18. Wahlperiode

Deutscher Bundestag
Verteidigungsausschuss

Wortprotokoll
der 61. Sitzung

Verteidigungsausschuss
Berlin, den 22. Februar 2016, 13:00 Uhr
Sitzungsort: 10557 Berlin, Konrad-Adenauer-Str. 1
Sitzungssaal: Paul-Löbe-Haus, Raum 4. 900

Vorsitz: Wolfgang Hellmich, MdB

Tagesordnung - Öffentliche Anhörung

Thema der öffentlichen Anhörung:
"Die Rolle der Bundeswehr im Cyberraum – Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr"

Anlagen:

Schriftliche Stellungnahmen der Sachverständigen **Seite**

Anwesenheitslisten

(Seite 4 bis Seite 11)

II. Sachverständigenliste
Öffentliche Anhörung

"Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr"

am Montag, 22. Februar 2016, 13:00 bis 17:00 Uhr, im Paul-Löbe-Haus (PLH), Raum 4.900

Einzelsachverständige:	
Staatssekretärin Dr. Katrin Suder Bundesministerium der Verteidigung	Staatssekretär Klaus Vitt Bundesministerium des Innern und Beauftragter der Bundesregierung für Informationstechnik
Dr. Thomas Kremer Vorstandsmitglied Deutsche Telekom AG, Datenschutz, Recht und Compliance	Prof. Dr. Gabi Dreo Rodosek Universität der Bundeswehr München
Prof. Dr. Thomas Rid King's College London	Dr. Marcel Dickow Stiftung Wissenschaft und Politik Berlin
Prof. em. Dr. Michael Bothe Rechtswissenschaftler	

III. Sprechregister der Sachverständigen und Abgeordneten

Einziger Punkt der Tagesordnung

Öffentliche Anhörung zu folgendem Thema

Die Rolle der Bundeswehr im Cyberraum – Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr

Vors. **Wolfgang Hellmich** (SPD): Meine sehr verehrten Damen und Herren! Ich eröffne die 61. Sitzung des Verteidigungsausschusses, zu der ich Sie alle ganz herzlich begrüßen darf. Einziger Tagesordnungspunkt der heutigen Sitzung ist die öffentliche Anhörung zum Thema „Die Rolle der Bundeswehr im Cyberraum". Der genaue Titel lautet: „Die Rolle der Bundeswehr im Cyberraum – verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenen Herausforderungen und Aufgaben für die Bundeswehr".

Ich danke Ihnen, meine sehr verehrten Sachverständigen, dass Sie unserer Einladung zu der heutigen öffentlichen Anhörung nachgekommen sind, um die Fragen meiner Kolleginnen und Kollegen zu beantworten. Es sind auch mehrere Kolleginnen und Kollegen aus anderen, beteiligten Ausschüssen anwesend. An dieser Stelle ein herzliches Willkommen zu dieser öffentlichen Anhörung. Weiter begrüße ich alle anwesenden Gäste und Zuhörerinnen und Zuhörer. Begrüßen darf ich weiter Vertreter der Bundesregierung aus den unterschiedlichen Ressorts sowie Vertreter aus dem Bereich des Bundesrates.

Die heutige Anhörung wird live im Parlamentsfernsehen übertragen. Die Übertragung kann auch auf www.bundestag.de oder über die App „Deutscher Bundestag" auf Smartphones und Tablets im Smart-TV verfolgt werden. Sie sehen, wir nutzen alle Möglichkeiten der modernen Kommunikation, um auch diese Anhörung zugänglich zu machen. Aufgrund des großen öffentlichen Interesses an dem Thema und der begrenzten Platzkapazitäten hier im Saal haben wir auch noch eine Liveübertragung in den Sitzungssaal 4.800 organisiert und geschaltet. Ich begrüße auch dort alle Zuhörerinnen und Zuhörer ganz herzlich.

