap-Henk Hoepman und Flavio D. Garcia, „A practical attack on the MIFARE Classic“, International Conference on Smart Card Research and Advanced Applications, Springer, 2008 und Flavio D. Garcia, „Dismantling MIFARE Classic“, 13th European Symposium on Research in Computer Security, 2008.
[17] Dieses Beispiel unterstreicht außerdem, dass das Prinzip „Security by Obscurity“ seit langem überholt ist und keine geeignete Grundlage bietet, die Sicherheit eines Systems zu garantieren. Vielmehr ist gerade im Kryptobereich Kerckhoffs Prinzip (vgl. Auguste Kerckhoffs, „La cryptographie militaire“, Journal des sciences militaires, Vol. IX, 1883) zu beachten, bei dem die Sicherheit *alleine* im Schlüssel eines Kryptosystems liegt, nicht in dessen Algorithmus.
[18] CVE 2017-5753, CVE 2017-5715
[19] CVE 2017-5754
[20] Auch als „Killswitch“ bezeichnet.
[21] Vgl. bspw. John Adams und Paulette Kurzer, „Remaking American Security: Supply Chain Vulnerabilities and National Security Risks Across the US Defense Industrial Base“, Alliance for American Manufacturing, 2013.
[22] Vgl. SolarWinds Security Advisory und bspw. Eike Kühl, „Ein Hackerangriff, der um die Welt geht“, Spektrum, 2021.
[23] Vgl. das Konzept der glaubhaften Abstreitbarkeit (Plausible Deniability, vgl. z.B. Church Committee Report).
[24] Actel/Microsemi ProASIC3 FPGA, vgl. Sergei Skorobogatov und Christopher Woods, „Breakthrough Silicon Scanning Discovers Backdoor in Military Chip“, LNCS Volume 7428, Springer, 2012.
[25] Vgl. Jordan Robertson und Michael Riley, „The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies“, Bloomberg Businessweek, 2018.
[26] Vgl. bspw. Theo Markettos, „Making sense of the Supermicro motherboard attack“, Security Group, Computer Laboratory University of Cambridge, 2018.

Beispiele hochwertiger Manipulationen vor[27].

Im Rahmen der Snowden-Dokumente[28] wurden weiterhin die sog. „Interdiction Operations“ der NSA bekannt, bei denen bspw. Hardwareimplantate zur Bereitstellung von mit konventionellen Sicherheitslösungen nicht detektierbaren, persistenten Hintertüren während des Versandwegs eingebracht wurden[29]. Beachtet werden muss, dass die Hürde für Angreifer zur Durchführung entsprechender Manipulationen stetig sinkt, bspw. sind bereits Kurse zur Herstellung von Hardware-Implantaten verfügbar[30], die einem versierten Hacker das notwendige Wissen als auch die praktischen Fähigkeiten vermitteln.

In der Praxis kann die Detektion entsprechend hochwertiger Angriffe auf bspw. Versorgungsketten äußerst komplex und nahezu unmöglich, oder wie im Falle SolarWinds Orion, spät und zufallsbehaftet sein; insbesondere ist derzeit sowie absehbar regelmäßig keine annähernd lückenlose Kontrolle möglich. Entsprechend greift die SWP-Studie „Militärische Cyber-Operationen“[31] durch die Fokussierung auf 0day-Schwachstellen und die Nichtberücksichtigung der wichtigen und hoch praxisrelevanten Angriffe der Ebene III - *Einbringen neuer Schwachstellen* - deutlich zu kurz.

Die Nutzung unbekannter 0day-Schwachstellen ist, im Gegensatz zur Folgerung der SWP-Studie, lediglich im mittleren Bedrohungsniveau einzuordnen, während die „Königsdisziplin“ die *bewusste Einbringung* von Schwachstellen darstellt. Auch ist der Rahmen möglicher Akteure weiter zu spannen. So ist die Suche nach 0days durch die bereits erwähnten Fuzzingtechnologien zunehmend einfach, weiterhin ist der Erwerb von 0day-Exploits für alle verbreiteten Zielsysteme und Effektebenen über Firmen wie bspw. ZERODIUM[32] sehr leicht möglich, auch ohne eigene Kapazitäten für technische Untersuchungen zur Verfügung zu haben. Dass auch kleine Nationen 0day-Exploits im staatlichen Rahmen einsetzen, hat bspw. die Entdeckung von mehreren durch den usbekischen Geheimdienst genutzter 0days unterstrichen[33].

Auch wenn es bisher, zumindest öffentlich bekannt, noch zu keinem „Cyber-9/11“ gekommen ist, darf die diesbzgl. vorhandene Gefährdung nicht unterschätzt werden[34]. Ein Blick auf bekannt gewordene Sicherheitsvorfälle zeigt[35], wie insbesondere auch gegen KRITIS zunehmend Cyberangriffe zu registrieren sind. Bekannt geworden sind u.a. Angriffe gegen Stromnetze, Wasserversorgungen und Verkehrsleitsysteme. Insbesondere gilt es zu beachten, dass entsprechende Aktionen oftmals nicht darauf angelegt sind, unmittelbar (umfassende) Effekte zu generieren, sondern vielmehr die Vorbereitung für einen späteren Zugriff sind[36] oder neue Angriffstechniken erproben.

[27] Vgl. bspw. die Beeinflussung und Standardisierung der Dual Elliptic Curve (Dual EC) durch die NSA. Daniel J. Bernstein, „Dual EC: A Standardized Back Door“, Springer LNCS Volume 9100, 2016.
[28] Vgl. bspw. Jacob Appelbaum et al., „Die NSA rüstet zum Cyber-Feldzug“, Spiegel Netzwelt, 2015.
[29] Vgl. bspw. GODSURGE-Tool und FLUXBABBITT Hardware-Implant für DELL Power Edge 1950 und 2950 Server, welches über das Joint Test Action Group (JTAG) Debugging-Interface auf das Zielsystem zugreift.
[30] Vgl. bspw. Joe FitzPatrick, „Applied Physical Attacks 4: Hardware Implants“, Hardware Security Resources, LLC.
[31] Matthias Schulze, „Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland“, SWP-Studie 2020/S, 2020.
[32] Vgl. ZERODIUM
[33] Vgl. Jürgen Schmidt, „l+f: Die freigiebige Zero-Day-Spender-Box“, Heise Medien GmbH & Co. KG, 2019.
[34] Vgl. bspw. Thomas M. Chen, „Cyberterrorism after Stuxnet“, Strategic Studies Institute U.S. Army War College, 2014.
[35] Vgl. bspw. Center for Strategic and International Studies (CSIS), „Significant Cyber Incidents“.
[36] „Preparation of the Battlefield“, vgl. bspw. Robert Koch und Mario Golling, „The Cyber Decade: Cyber Defence at a X-ing Point“, 10th International Conference on Cyber Conflict (CyCon), IEEE, 2018.

Was sind die Besonderheiten, Vor- und Nachteile von Cyberwirkmitteln?

Um eine Analyse der Möglichkeiten, Vor- und Nachteile von Cyberwirkmitteln zu eröffnen, ist insbesondere eine geeignete Terminologie erforderlich. Während oftmals von „Cyberwaffen“ gesprochen wird, ist die Nutzung dieser Begrifflichkeit nicht zielführend. Vielmehr gilt es, eine grundlegende Unterscheidung zwischen *Schadsoftware* und *Cyberwirkmitteln* vorzunehmen, um die Charakteristika und Einsatzmöglichkeiten zu beleuchten. Cyberwirkmittel sind, im Gegensatz zu Schadsoftware, regelmäßig auf konkrete Ziele zugeschnitten und präzise. Weiterhin sind Cyberwirkmittel in der Regel nicht letal und reversibel.