Im Ausschuss geht es heute darum, sich einen Überblick über den derzeitigen Diskussionsstand zu diesem sehr aktuellen Thema zu verschaffen. Die Ergebnisse dieser Anhörung dienen dazu, die weiteren Beratungen im Ausschuss und auch in der Öffentlichkeit auf eine fundierte wissenschaftliche Grundlage zu stellen. Der Cyberraum umfasst alle durch das Internet über territoriale Grenzen hinweg weltweit erreichbaren Informationsinfrastrukturen. Das ist eine Dimension in einem Raum, die wissenschaftlich-technisch einen Neuigkeitsgrad hat, mit dem wir uns politisch intensiv auseinandersetzen müssen. Er ist nicht nur zu einem wesentlichen staatlichen und öffentlichen Raum geworden, sondern er hat sich auch zu einem internationalen strategischen Handlungsraum entwickelt. Jenseits eines nationalen Bezugsrahmens sind Cybersicherheit und die Sicherheit kritischer Ressourcen des Cyberraums sowie der darin gespeicherten, verarbeiteten und übertragenden Informationen eine globale Herausforderung für alle Gesellschaften des 21. Jahrhunderts. Dies gilt auch für den Verteidigungsbereich. Der NATO-Generalsekretär Jens Stoltenberg hat im Frühjahr des letzten Jahres, am 19. Mai 2015, anlässlich des NATO-Transformation Seminars ausgeführt, dass Cyber heute praktisch ein zentraler Bestandteil nahezu aller Krisen und Konflikte ist. Cyberangriffe könnten möglicherweise sogar eine Artikel-5-NATO-Vertrag-Reaktion auslösen. Cyberattacken müssten schnellstmöglich erkannt und es müsste ihnen frühzeitig entgegengewirkt werden. Die Widerstandsfähigkeit müsste verbessert werden. Ebenso müsse man in der Lage sein, sich schnell von einem Angriff wieder zu erholen. Cyberverteidigung sei eine der Fähigkeiten die man benötige, um mit dem veränderten Sicherheitsfeld umzugehen. Das Thema Cyber soll auch auf dem nächsten NATO-Gipfel in Warschau ein wichtiges Thema sein.

Auch im Rahmen des laufenden Weißbuchpro-

zesses spielte das Thema Cybersicherheit bereits eine wichtig Rolle. Im September letzten Jahres fand dazu ein Expertenworkshop mit Akteuren aus Politik, Wirtschaft und Zivilgesellschaft statt, deren Ergebnisse sicherlich sehr umfangreich in das neue Weißbuch Eingang finden werden. Wie die Bundesministerin der Verteidigung in ihrem Tagesbefehl vom 17. September 2015 ausgeführt hat, ist die Bundeswehr im Cyberraum auf mindestens zwei Arten unmittelbar betroffen: Zum einen ist der Cyberraum bereits heute ein fester Begleiter konventioneller Operationsführung und stellt somit eine eigene Dimension wie bislang Land, Luft, See und Weltraum dar und zum anderen ist die Bundeswehr eine hochgradig vernetzte, zunehmend digitalisierte große Organisation, die sich schützen muss.

Das Thema ist also für den Verteidigungsbereich besonders aktuell. Beide Aspekte wollen wir hier heute hinterfragen und beleuchten. Hierzu begrüße ich nochmals ganz herzlich unsere Sachverständigen, die sich heute bereit erklärt haben, uns mit ihrer Expertise zur Verfügung zu stehen. Wir haben – und das ist eine Besonderheit – auch zwei amtierende Staatssekretäre als Sachverständige eingeladen. Das ist unüblich, aber beide verfügen über umfangreiche IT-Erfahrungen sowohl im privaten als auch im öffentlichen Sektor. Davon wollen wir heute profitieren. Wir haben Ihnen, sehr geehrte Sachverständige, mit dem Einladungsschreiben die Möglichkeit eingeräumt, eine schriftliche Stellungnahme zum Thema der Anhörung abzugeben. Für die eingegangenen Stellungnahmen bedanke ich mich ganz herzlich. Sie sind an die Mitglieder des Verteidigungsausschusses verteilt worden und werden dem Protokoll der Sitzung auch beigefügt.

Um noch einige technische Details zu klären: Von der heutigen Sitzung wird ein Wortprotokoll erstellt. Zu diesem Zweck wird unsere Anhörung auf digitalem Tonträger aufgezeichnet. Ich bitte Sie, bei jedem Wortbeitrag, das Mikrofon zu benutzen sowie ihren Namen zu nennen, damit wir alles auch ordentlich im Protokoll verzeichnen können. Wie Sie der Einladung bzw. auch der Tagesordnung entnehmen konnten, ist für diese Anhörung insgesamt eine Zeit bis 17.00 Uhr vorgesehen. Bevor ich den Sachverständigen das Wort gebe, habe ich noch eine Bitte an unsere Zuhörer: Die Dauer, der Umfang und das Interesse der Öffentlichkeit an dieser Anhörung sind groß. Bitte tragen Sie auch durch Ihr individuelles Verhalten dazu bei, dass wir diese Anhörung in der üblichen sachgerechten Weise durchführen können. Insbesondere bitte ich Sie, von jeglichen Beifalls- oder Missfallensbekundungen oder sonstigen anderen Äußerungen Abstand zu nehmen. Das könnte durchaus den Ablauf stören.

Einleitend möchte ich noch jedem Sachverständigen, jeder Sachverständigen die Gelegenheit geben, in einer kurzen Erklärung von etwa fünf bis zehn Minuten zu dem Thema Stellung zu nehmen. Danach werden wir mit der Befragung der Sachverständigen durch die Fraktionen fortfahren. Die Fraktionen haben sich darauf verständigt, drei Fragerunden durchzuführen, für die jeweils die sogenannte „Berliner Stunde" mit dem vom Bundestag beschlossenen erhöhten Oppositionszuschlag zugrunde gelegt wird. Dieser Oppositionsanteil wurde darüber hinaus für diese Sitzung noch etwas weiter nach oben aufgerundet, um der Minderheit hinreichend Möglichkeit für eine Befragung zu geben. Es beginnt die CDU/CSU-Fraktion, der 25 Minuten für jeden Komplex von Fragen und Antworten zur Verfügung stehen, gefolgt von der SPD-Fraktion, der 15 Minuten zur Verfügung stehen, der Fraktion DIE LINKE. und der Fraktion BÜNDNIS 90/DIE GRÜNEN, die jeweils insgesamt 10 Minuten für jede Fragerunde zur Verfügung haben. Innerhalb dieser Zeitkontingente bestimmen die Fraktionen selbst, wer eine Frage stellt und an wen sich die Frage jeweils richtet. Die Zeitkontingente umfassen dabei Fragen und Antworten.

Wir beginnen nun mit den Eingangsstatements. Ich gebe zunächst dem Staatssekretär Klaus Vitt aus dem Bundesministerium des Innern, Beauftragter der Bundesregierung für Informationstechnik, danach, in folgender Reihenfolge, der Staatssekretärin Dr. Katrin Suder aus dem Bundesministerium der Verteidigung, Dr. Thomas Kremer, Vorstandmitglied der Deutschen Telekom AG, zuständig für Datenschutz, Recht und Compliance, Prof. Dr. Thomas Rid vom King`s

College aus London, Prof. Dr. Gabi Dreo Rodosek von der Universität der Bundeswehr in München, Prof. em. Dr. Michael Bothe, Rechtswissenschaftler, vormals an der Universität Frankfurt, und Dr. Marcel Dickow von der Stiftung Wissenschaft und Politik. Vielen Dank, dass Sie mir so geduldig zugehört haben. Als erstes übergebe ich dem Staatssekretär Herrn Vitt das Wort.