Vorteile von Cyberwirkmitteln Cyberwirkmittel können auf konkrete Ziele, bspw. eine militärisch relevante Komponente in einem Stromnetz, zugeschnitten werden. Dabei können im Unterschied zu anderen Wirkmöglichkeiten insbesondere temporäre, reversible Effekte generiert werden, was bei einer Erbringung in einer anderen Dimension, bspw. bei einer Zielbekämpfung mit Luft-Boden-Raketen, typischerweise nicht möglich ist. Der Wurm Stuxnet hat demonstriert, dass ein zielgerichteter Angriff auf ein spezifisches System möglich ist. Auch wenn im Verlauf der Operation eine weitere Verbreitung des Wurms in Systemen weltweit erfolgt ist, kam es durch das extakte Zuschneiden von Stuxnet auf das Zielsystem, die iranische Urananreicherungsanlage in Natanz, zu keinem dokumentierten, unbeabsichtigen ähnlichen Effekt. Im Gegenteil, die Verbreitung hat demonstriert, dass weder eine unbeabsichtigte Zerstörung eines Nicht-Ziels durch das Cyberwirkmittel erfolgt ist, ein Kollateralschaden also vermieden werden konnte, weiterhin hatte sich die nach Bekanntwerden der Verbreitung des Wurms in der Presse diskutierte Befürchtung, Cyberterroristen könnten auf Basis des Wurmcodes Angriffe gegen Systeme der KRITIS fahren[37], auch bis jetzt nicht bestätigt. Dies liegt auch an den für die Entwicklung des Cyberwirkmittels erforderlichen Informationen über Zielsysteme wie im Beispiel die Zentrifugensteuerung der Anlage in Natanz, welche oftmals nicht allein über den Cyberraum generiert werden können. Dadurch kann aber nicht ausgeschlossen werden, dass es zukünftig nicht zu solchen terroristischen Angriffen kommen kann.

Cyberwirkmittel können Effekte rein auf IT-Systeme beschränkt, aber auch physische Auswirkungen generieren. Auch wenn der tatsächlich genutzte Angriffsvektor im Rahmen der Operation „Outside the Box“[38] der Israelischen Luftwaffe gegen einen im Bau befindlichen, syrischen Reaktor am 5. und 6. September 2007 nicht mit letzter Sicherheit bestimmt werden kann[39], ist Tatsache, dass die syrischen Radaranlagen die israelischen F-15I und F-16I nicht detektieren bzw. darstellen konnten. Wahrscheinlich ist ein Angriff im elektromagnetischen Spektrum, welcher ein falsches Bild der Luftlage in die syrischen Systeme eingespielt hat[40], ggf. auch die Ausnutzung einer Hintertür in den syrischen Radarsystemen[41].

[37] Vgl. bspw. Thomas M. Chen, ebd.
[38] Auch bekannt unter dem Namen „Operation Orchard“. Eine öffentliche Stellungnahme und ein Bekennen zur Durchführung der Operation erfolgte durch Israel erstmals am 21. März 2018, vgl. z.B. Barbara Opall-Rome, „Declassified: How an Israeli operation derailed Syria’s nuclear weapons drive“, DefenseNews, 2018.
[39] Vgl. bspw. Sally Adee, „The Hunt for the Kill Switch“, IEEE Spectrum, 2008.
[40] Vgl. bspw. David A. Fulghum et al., „Black Surprises“, Aviation Week and Space Technology.
[41] Vgl. bspw. Security Alliance, „Spies in the Middle East: Israeli Cyber Operations“, 2018.

Gerade die Komplexität militärischer Systeme und deren Abhängigkeit von IT eröffnen hier zahlreiche Handlungsoptionen und machen den Schutz eigener System sehr herausfordernd[42]. Der Wurm Stuxnet wiederum hat gezeigt, wie physische Auswirkungen durch Cyberwirkmittel generiert werden können.

Nachteile von Cyberwirkmitteln Nachteil eines Cyberwirkmittels können der Pflegeaufwand sein, wenn bspw. zu nutzende Schwachstellen aktualisiert werden müssen. Dabei muss jedoch berücksichtigt werden, dass auch im konventionellen Vergleich entsprechende Aufwände vorhanden sind. So sind bei seegehenden Einheiten bspw. entsprechend regelmäßig Konservierungsmaßnahmen zur Erhaltung der vollen Funktionsfähigkeit des Materials erforderlich, wie zum Beispiel die Erneuerung des Anstrichs insbesondere auch im Unterwasserbereich. Die Pflege eines Cyberwirkmittels differiert in der Praxis daher nicht zu sehr von den Notwendigkeiten klassischer Systeme, wenn diese auch in anderer, mitunter aber sogar einfacher durchzuführender Form, erbracht werden muss.

Für das Zuschneiden auf ein Ziel ist weiterhin eine entsprechende Aufklärung im Vorfeld erforderlich, was sich somit aber nicht elementar von den klassischen Dimensionen unterscheidet. Für die zielgerichtete Nutzung eines Cyberwirkmittels ist jedoch typischerweise eine entsprechende Vorbereitungszeit zur Entwicklung und Überprüfung des Wirkmittels erforderlich.

Weitere Charakteristika Cyberwirkmittel können ggf. „Einmalwaffen“ darstellen, da mit deren Nutzung, insbesondere bei der Generierung physischer Effekte, eine entsprechende Detektionswahrscheinlichkeit verbunden ist, was folglich zu einer Schließung der ausgenutzten Schwachstelle oder zumindest einer entsprechenden Mitigation führen kann. Auch hier besteht jedoch kein elementarer Unterschied zu klassischen Waffensystemen, bspw. stellt der Einsatz eines Flugkörpers eine äquivalente Situation einer „Einmalwaffe“, bezogen auf das jeweilige Einzelexemplar, dar; bzgl. Entwicklung und Pflege kann das Cyberwirkmittel dabei aber ggf. günstiger sein. Vielmehr gilt, dass die tatsächliche Nutzungsdauer des Cyberwirkmittels in der Praxis insbesondere von der Art des ausgelösten Effekts, der regulären Entdeckungswahrscheinlichkeit der Schwachstelle[43] sowie der Geheimhaltungsfähigkeit der Operationsdurchführung abhängig ist. So lief der Cyberangriff mittels des Wurms Stuxnet für mindestens ein Jahr unentdeckt, *obwohl* die generierten Effekte physischer Natur waren[44].

Bzgl. einer öfters diskutierten Gefahr einer schnellen Eskalation bei Cyberangriffen sind bisher kaum systematische Untersuchungen verfügbar. Ein Arbeitspapier der SWP vom Dezember 2020 kommt jedoch, auch wenn noch weiterer Forschungsbedarf gesehen wird, zum Ergebnis dass Cyberangriffe *nicht* von selbst eskalieren und in der Regel mit Cyberangriffen von ungefähr gleicher Intensität beantwortet werden[45].

[42] Vgl. bspw. Robert Koch und Mario Golling, „Weapons Systems and Cyber Security - A Challenging Union“, 8th International Conference on Cyber Conflict (CyCon), IEEE, 2016.

[43] Vgl. bspw. Lillian Ablon und Andy Bogart, „Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits“, RAND Corporation, 2017.

[44] Dies ist insbesondere darin begründet, dass die angegriffenen Zentrifugen des Typs IR-1 per se erhöhte Ausfallraten hatten und der Anstieg daher zunächst keinen Verdacht erweckt hat. Weiterhin hat Stuxnet zunächst Manipulationen in der Drucksteuerung vorgenommen, um das Anreicherungsprodukt unnutzbar zu machen; erst eine spätere Version hat auf die Umdrehungsgeschwindigkeit der Zentrifugen eingewirkt und somit zur physischen Zerstörung geführt; vgl. bspw. Ralph Langner, „Stuxnet und die Folgen“, 2017.

[45] Matthias Schulze, Josephine Kerscher und Paul Bochtler, „Cyber Escalation. The conflict dyad USA/Iran as a test case“, SWP-WP Nr. 01, 2020.

Was sind die Möglichkeiten und Grenzen der Attribuierung und Beweisführung?

Aufgrund seiner Struktur bietet der Cyber- und Informationsraum versierten Angreifern hinreichende Möglichkeiten, ihre Identität zu verschleiern und anonym zu agieren. Eine Attribuierung von Angriffen kann für die Einschätzung der Sicherheitslage von hoher Bedeutung sein. Unterschieden werden kann die faktische Zuordnung, rechtliche Zurechnung sowie die politische Verantwortlichkeit[46]. Die faktische Attribuierung basiert auf einer technischen Analyse des Angriffs mit dem Ziel der Zuordnung zu einem IT-System und darauf aufbauend, weiter zu einem Angreifer. Die rechtliche Attribuierung dient der Feststellung der völkerrechtlichen Verantwortlichkeit eines Staates. Da beide, faktische wie rechtliche Attribuierung in der Praxis regelmäßig längere Zeit in Anspruch nehmen können, dient die politische Attribuierung als Grundlage für Maßnahmen, welche keiner rechtlichen Zurechnung bedürfen[47].

Anonymisierungsnetze Mit Blick auf die technische Analyse bieten sich einem Angreifer zahlreiche Möglichkeiten, die eigene Identität zu verschleiern. Neben dem Legen falscher Spuren bspw. durch Anmerkungen im Programmcode in einer bestimmten Sprache[48], um bspw. im Rahmen einer Analyse von Schadcode abzulenken, können insbesondere technische Verfahren zur Anonymisierung genutzt werden. Bspw. ermöglicht das Tor-Netz[49] eine Anonymisierung der IP-Adresse, so dass eine Rückverfolgung nicht beim eigentlichen Nutzer, sondern bei einem der Ausgangsknoten[50] des Tor-Netzes endet. Solche Ausgangsknoten werden weltweit zur Verfügung gestellt, in Deutschland bspw. durch den Chaos Computer Club[51]. Während Proxy-Ketten[52] lediglich die Rückverfolgung erschweren, grundsätzlich aber nur eine Pseudonymisierung liefern können, ermöglicht das Tor-Netz eine *echte* Anonymisierung. Hierbei muss jedoch beachtet werden, dass das Tor-Netz unter permanenter Beobachtung zahlreicher Behörden, Organisationen sowie der Forschung steht, welche bspw. auch Ausgangsknoten betreiben, den darüber laufenden Datenverkehr untersuchen und Sicherheitsanalysen des Netzes vornehmen.

De-Anonymisierung Grundsätzlich ist eine De-Anonymisierung bspw. aufgrund von Programmierfehlern der Tor-Software bzw. Designfehlern im Tor-Protokoll möglich, jedoch selten[53]. Eher anzutreffen ist eine De-Anonymisierung auf Basis von Fehlern im Tor-Browser[54], welcher letztendlich ein für den Zugriff auf das Tor-Netz erweiterter und konfigurierter Firefox-Browser ist, oder auf entsprechende Browser-Plugins[55]. Die häufigste Ursache für De-Anonymisierung ist jedoch fehlerhaftes Nutzerverhalten, bspw.

[46] Vgl. bspw. Katharina Ziolkowski, „Attribution von Cyber-Angriffen“, GSZ Zeitschrift für das Gesamte Sicherheitsrecht, 2. Jahrgang, 2/2019.
[47] Vgl. ebd.
[48] Vgl. insb. das „Anti-Forensic Marble Framework“ der CIA zur Verschleierung und Förderung einer Fehlattribuierung.
[49] The Onion Router
[50] Tor Exit Nodes
[51] Vgl. Anonymizer des Chaos Computer Club e.V.
[52] Leiten des Datenverkehrs über mehrere Proxy-Rechner im Internet, um die Rückverfolgung zu erschweren.
[53] Vgl. bspw. Tor Blog, „Tor security advisory: "relay early" traffic confirmation attack“, 2014.
[54] Defend yourself. Download-Seite des Tor-Browsers.
[55] Vgl. bspw. Pierluigi Paganini, „NIT code was used by the FBI to deanonymize Tor users“, Security Affairs, 2015.

die Verwendung einer Email-Adresse sowohl mittels des Klarnetzes, als auch im Rahmen von Tor[56].

Die Kombination von wenn auch schwierigen De-Anonymisierungsmöglichkeiten[57], einer intensiven Überwachung des Tor-Netzes sowie technischen Restriktionen durch die Architektur des Netzes selbst[58], schränken den Anwendungsbereich für hochwertige Angriffe in der Praxis ein[59]. Aufgrund dieser Restriktionen findet sich in der Praxis insbesondere auch die Nutzung von ungenügend gesicherten Routern zur Verschleierung der Herkunft, wie bspw. in geleakten Unterlagen des kanadischen CSEC[60] ersichtlich[61]. Der „Home Router Security Report“[62] des Fraunhofer FKIE[63] vom Juni 2020 zeigt die weiterhin sehr hohe Anfälligkeit des IT-Equipments in diesem Bereich und beschreibt ein hohes Gefährdungspotential.

Für die Attribuierung bedeutet diese herausfordernde Situation insbesondere, dass um die notwendige Höhe der Attribuierung zu erreichen und die dafür erforderliche Zeit zu minimieren, ein gesamtstaatlicher Ansatz, welcher die respektiven Informationen aller sicherheitsrelevanten Behörden zusammenführt, erforderlich ist. Hier kann bspw. das Cyber-AZ, welches die zentrale Kooperationsplattform aller entspechender Behörden ist[64], eine besondere Rolle einnehmen.

Was sind Maßnahmen und Grenzen zur Verbesserung des Schutzes eigener Systeme?

Schon der Schutz gegen Angriffsvektoren der unteren Ebene ist in der Praxis oftmals nur eingeschränkt möglich. Selbst bei Vorhandensein eines Patches kann die flächendeckende Anwendung lange Zeit in Anspruch nehmen und bei Endanwendern mitunter nicht erzwungen werden[65], sich die Installation herausfordernd darstellen, bspw. durch die Notwendigkeit der Rezertifizierung im Bereich der Luftfahrt und bei medizinischem Gerät, oder durch 24/7-Betrieb und seltene Wartungsfenster, bspw. im Bereich der Stromversorgung, deutlich verzögern. In solchen Bereichen sind oftmals weiterhin harte Echtzeitanforderungen an die Kommunikationssysteme gestellt[66], welche durch einen Patch nicht negativ beeinflusst werden dürfen. Auch ist zu berücksichtigen, dass die Patchqualität nicht immer genügend ist, Schwachstellen nicht notwendigerweise vollständig geschlossen werden, Systemfunktionalitäten negativ beeinflusst oder gar neue Schwachstellen geöffnet werden können.

[56] Vgl. bspw. Dave Lee, „Silk Road: How FBI closed in on suspect Ross Ulbricht“, BBC News, 2013.
[57] Die NSA scheint daher bspw. den Weg zu präferieren, schon den Download des Tor-Browers oder der Anonymisierungs-Distribution TAILS mittels XKeyscore zu registrieren, vgl. bspw. Lena Kampf, Jacob Appelbaum und John Goetz, „Von der NSA als Extremist gebrandmarkt“, Tagesschau, 2014.
[58] Vgl. bspw. Robert Koch et al., „How anonymous is the tor network? A long-term black-box investigation“, Computer Volume 49, Issue 3, 2016.
[59] Vgl. bspw. Robert Koch, „Hidden in the Shadow: The Dark Web-A Growing Risk for Military Operations?“, 11th International Conference on Cyber Conflict (CyCon), IEEE, 2019.
[60] Communications Security Establishment Canada, kanadischer Nachrichtendienst und Kryptographie-Behörde.
[61] LANDMARK-Program, Nutzung einer sog. Operational Relay Box (ORB)-Infrastruktur für ein zusätzliches Level der Nicht-Attribuierbarkeit.
[62] Vgl. Peter Weidenbach und Johannes vom Dorp, „Home Router Security Report 2020“, Fraunhofer FKIE, 2020.
[63] Fraunhofer FKIE
[64] Vgl. bspw. Webseite des BSI, „Das Nationale Cyber-Abwehrzentrum“.
[65] Vgl. Gerald Spindler, „Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären“, Studie im Auftrag des BSI, Stand 2020.
[66] Vgl. bspw. Norm IEC 61850 (International Electrotechnical Commission) im Bereich Automatisierung von Schaltanlagen.