SV Sts **Klaus Vitt** (BMI und Beauftragter der Bundesregierung für Informationstechnik): Sehr geehrter Herr Vorsitzender, vielen Dank! Ich möchte einmal bei der Digitalisierung beginnen. Wenn Sie die Digitalisierung betrachten: Es werden sich mit der zunehmenden Digitalisierung die Prozesse und die Abläufe sowohl in der Wirtschaft als auch bei uns im Staat erheblich verändern. In der Wirtschaft wird es teilweise komplett neue Geschäftsmodelle geben. Wenn man dann die Digitalisierung ein bisschen mehr und näher betrachtet, sind das eine intensivere IT-Unterstützung der Prozesse und Abläufe und ein intensiverer Informationsaustausch. Man hat bei der Digitalisierung auf der einen Seite zwar Chancen und Potentiale, aber auf der anderen Seite – das muss man ganz realistisch betrachten – nimmt die Abhängigkeit von den IT-Systemen zu. Damit bekommen die Verfügbarkeit und die Sicherheit der IT-Systeme eine immer höhere Bedeutung. Um das vielleicht noch etwas anders auszudrücken: Die digitale Verwundbarkeit wird durch die Digitalisierung sowohl in der Wirtschaft als auch in den staatlichen Einrichtungen deutlich zunehmen. Wenn ich dann noch die Cyberbedrohungslage betrachte; diese entwickelt sich zunehmend kritischer. Auf der einen Seite haben wir Angreifer, die immer professioneller werden, auf der anderen Seite gibt es immer neuere Angriffsarten oder Varianten von Angriffsarten.

Ich würde vielleicht nochmal kurz auf den Lagerbericht des Bundesamts für Sicherheit und Informationstechnik von 2015 eingehen. Da haben zum Beispiel die DDoS-Angriffe um 17 Prozent zugenommen, die kritischen Schwachstellen in Standard-IT-Produkten, die verfügbar sind, haben um 40 Prozent zugenommen und die Anzahl von Schadsoftware, die sozusagen verteilt wird, hat um 30 Prozent zugenommen. Schwerpunktmäßig ist hier das Betriebssystem Android von Smartphones betroffen. Es gibt einen weiteren Bereich, die sogenannten APT-Angriffe, die sowohl in der Wirtschaft als auch bei uns im Staat eine große Bedrohung darstellen. Ein Beispiel, das aktuell ja sehr diskutiert wird, ist das Thema bei dem Lukaskrankenhaus. Dort gibt es so einen Befall von einer Schadsoftware. Wie funktioniert so etwas? Da werden Mails rausgeschickt und die Mails haben entsprechende Anhänge, die präpariert sind. Wenn man da keine Sicherheitsvorkehrungen getroffen hat, werden dann die Systeme befallen und sozusagen von diesem Schadprogramm beschlagnahmt. Wenn man sich dann betrachtet, was besonders kritische Angriffsobjekte sind: das sind die Betreiber kritischer Infrastrukturen; da besteht die Möglichkeit von Angriffen auf diese Infrastrukturen. Denn wenn so ein Betreiber angegriffen wird, hat das eine entsprechende Auswirkung – sowohl schadensmäßig als auch flächenmäßig. Das heißt, wenn ich das andersrum formuliere, Cybersicherheit wird zu einer grundlegenden Voraussetzung für den Erfolg der Digitalisierung werden. Und nur wenn wir, Wirtschaft und Staat sowie innerhalb der Ministerien, eng zusammenarbeiten, unsere Kompetenzen bündeln, werden wir diese Herausforderungen der Zukunft meistern.