Die öfters zu findende Forderung, Schwachstellen generell zu veröffentlichen, um sie mittels von den jeweiligen Herstellern bereitgestellter Patche zu schließen, greift daher zu kurz und vernachlässigt die Komplexität der realen IT-Landschaft. Vielmehr ist ein Prozess erforderlich, der alle Aspekte bzgl. einer Schwachstelle, deren Verbreitung und Gefährlichkeit, den Möglichkeiten der Schließung und den Vor- und Nachteilen einer Veröffentlichung bzw. Geheimhaltung mit einbezieht[67].

Ist keine direkte Schließung einer Schwachstelle möglich, wird eine Mitigation durch andere Maßnahmen erforderlich, welche typischerweise Nachteile beinhalten. So kann sich die Einbringung einer zusätzlichen Firewall oder eines Systems zur Einbruchserkennung[68] mit Sperrregeln gegen maliziösen Verkehr negativ auf die Echtzeitfähigkeit des Netzes auswirken und auch durch die Einbringung von Schutzsystemen kann sich die Angriffsoberfläche erhöhen und im Extremfall somit in einer weiteren *Schwächung* des zu schützenden Systems resultieren. Bspw. hat Tavis Ormandy wiederholt demonstriert, wie z.B. Architektur- und Programmierfehler oder veraltete Bibliotheken von Antivirensoftware bis zur entfernten Übernahme mit administrativen Rechten von eigentlich durch die Software zu schützenden Systemen führen können[69]. Die Nutzung nicht-intrusiver Verfahren wie bspw. eine Angriffserkennung auf Basis der Auswertung des Stromverbrauchs des Systems[70] kann insbesondere im Bereich KRITIS eine Möglichkeit zur Verbesserung des Schutzniveaus auch für Bestandssysteme darstellen, wobei zu beachten ist, dass bei nicht-intrusiver Umsetzung zunächst auch keine direkte automatisierte Reaktion auf einen Angriff erfolgen kann.

Maßnahmen auf Softwareebene Neben der Implementierung geeigneter Schutzsysteme gilt es daher insbesonders, die Systembasis zu härten. Bei geeigneter Nutzung von Open Source können hierbei positive Effekte erzielt werden. Für sicherheitskritische Systeme, insbesondere im Bereich von KRITIS und Steuerungssystemen, ist die Nutzung von Mikrokernen wie bspw. der L4-Mikrokernel-Familie[71] von grundlegender Bedeutung zur Minimierung der Angriffsoberfläche. Die Möglichkeiten, die Hürde für Angreifer durch die Nutzung formaler Methoden wie beim mathematisch verifizierten Mikrokern seL4 deutlich zu erhöhen, wurden durch das HACMS-Programm[72] der DARPA[73] eindrucksvoll demonstriert[74]. Insbesondere hat das Programm gezeigt, dass sich auch Bestandssysteme härten lassen; die Komplexität des zu betrachtenden Systems und entsprechende Grenzen müssen hierbei natürlich berücksichtigt werden.

Maßnahmen auf Hardwareebene Manipulationen auf Hardwareebene zeichnen sich durch eine besonders herausfordernde Detektierbarkeit aus. Zwar entwickelt sich auch dieser Bereich und Detektionsmöglichkeiten werden zunehmend erforscht und (weiter-)entwickelt, unterliegen in der Praxis aber immer noch umfassenden Restriktionen[75]. Entsprechend sind eigene Kapazitäten im Bereich der Hardwareproduktion wünschenswert. Während in einigen Spezialbereichen wie bspw. TPM-Chips[76] deutsche Unternehmen

[67] Vgl. bspw. „Vulnerabilities Equities Policy and Process for the United States Government“, 2017.
[68] Intrusion Detection System, IDS
[69] Vgl. z.B. Tavis Ormandy, „How to Compromise the Enterprise Endpoint“, Google Project Zero, 2016.
[70] Vgl. bspw. Robert und Teo Kühn, „Defending the Grid: Backfitting Non-Expandable Control Systems“, 9th International Conference on Cyber Conflict (CyCon), IEEE, 2017.
[71] Vgl. bspw. Operating Systems Group, „The L4 µ-Kernel Family“, Technische Universität Dresden, 2015.
[72] Vgl. Raymond Richards, „High-Assurance Cyber Military Systems (HACMS)“, DARPA.
[73] Defense Advanced Research Projects Agency
[74] Vgl. bspw. Kathleen Fisher et al., „The HACMS program: using formal methods to eliminate exploitable bugs“, Philosophical Transactions, Series A, Mathematical, Physical, and Engineering Sciences Vol. 375,2104, 2017.
[75] Vgl. bspw. Sam Thomas, Aurélien Francillon, „Backdoors: Definition, Deniability and Detection“, Proceedings of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2018.
[76] Trusted Platform Module

führend sind, besteht eine hohe Abhängigkeit im Bereich von General-Purpose Hardware.

Der Aufbau umfassend eigener, autarker Kapazitäten ist aufgrund des erforderlichen Know-Hows, insbesondere aber auch aus Kostengründen kaum möglich. Selbst groß angelegte Programme wie das „Trusted Foundry Program“ des United States Department of Defense stoßen dabei immer wieder an Grenzen[77]. Entsprechend ist im Bereich der Hardware eine Fokussierung auf Systemanteile erforderlich, welche zum einen eine hohe Relevanz für die Sicherheit des Gesamtsystems haben, zum anderen aber realistisch erreichbar sind. Gerade im Bereich von hochsicheren und Steuerungssystemen offerieren sich diesbzgl. Möglichkeiten, da entsprechende Systemkomponeten typischerweise weniger komplex sind und oftmals keine „High-End“ Performance abbilden müssen. Entsprechend können Open Source Prozessordesigns wie der RISC-V[78] Basis für ein hochsicheres, in eigenen Produktionskapazitäten gefertigtes System sein. Der MiG-V[79] ist Beispiel eines RISC-V basierten Prozessors Made in Germany, welcher zusammen mit dem verifizierten Mikrokern seL4 eingesetzt und somit die Basis für ein hochsicheres System liefern kann[80].

Neue Technologien Mit der exponentiellen technologischen Entwicklung eröffnen sich vielversprechende Möglichkeiten zur Erhöhung der Cybersicherheit. Bekannte Beispiele sind abhörsichere Kommunikationsverbindungen auf Basis von Quantenschlüsselaustausch[81] oder selbstheilende Systeme, welche Angriffe automatisch erkennen und analysieren können, Patche für die entsprechenden Schwachstellen entwickeln und diese ebenfalls automatisch anwenden. Das Finale der „Cyber Grand Challenge“ der DARPA im Jahre 2016[82] hat eindrucksvoll demonstriert, welches Potential in diesem Forschungsgebiet liegt.

Beachtet werden muss jedoch, dass auch bei Systemen mit in der Theorie perfekter Sicherheit wie bspw. im Bereich des Quantenschlüsselaustauschs, in der Praxis immer Angriffsvektoren durch die physikalische Implementierung verbleiben, bspw. durch Seitenkanalangriffe aber insbesondere durch Angriffe der oberen Ebene - dem bewussten Einbringen von Schwachstellen durch einen hochwertigen Angreifer. So kann bspw. die tatsächliche Sicherheit eines Quantenschlüsselaustauschs von der Qualität der zugrundliegenden Zufallszahlen abhängen[83] - diese sind in der Praxis per se schwierig zu erzeugen, schwer erkennbare Angriffe können die Sicherheit des betroffenen Systems nachhaltig schwächen[84].

Möglichkeiten und Grenzen der Resilienz Mit Blick auf die heutige Systemlandschaft kann deren Resilienz insbesondere auch im Bereich KRITIS durch bspw. die genannten Technologien noch erheblich gesteigert werden. Eine 24/7-Überwachung von Netzen und Systemen, ausreichende Kapazitäten im Bereich Incident Response und IT-Forensik sowie Investitionen im Bereich Cyber-Awareness sind essentiell, Maßnahmen zur Erhöhung der Digitalen Souveränität sind in diesem Kontext besonders zu begrüßen.

[77] Vgl. bspw. Mark Lapedus „A Crisis In DoD's Trusted Foundry Program?“, Semiconductor Engineering, 2018.
[78] Vgl. RISC-V International, „RISC-V: The Free and Open RISC Instruction Set Architecture“.
[79] Made in Germany RISC-V, „MiG-V“, HENSOLDT Cyber GmbH.
[80] Vgl. bspw. Andrea Letzner, „MiG-V: First RISC-V Made in Germany with HW Security Features“, Blog der RWTH Aachen, 2020.
[81] Quantum Key Distribution, QKD. Vgl. bspw. Quantiki, „BB84 and Ekert91 protocols“, 2015.
[82] Vgl. Dustin Fraze, „Cyber Grand Challenge (CGC) (Archived)“, DARPA.
[83] Vgl. bspw. Hong-Wei Li et al., „Randomness determines practical security of BB84 quantum key distribution“, Scientific Reports 5, 16200, 2015.
[84] Vgl. bspw. Georg T. Becker et al., „Stealthy Dopant-Level Hardware Trojans“, International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2013.

Beachtet werden muss jedoch, dass sich die Situation unsicherer Systeme nicht einfach und schnell ändern lässt, sondern es selbst unter *optimalen* Bedingungen viele Jahre dauern kann, bis eine spürbare und effektive Härtung des Gesamtsystems erreicht wird. Die lange Nutzungsdauer des Mobilfunkstandards GSM und dessen Verfügbarkeit auch noch in modernen Netzen, oder die lange Transition vom Internet Protokoll (IP) Version 4[85] zur Version 6[86] mit Parallelnutzung beider Varianten und daraus resultierender Sicherheitsimplikationen sind Beispiele für die praktischen Herausforderungen bei der Weiterentwicklung komplexer Netze und Systeme. Auch gilt, dass grundsätzliche Architektureigenschaften des Internets, welche für einen zuverlässigen Betrieb erforderlich sind, auch künftig ausgeklügelte Angriffe erlauben werden; RFCs[87] und darauf basierende Standardisierungen ermöglichen oftmals einen gewissen Interpretationsspielraum[88], welcher bewusst vorhanden ist, um die Kompatibilität und Interoperabilität der Implementierungen verschiedener Hersteller zu unterstützen. Ein solcher Interpretationsspielraum resultiert bspw. in unterschiedlichen initialen Werten für die „Lebenszeit“[89] eines IP-Pakets. Da diese somit vom Hersteller bzw. System abhängen kann, kann dies bspw. zur Erkennung eines eingesetzten Betriebssystems bei einem Netzscan herangezogen werden[90]. Die vorhandenen Freiheitsgrade lassen sich aber bspw. auch für die Implementierung von schwer detektierbaren Seitenkanälen nutzen[91], auch auf unteren Schichten des ISO/OSI-Referenzmodells.

Die Aktivitäten zahlreicher professioneller Angreifergruppen[92] werden absehbar nicht verschwinden. Dazu kommen die latente Gefährdung durch bereits in Systeme eingebrachte Hintertüren sowie Angriffe der oberen Bedrohungsebene, nicht komplett vermeidbare Implementierungsfehler, unerwartete Seiteneffekte oder neue Technologiesprünge, welche Handlungsmöglichkeiten auch für Angreifer eröffnen. Neue Schutzverfahren ziehen neue Angriffsverfahren nach sich, neue Technologien und Erkenntnisse eröffnen neue Schwachstellen.

Die Erhöhung der Systemresilienz ist unter dem Einfluss der zahlreichen realen Bedrohungsvektoren die absolut notwendige Grundlage, aber auch absehbar nicht ausreichend. Dies erfordert das Vorhalten offensiver Fähigkeiten, um bspw. bei der Entwicklung einer Cyberkrise handlungsfähig zu sein und zu bleiben. Insbesondere auch im militärischen Bereich muss jederzeit mit Cyber-Hochwertfähigkeiten von Akteuren gerechnet werden, was die Verfügbarkeit offensiver Cyberkapazitäten zwingend für den sicheren Betrieb, als auch für die Durchsetzungsfähigkeit macht.

[85] Internet Protocol, RFC 791
[86] Internet Protocol, Version 6 (IPv6), RFC 2460 (obsolete), RFC 8200
[87] Requests for Comments sind Veröffentlichungen der Internet Society und zugehöriger Gruppen wie bspw. der Internet Engineering Task Force (IETF), welche für die (Weiter-) Entwicklung von Internetstandards verantwortlich ist.
[88] Vgl. insb. RFC 2119, „Key words for use in RFCs to Indicate Requirement Levels“.
[89] TTL, Time-to-Live
[90] Vgl. RFC 793, RFC 1122, Sektion 3.2.1.7 und RFC 1700. Der derzeitig *empfohlene* Default-Wert beträgt 64.
[91] Covert Channels. Vgl. bspw. R.P Murphy, „IPv6/ICMPv6 Covert Channels“, 2006.
[92] Vgl. bspw. Google Docs, „APT Groups and Operations“.

Stellungnahme von Thomas Reinhold[1], TU Darmstadt, zur öffentlichen Anhörung am 14.12.2020 im Verteidigungsausschuss des deutschen Bundestages zum Thema:

„Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen“

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)936
03.12.2020 - 19/3482
5410

Vorbemerkung zur Stellungnahme: Der Autor ist weder Völkerrechtler noch Jurist, sondern Informatiker sowie Friedens- und Sicherheitsforscher. Schlussfolgerungen zu rechtlichen Fragen werden vor allem auf Basis der technischen Grundlagen und Zusammenhänge in Bezug auf die Fragestellung sowie damit verbundener Belange gezogen.

[1] Webseite und Profil auf cyber-peace.org --- https://peasec.de/team/reinhold --- @CyberPeace1

Aus Sicht der Friedens- und Konfliktforschung ist die zunehmende Militarisierung des Cyberraums mit großer Sorge zu bewerten. Diese betrifft insbesondere folgende Problematiken, die nachfolgend näher erläutert werden:

1. Nachrichtendienstliche und militärische Aktivitäten in IT-Systemen gefährden die globale IT-Sicherheit.
2. Bereits Aufklärungsaktivitäten im Cyberraum können aufgrund der notwendigen Manipulationen an IT-Systemen dem Verbot friedensstörender Handlungen nach Art. 26 Abs. 1 GG entgegenstehen.
3. Entwicklung und Einsatz offensiv wirksamer Cyber-Hilfsmittel fördern den globalen Markt für Sicherheitslücken und unterbinden die Beseitigung von Verwundbarkeiten großflächig eingesetzter ziviler IT-Produkte.
4. Die Zunahme nachrichtendienstlicher und militärischer Aktivitäten unterhalb der Schwelle offener militärischer Konflikte erhöht das Eskalationspotential.
5. Fehlende internationale Vereinbarungen über Grenzen nachrichtendienstlicher und militärischer Aktivitäten in IT-Systemen steigern das Risiko von Fehlinterpretationen und Fehlreaktionen.
6. Die Priorisierung militärischer Offensiv-Maßnahmen im Cyberraum anstelle einer institutionellen Harmonisierung von IT-Sicherheit verschärft die Ressourcenknappheit bei IT-Fachkräften und technischem Knowhow.
7. Fehlende Maßnahmen der Rüstungskontrolle sowie technische Verfahren zur Stärkung der Vertrauensbildung im Cyberraum erschweren die Eingrenzung von Rüstungswettläufen im Cyberraum sowie die Reduktion von Konfliktpotentialen.