Wenn ich jetzt nochmal in den Cyberraum gehe und den Cyberraum betrachte, da muss man Folgendes feststellen: Innere und äußere Sicherheit fallen in wenigen Bereichen so eng zusammen wie im Cyberraum. Die Bedrohungslage im Cyberraum erfordert eine ganzheitliche Betrachtung im Rahmen unserer Cybersicherheitspolitik. Das heißt, die Wahrung der Cybersicherheit und der Cyberverteidigung ist nach Überzeugung der einzelnen Ressorts deshalb eine gesamtstaatliche Aufgabe, weil einer alleine das nicht mehr lösen können wird. Das können wir nur gemeinschaftlich bewältigen. Dazu gehört auch – das ist das was ich vorhin erwähnte – der Schutz der kritischen Infrastrukturen.

Wie geht es weiter? Die Konkretisierung der Aufgabenwahrnehmung erfolgt im Rahmen der Fortschreibung unserer Cybersicherheitsstrategie

unter Federführung bei uns im Innenministerium. Verteidigungsaspekte der gesamtstaatlichen Cybersicherheit sind dabei originäre Aufgaben vom BMVg und der Bundeswehr. Wenn Sie die Cybersicherheitsstrategie betrachten: Die stammt aus dem Jahr 2011. Die hat in wesentlichen Teilen noch Bestand. Damals sind Maßnahmen initiiert worden, die auch umgesetzt wurden, die die Sicherheit deutlich erhöht haben. Ich nenne mal hierzu das IT-Sicherheitsgesetz, das Mitte 2015 in Kraft getreten ist. Mit dem IT-Sicherheitsgesetz wurden Mindeststandards für die IT-Sicherheit bei den Betreibern von kritischen Infrastrukturen und die Meldepflicht bei kritischen IT-Sicherheitsvorfällen eingeführt. Wir arbeiten jetzt konkret an der Rechtsverordnung für die ersten vier Sektoren und Ende des Jahres für die nächsten drei Sektoren. Mit einer Übergangszeit von zwei Jahren werden wird dann diese Verordnung entsprechend in Kraft gesetzt haben und die Firmen haben einen Übergangszeitraum von zwei Jahren.

Dann haben wir noch das Cyberabwehrzentrum als übergreifende Informationsplattform für den strategischen und operativen Austausch der relevanten Bundesbehörden für die Bekämpfung von Cyberangriffen gegründet. Wir wollen in diesem Jahr unsere Cybersicherheitsstrategie aufgrund der Ausgangssituation – zunehmende Digitalisierung auf der einen Seite und die Cyberbedrohungslage, die sich kritisch entwickelt, auf der anderen Seite – aktualisieren. Wir werden diese Cybersicherheitsstrategie diskutieren. Wir haben in diesem Monat eine Diskussion in unserem Cybersicherheitsrat gehabt. Dort sind die Länder, die einzelnen Ministerien und die Wirtschaft vertreten. Dort haben wir unsere ersten Eckpfeiler diskutiert, Anregungen aufgenommen und im nächsten Schritt würden wir dann in die interne Abstimmung gehen.

Was sind wesentliche Eckpunkte der neuen Cybersicherheitsstrategie? Das sind die digitale Souveränität auf der einen Seite, die intensivere Zusammenarbeit von Staat und Wirtschaft und eine Cybersicherheitsarchitektur, wo wir nochmal konkret formulieren möchten, wie die Zusammenarbeit zwischen den einzelnen Akteuren ist. Wir arbeiten in diesen Fragen sehr intensiv mit dem BMVg zusammen, denn nur gemeinsam werden wir in der Lage sein, diese Herausforderung zu meistern.

SV Stsin **Dr. Katrin Suder** (BMVg): Vielen Dank und guten Tag auch von meiner Seite! Auch ich möchte kurz, dreigeteilt Stellung nehmen: zunächst etwas vielleicht ein wenig mehr aus dem Blickwinkel der Cyberbedrohung für die Bundeswehr zur Lage sagen, dann zu dem, was dies gesamtstaatlich bedeutet, und anschließend, was es für die Bundeswehr bedeutet.