Zu 1: Nachrichtendienstliche und militärische Aktivitäten in IT-Systemen gefährden die globale IT-Sicherheit.

Nahezu[2] jegliche nachrichtendienstliche oder militärische Aktivität gegen oder in IT-Systemen erfordert Maßnahmen zur Umgehung von Schutzmaßnahmen, zur Erlangung spezifischer technischer Zugangs- und Ausführungsberechtigungen sowie zum Beseitigen digitaler „Fußspuren“ in den Systemen. Aus der Perspektive der IT-Sicherheit entspricht dies einer Manipulation des Regelverhaltens des betroffenen Systems, genauer einer Verletzung der IT-Schutzziele[3] „Vertraulichkeit” und „Integrität” sowie ggf. auch dessen „Verfügbarkeit”. Manipulierte Systeme können sich unerwartet verhalten, in der Ausführung ihrer Dienste gestört werden oder ausfallen. Dies gilt unabhängig vom eigentlichen Ziel der Cyberoperation bereits für Informationsgewinnungsaktivitäten ebenso wie für offensive Maßnahmen der „aktiven Verteidigung“, „Vorwärtsverteidigung”, „Hack-Backs“[4] oder einem „Persistent Engagement“[5]. Des Weiteren erfordern komplexe Cyberoperationen in aller Regel auch entsprechende manipulierende Aktivitäten gegen unbeteiligte, vorgeschaltete Systeme, um über Netzwerke hinweg Zugriff auf das Zielsystem zu erlangen. Einem IT-System ist weder von außen noch, mit ausreichender Sicherheit, von innen der Zweck und die Aufgaben des Systems sowie die Abhängigkeiten zu anderen IT-Systemen anzusehen. Direkte und indirekte Konsequenzen von Manipulationen sind dadurch kaum sicher abzuschätzen oder einzugrenzen. Damit werden zivile oder unbeteiligte IT-Systeme und die von ihnen ausgeführten Dienste durch Manipulationen in Gefahr gebracht und ggf. schwer kalkulierbare Kettenreaktionen ausgelöst.

Zu 2: Bereits Aufklärungsaktivitäten im Cyberraum können aufgrund der notwendigen Manipulationen an IT-Systemen dem Verbot friedensstörender Handlungen nach Art. 26 Abs. 1 GG entgegenstehen.

---

[2] Ausgenommen sind Zugriffe auf IT-Systeme mit Hilfe gültiger, gestohlener oder anderweitig erlangter Zugangsdaten. Selbst in diesem Fall kann es jedoch erforderlich sein, unerlaubte Zugriffe auf die Systeme durch das digitale „Verwischen von Spuren“ mit entsprechenden Manipulationen zu verbergen.

[3] Zu den drei Grundprinzipien der IT-Sicherheit siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

[4] Eine gesonderte Diskussion der sog. Hack-Backs findet sich unter https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/AP_Schulze_Hackback_08_2017.pdf

[5] Für eine ausführlichere Darstellung dieser, aktuell insbesondere von den USA verfolgten Maßnahme proaktiver Cyberoperationen in IT-Systemen mutmaßlicher Gegner siehe https://cyber-peace.org/2019/06/17/kurz-notiert-usa-weiten-offensive-cyber-operationen-aus-mehr-fruehere-schnellere-reaktion-auf-cyberbedrohungen/

In einem Gutachten des wissenschaftlichen Dienstes des Bundestages von 2018[6] stellt dieser fest, dass sich das Verbot friedensstörender Handlungen nach Art. 26 Abs 1 auch auf Cyber-Aktivitäten staatlicher Institutionen beziehen kann, unabhängig davon welche staatliche Institution diese ausführt. Das Gutachten betont dabei den Zusammenhang zwischen Art. 26 Abs. 1 GG und der Bewertung eines Cyberangriffs im Sinne von Art. 51 der UN-Charta, bei dem Menschen verletzt oder getötet oder erhebliche Sachgüter zerstört werden. Hinsichtlich der Wahrnehmung und Interpretation von Vorfällen im Cyberraum wird darüber hinaus betont, dass die Gefahr von Fehlinterpretationen und damit von ungewollten Eskalationen im Cyberraum erheblich ist.

Mit Blick auf die voran erläuterten technischen Aspekte von nachrichtendienstlichen und militärischen Aktivitäten im Cyberraum muss festgehalten werden, dass eine rein passive Aufklärung kaum möglich ist. Verfahren wie das sog. Port-Scanning[7] oder der Zugriff auf Systeme durch valide, auf anderem Wege erworbene Zugangsdaten[8] bieten zwar nicht-intrusive Möglichkeiten ein IT-System zu untersuchen, allerdings mit geringem nachrichtendienstlichen Erkenntnisgewinn. In aller Regel werden solche Maßnahmen nur als Vorbereitung für einen weitergehenden, manipulationsbehafteten Zugriff auf die Systeme verwendet. Darüber hinaus ermöglichen diese Verfahren jeweils nur den Zugriff auf die äußersten Schichten eines Zielnetzwerkes, während sich Hochwertziele in aller Regel tief in IT-Netzwerken eingebettet befinden, umgeben von anderen IT-Systemen und Schutzmaßnahmen. Ein Zugriff auf diese Hochwertziele ist nur durch ein sukzessives Ausspähen, Unterwandern und Manipulieren vorgeschalteter Systeme möglich. Dies gilt in jedem Fall auch dann, wenn diese Operation „nur" zum Zweck der Analyse und Aufklärung dieser Systeme durchgeführt werden. Es muss daher in aller Deutlichkeit festgestellt werden, dass jegliche Operationen in IT-Systemen, beginnend bei ausschließlichen Aufklärungsaktivitäten diese und angeschlossene IT-Systeme aufgrund der erläuterten technischen Sachverhalte hochgradig gefährden und unbeabsichtigte Schäden an Sachgütern und u.U. Menschenleben zur Konsequenz haben können.

Vor diesem Hintergrund ist auch die im Gutachten betonte Beschränkung der Nachrichtendienste auf Aufklärungsmaßnahmen relevant. Diesen Diensten stehen nach

---

6 https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf

7 Bei einem Port-Scan werden IT-Systeme von außen durch reguläre Anfragen auf Hinweise auf mögliche Sicherheitslücken analysiert, ohne in die Systeme direkt einzudringen. Selbst ein massenhafter Port-Scan kann jedoch ungenügend konfigurierte Schutzmaßnahmen zu einem Fehlverhalten bringen.

8 Vgl. Fußnote 2

Ansicht des wissenschaftlichen Dienstes auf Basis der derzeitigen Rechtslage keine klassischen Eingriffsbefugnisse zu. Wie erläutert, ist eine Aufklärung von IT-Systemen ohne Eingriff nicht sinnvoll umzusetzen. Es ist daher die Schlussfolgerung des Gutachtens, dringend zu betonen, dass „eine Durchführung von Cyberangriffen durch Nachrichtendienste (..) jedenfalls zu einer erheblichen Erweiterung der bisherigen nachrichtendienstlichen Befugnisse führen [würde]"[9].

Zu 3: Entwicklung und Einsatz offensiv wirksamer Cyber-Hilfsmittel[10] fördern den globalen Markt für Sicherheitslücken und unterbinden die Beseitigung von Verwundbarkeiten großflächig eingesetzter ziviler IT-Produkte.

Die Grundlage für Cyberoperationen und die dabei eingesetzten offensiv wirksamen Cyber-Hilfsmittel[11] bilden Zero-Day-Exploits[12] oder allgemein Sicherheitslücken in IT-Produkten, für die es bis dato noch keine Sicherheitsaktualisierung zur Behebung der Verwundbarkeiten gibt. Der steigende Bedarf durch staatliche Stellen für derartige Informationen fördert deren Marktwert und schafft Anreize für Unternehmen zum Aufkauf und Handel mit diesen Informationen. Je tiefgreifender oder weitreichender eine Sicherheitslücke ist, umso höher ist deren Wert und der Anreiz diese Information an Bedarfsträger zu verkaufen. Die Kenntnisse über entsprechende Verwundbarkeiten werden dadurch zurückgehalten, dem Hersteller des betroffenen IT-Produktes nicht gemeldet und folglich nicht geschlossen. Aufgrund des hohen Dual-Use-Charakters von IT-Produkten betreffen Verwundbarkeiten in Produkten, die für Nachrichtendienste und militärische Kräfte interessant sind, damit in aller Regel auch breit eingesetzte zivile IT-Produkte wie Betriebssysteme, Office-Anwendungen oder Smartphone-Programme.. Da ein Zugriff auf ein Zielsystem oft über diverse unterschiedlichste und zumeist

[9] Siehe Fußnote 6

[10] Als "offensiv wirksame Cyber-Hilfsmittel" werden jegliche Formen von fertiger oder spezifisch angefertigter Software sowie Verfahren verstanden, mit deren Hilfe IT-Systeme manipuliert, IT-Schutzmaßnahmen umgangen sowie anderweitig die reguläre Ausführung von Operationen in einem IT-System verändert werden können.

[11] Die Bezeichnung "Cyberwaffe" für derartige Hilfsmittel wird an dieser Stelle nicht verwendet, da es noch keine allgemein anerkannte Definition für den Waffen-Begriff im Kontext schadhafter Hilfsmittel im Cyberraum gibt. In der aktuellen Forschung sowie sicherheitspolitischen Debatten werden als "Cyberwaffen" üblicherweise all jene Hilfsmittel bezeichnet, die im Cyberraum wirken und im Sinne der völkerrechtlichen Perspektive auf bisherige Waffen-Technologien signifikante Schäden an Sachgütern oder der Gesundheit und dem Leben von Menschen verursachen können.

[12] Ein Zero-Day-Exploit (auch als 0-Day-Exploit bezeichnet) ist ein Angriff auf Grundlage einer Sicherheitslücke in einem IT-Produkt, die denjenigen unbekannt ist, die an der Verringerung der Sicherheitsanfälligkeit interessiert sein sollten, wie den Anwendern sowie dem Hersteller des Produktes. Da für eine Zero-Day-Sicherheitslücke noch keine Sicherheitsaktualisierung des Produktes verfügbar ist, kann diese Schwachstelle ungehindert durch jeden ausgenutzt werden, der über diese Information verfügt.

schlechter geschützte „Zwischenstationen" in den Zielnetzwerken realisiert wird, müssen in aller Regel mehrere Schwachstellen und Exploit-Ketten[13] verwendet werden. Derart nichtbehobene Schwachstellen können ebenfalls durch andere staatliche, nicht-staatliche oder kriminelle Akteure entweder entdeckt oder ihrerseits kommerziell erworben und für eigene Zwecke ausgenutzt werden. Dies kann unter Umständen extreme globale wirtschaftliche Schäden verursachen, wie im Falle von NotPetya[14]. Diese Schadsoftware basierte auf einer Sicherheitslücke in Microsoft Windows-Betriebssystemen, die mutmaßlich der US-amerikanischen NSA länger bekannt war und durch diese zurückgehalten wurde. Nach einem Diebstahl der Informationen wurden diese öffentlich bekannt und konnten von den Urhebern von NotPetya ausgenutzt werden[15].

Zu 4: Die Zunahme nachrichtendienstlicher und militärischer Aktivitäten unterhalb der Schwelle offener militärischer Konflikte erhöht das Eskalationspotential.

Die zunehmende Bewertung des Cyberraums als Domäne für nachrichtendienstliche und militärische Aktivitäten – von der Lagebilderstellung bis zur offensiven Cyberoperation – fördert eine Dynamik der globalen Bedrohungswahrnehmung in dieser Domäne, erkennbar an der zunehmenden Einrichtung staatlicher Institutionen zur Cyberverteidigung[16]. Gleichzeitig erfordert die Durchführung offensiver Maßnahmen in dieser Domäne Kenntnisse über Zielsysteme, deren Erreichbarkeit und Schwächen. Derartige Informationen müssen in aller Regel bereits im Vorfeld potentieller Operationen zusammengetragen werden, um im Bedarfsfall geeignete Angaben über mögliche Zugriffspunkte oder sogar bereits vorbereitete Zugangsmöglichkeiten zu relevanten Systemen zu verfügen. Dies gilt umso mehr, wenn die, auch im Rahmen der Bundeswehrfähigkeiten diskutierten offensiven Cyberoperationen schnell und flexibel gegen akute Cyberbedrohungen eingesetzt werden sollen. Offensive Cyberoperationen erhöhen demzufolge den Bedarf an Aufklärungsaktivitäten in Friedenszeiten um Zielinformationen zu sammeln und zeitnah bereitstellen zu können. Wie vorangehend

[13] Siehe Fußnote 12

[14] Details zu NotPetya sowie der zugrunde liegenden Sicherheitslücke „EternalBlue" unter https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/petya_notpetya/

[15] Es ist anzumerken, dass nach dem Diebstahl der Informationen die NSA den Softwarehersteller Microsoft informierte und diese umgehend eine Sicherheitsaktualisierung bereitgestellt haben. Aufgrund des jedoch z.T. recht langsamen "Ausrollens" von Sicherheitsaktualisierungen in Unternehmen und Behörden konnte NotPetya dennoch erhebliche Schäden in ungesicherten und entsprechend verwundbaren Systemen verursachen.

[16] Siehe dazu exemplarisch die Liste der nationalen Cybersicherheits- und Verteidigungsstrategien wie sie durch das NATO Cooperative Cyber Defence Centre of Excellence bereit gestellt wird unter https://ccdcoe.org/library/strategy-and-governance/

erläutert, bergen derartige Aufklärungsaktivitäten dabei stets die Gefahr der unbeabsichtigten Störung von IT-Systemen mit unkalkulierbaren Konsequenzen. Je nach politischer Situation sowie den zwischenstaatlichen Beziehungen könnten solche Störungen durch einen Staat als Angriff auf die eigene staatliche Souveränität bis hin zu einem bewaffneten Angriff interpretiert werden.

Durch derartige Cyber-Aktivitäten verschwimmen zum einen zunehmend die Grenzen zwischenstaatlicher Konflikte. Andererseits verstärkt der Bedarf an Informationen die weitere Verzahnung geheimdienstlicher und militärischer Aktivitäten um bspw. dem für Deutschland geltenden Primat der defensiven Ausrichtung der Bundeswehr Rechnung tragen zu können. Eine solche Zunahme nachrichtendienstlicher Aufgaben muss jedoch durch eine adäquate parlamentarische Kontrolle überwacht und begrenzt werden können.

Zu 5: Fehlende internationale Vereinbarungen über Grenzen nachrichtendienstlicher und militärischer Aktivitäten in IT-Systemen erhöhen das Risiko von Fehlinterpretationen und Fehlreaktionen.