Zum ersten, zur Lage. Herr Vitt hat es schon gesagt. Im Grunde könnte man sagen, Cyber ist so eine Art Steuer auf die Digitalisierung. Das heißt, Staat, Wirtschaft und Gesellschaft sind eben zunehmend digitalisiert und damit auch verwundbarer geworden. Ein paar Charakteristiken vielleicht, wie diese Verwundbarkeit sich darstellt und wie sie auch durch staatliche und nichtstaatliche Akteure genutzt wird: Zum einen ist Cyber relativ kostengünstig und effektiv; das ist ein Charakteristikum. Und damit ist es – könnte man in großen Anführungszeichen sagen – „ideal" für asymmetrische Wirkung. Häufig kann es eben eingesetzt werden, um Ziele auch unterhalb der Schwelle eines militärischen Angriffs durchzusetzen. Cyberangriffe können Spionage, Informationsmanipulation und mögliche Cyberterrorakte bis hin zu – Sie haben es angesprochen – groß angelegten Sabotageakten, beispielsweise an kritischer Infrastruktur, umfassen. Eine dritte Eigenschaft, die ich noch erwähnen möchte, ist das Thema Proliferation und exponentielle IT-Entwicklung, die natürlich noch diesen Trend und auch ein bisschen dieses Gefühl verstärkt, dass die Bedrohung überproportional zu den Fähigkeiten auf der IT-Sicherheitsseite wächst. Einige dieser Eigenschaften sind allerdings so gesehen auf einer Metaebene. Wenn man sich dies anguckt, ist es nicht neu, denn die kennen wir aus dem Thema hybride Kriegsführung. Allerdings – und das ist, glaube ich, das, was uns auch beschäftigt – ist die Quantität definitiv erhöht. Wir haben gerade Zahlen gesagt; wir reden über Millionen von sicherheitsrelevanten Ereignissen auf die entsprechenden Infrastrukturen. Aber auch

die Qualität der Bedrohung hat sich spürbar entwickelt. Und damit meinen wir, dass die Entwicklung von einfachen Viren hin zu komplexen, schwer erkennbaren Attacken, diesen sogenannten Advanced Persistent Threats oder APTs, geht, die einen deutlichen Qualitätssprung darstellen. Hierzu vielleicht auch eine Zahl: Im Schnitt braucht man ungefähr – und das ist nur das, was wir wissen – 200 Tage, bis man überhaupt einen APT erkennt. Dann dauert es in der Regel nochmal mehr als einen Monat, bis man die entsprechenden Probleme beheben kann.

Solche Cyberangriffe auf Staaten, kritische Infrastrukturen – Sie haben gerade das Beispiel des Krankenhauses genannt – sind schon lange keine Fiktion mehr, sondern Realität. Bekannte Beispiele sind sicher der Stuxnet-Angriff, der uns gerade in Berlin mit der Berlinale beschäftigt hat; es ist ja ein Film zu dem Thema rausgekommen; eines der Themen des Wochenendes hier in Berlin. Man kann auch den OPM-Breach nehmen – OPM ist das Office of Personnel Management – mit einem Datenabfluss von geschätzten 20 Millionen personenbezogenen Daten von Staatsangestellten in den USA oder auch das Thema Bundestags-Hack, das uns ja alle beschäftigt hat. Wenn man sich die APTs anguckt, kann man vereinzelte Muster erkennen, aber ein wichtiges Charakteristikum ist, dass sie sehr kompliziert und maßgeschneidert sind.