Den beschriebenen Aktivitäten in IT-Systemen durch Nachrichtendienste und militärische Kräfte steht das Fehlen spezifischer und verbindlicher internationaler Übereinkommen gegenüber, die derartige Maßnahmen regulieren oder begrenzen können. Gleichzeitig erhöht die Verfügbarkeit von Maßnahmen zur aktiven Gegenwehr bei Cyberattacken in Verbindung mit einer gebotenen Reaktionsgeschwindigkeit den Handlungsdruck, in Krisensituationen derartige Mittel einzusetzen. Vergangene Vorfälle verdeutlichen jedoch immer wieder das Problem der zuverlässigen Zuordnung des tatsächlichen Ursprungs einer Cyberattacke sowie des dahinterstehenden Angreifers. Neben der Problematik gezielter *False Flag*-Operationen[17] ist eine zuverlässige Attribution insbesondere bei komplexen IT-Angriffen oft nur zeitaufwendig und im mehrmonatigen Rahmen mit Hilfe von IT-Forensik, zum Teil auf Basis internationaler Kooperationen beim Zugriff auf die für den Angriff verwendeten IT-Systeme, umsetzbar. Vorschnelle Schlussfolgerungen bergen eine hohe Gefahr von Fehlinterpretationen und damit von Fehl- oder Überreaktionen, die sich unter Umständen gegen unbeteiligte Dritte richten. Gleichzeitig ist die Bewertung von offensiven Cyberhilfsmitteln als „chirurgische“ Einwirkung empirisch nicht belegbar da eine verlässliche

[17] Als *False Flag*-Operationen werden Cyberangriffe bezeichnet, bei denen der Angreifer durch die Wahl seiner eingesetzten Mittel wie dem Standort von Command & Control-Servern oder der im Code verwendeten Muttersprache gezielt die Aufmerksamkeit auf einen dritten, unbeteiligten Akteur zu lenken versucht.

Wirkungsentfaltung bei aktiven Reaktionen gegen IT-Systeme aufgrund der erläuterten komplexen Abhängigkeiten und Wechselwirkungen in IT-Netzwerken kaum möglich ist.

Zu 6: Die Priorisierung militärischer Offensivmaßnahmen im Cyberraum anstelle einer institutionellen Harmonisierung von IT-Sicherheit verschärft die Ressourcenknappheit bei IT-Fachkräften und technischem Knowhow.

Die Aufklärung und Vorbereitung offensiver Cybermaßnahmen erfordert eine umfangreiche Vorfeldaufklärung, den Zugriff auf vorgeschaltete Systeme sowie gegebenenfalls die Vorinstallation von Hintertüren für eine effektive Aktivierung des Wirkmittels im Bedarfsfall. Solche Vorbereitungen sind nur mit umfangreichem technischem Knowhow und entsprechend hohem Einsatz von IT-Fachkräften umsetzbar. Derartige Maßnahmen wären dementsprechend nur gegen ausgewählte, strategisch relevante potentielle Ziele umsetzbar, während ihr Nutzen und ihre Wirksamkeit – zusätzlich zu den voran erläuterten Problemen und Gefahren – in hohem Maße kritisch bewertet werden muss. Gleichzeitig ist auch die Wirksamkeit von Verteidigungsmaßnahmen auf Basis offensiver Gegenreaktionen im Cyberraum anzuzweifeln. Ein Angreifer, der mit derartigen Gegenmaßnahmen rechnen muss, wird geeignete Redundanzmaßnahmen, auf die gegebenenfalls ausgewichen werden kann, in die Angriffsinfrastruktur einbauen und in seinem taktischen Vorgehen wie beispielsweise durch die Nutzung von IT-Systemen dritter Parteien berücksichtigen. Vor diesem Hintergrund muss auch die Abschreckungswirkung militärischer Offensivfähigkeiten im Cyberraum dahingehend in Frage gestellt werden.

Gleichzeitig wäre angesichts der Breite potentieller staatlicher, nicht-staatlicher und krimineller Angreifer sowie der Heterogenität der deutschen IT-Landschaft der Aufbau umfangreicher Offensivmaßnahmen kein Ersatz für eine weitere Intensivierung defensiver Maßnahmen aus dem Bereich der IT-Sicherheit. Diese sollte primär gefördert und ausschließlich dort, wo sinnvoll durch nachrichtendienstliche und militärische Ressourcen, wie Knowhow oder Bedrohungsanalysen unterstützt werden. Die eigenen nationalen IT-Systeme sind der geeignete Raum zu Gestaltung von IT-Sicherheit. Auch angesichts gegenwärtiger und mittelfristig knapper Ressourcen bei IT-Fachkräften ist die Priorisierung einer defensiven Ausrichtung dringend angeraten, verbunden mit einer Stärkung ziviler IT-Sicherheit wie der Verbesserung der Qualität großflächig eingesetzter kommerzieller IT-Produkte. Die grenzüberschreitende Nachverfolgung und Abwehr von Cyberattacken sollte in internationaler Kooperation erfolgen und dafür die Zusammenarbeit im Rahmen bi- und multilateraler Übereinkommen verbessert und gestärkt werden. Gleichzeitig sollte international das *Due Dilligence*-Prinzip staatlicher

Verantwortungspflicht weiterhin mit Nachdruck betont und Staaten zur Zusammenarbeit motiviert werden.

Zu 7: Fehlende Maßnahmen der Rüstungskontrolle sowie technische Verfahren zur Stärkung der Vertrauensbildung im Cyberraum erschweren die Eingrenzung von Rüstungswettläufen im Cyberraum sowie die Reduktion von Konfliktpotentialen.

Ein wesentliches Hemmnis bei der Entwicklung internationaler Übereinkommen zur Regulierung und Reduzierung ungehemmter nachrichtendienstlicher und militärischer Aktivitäten im Cyberraum ist das fehlende gemeinsame Verständnis elementarer Begriffe wie „Cyberwaffe“[18] oder „Cyberangriff“. Bisherige Konzepte orientieren sich an etablierten Verfahren der Rüstungskontrolle aus anderen Technologiebereichen, tragen den technischen Besonderheiten der Domäne Cyberraum aber nur ungenügend Rechnung. So wird bspw. die Abschätzung des möglichen Schadens sowie die mutmaßlichen Intentionen eines Angreifers in aller Regel als Grundlage für die Bewertung einer potentiellen Cyberwaffe herangezogen. Eine solche Abschätzung ist jedoch im Gegensatz zu kinetischen Wirkmitteln aufgrund der abweichenden, zum Teil verzögerten und sukzessiven Wirkungsentfaltung von Cyberwaffen erheblich erschwerter und zuverlässig erst nach dem Einsatz der Cyberwaffe zu bewerten. Für Maßnahmen der Konfliktreduktion im Rahmen von Rüstungskontroll- und Abrüstungsübereinkommen, die auf einer Bewertung von potentiellen offensiv wirksamen Cyber-Hilfsmitteln vor deren Einsatz basieren, sind derartige Analyse-Verfahren nicht geeignet. Gleichzeitig fehlen im Bereich der naturwissenschaftlichen Friedens- und Konfliktforschung hinreichend entwickelte Konzepte und technische Verfahren, um diesen Herausforderungen der Rüstungskontrolle zu begegnen sowie andere geeignete Maßnahmen zur Unterstützung von Vertrauensbildung. Ein weitere gezielte Förderung und Anwendung derartiger Forschung im Rahmen deutscher außenpolitischer Initiativen als Gegengewicht zur allgemein zunehmenden Militarisierung des Cyberraum ist dringend geboten. Die friedliche Entwicklung des Cyberraum als globale, vernetzte und hochgradig voneinander abhängige Domäne ist für unsere Gesellschaft, Wirtschaft und Sicherheit von entscheidender Bedeutung.

[18] Vgl. dazu Fußnote Nr. 6

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.”