In Summe hat sich der Cyberraum zu einem internationalen und strategischen Handlungsraum entwickelt, der sich den klassischen Kategorien in manchen, jedoch nicht allen Dimensionen entzieht. Was meinen wir damit? Im Cyberraum existieren in dem Sinne keine Grenzen. Das Internet lässt sich so schwer an Staatsgrenzen festhalten. Angriffe können damit weltweit wirken und werden auch stetig weiterentwickelt und verfeinert. Die Grenzen zwischen Krieg und Frieden, innerer und äußerer Sicherheit oder auch kriminell und politisch motivierten Angriffen verschwimmen. Dazu kommt das ganze Thema der Attribution, was wir im Ausschuss ja auch schon diskutiert haben, das heißt der zweifelsfreien Rückführung von Angriffen auf einen Verursacher. Und das verstärkt in gewisser Weise das Gefühl dieser Grenzenlosigkeit des Cyberraumes. Aber – auch das muss man sagen – natürlich gibt es einen klaren Rechtsrahmen.

Wie kann man jetzt diesen vernetzten und sich steigernden Bedrohungen im Cyberraum begegnen? Zum einen – und das auch nochmal ganz klar aus meiner Sicht und auch von der Erfahrung vorher – nur gesamtstaatlich. Innere und äußere Sicherheit fallen in diesen Bereichen so zusammen wie in kaum einem anderen. Das heißt, es erfordert eine ganzheitliche und gesamtstaatliche Betrachtung und in dem Sinne darf nichts durch die Ritzen fallen. Herr Vitt hat es erwähnt: Wir, das BMI und das BMVg, sind in enger Abstimmung. Man muss sich komplementär und gleichzeitig eng verzahnt aufstellen, um die Cybersicherheit als gesamtstaatliche Aufgabe anzugehen, die man gemeinsam bewältigen muss. Dazu gehört auch, dass man sich gemeinsam überlegt, wie bestimmte Infrastrukturen geschützt werden können. Verteidigungsaspekte sind originäre Aufgabe vom BMVg und Bundeswehr. Es gibt übrigens ganz interessante Beispiele, wie so ein verzahntes Miteinander funktionieren kann, zum Beispiel im Bereich der Sicherheit im Luftraum.

Gemeinsam gilt es, die Kette von Prävention bis Reaktion, aber vor allem auch von einfachen bis zu komplexen Angriffen zu beherrschen; das ist, glaube ich, auch die Herausforderung. Dazu gehört ein großer Schwerpunkt auf der sogenannten Cyberhygiene, also der Cyberawareness, dass Mitarbeiterinnen und Mitarbeiter geschult werden, dass klar ist, dass wir Cyberresilienz bei Mitarbeiterinnen und Mitarbeitern, aber auch bei Bürgern, in der Wirtschaft und natürlich beim gesamten Staat unbedingt erhöhen müssen. Denn beim Hygienelevel sind eben Tür und Tor für viele Angriffe geöffnet und das ist das, wo viele ansetzen.

Gleichzeitig – das macht es eben kompliziert – müssen wir uns neben diesem Grundschutz auch mit den Hochwertangriffen, mit diesen APTs beschäftigen, und wir müssen dagegen gerüstet sein, gerade auch weil wir als Bundeswehr in dem Sinne ein Hochwertziel sind. Deshalb

brauchen wir genau diese Fähigkeiten im defensiven und im offensiven Bereich, die es kontinuierlich zu üben gilt, damit wir gerüstet sind.

Es ist mir wichtig, nochmal zu betonen: Dabei gelten für den Einsatz der Streitkräfte im Cyberraum stets die gleichen rechtlichen Voraussetzungen wie sie beim Einsatz anderer Fähigkeiten gelten. Es gibt keinen Einsatz von Cyberkräften ohne entsprechende Einsatzmandatierung im Sinne des Parlamentsbeteiligungsgesetzes durch den Deutschen Bundestag.

Letzter Punkt. Sicht auf die Bundeswehr. Wie muss sich die Bundeswehr jetzt im Cyberraum aufstellen und wie gilt es, sich weiterzuentwickeln? Vier Punkte. Das eine hatte ich schon angesprochen. Cybersicherheit ist ein riesiger Schwerpunkt und auch ein Schwerpunkt dessen, was wir jetzt tun: die eigenen Cyberfähigkeiten ausbauen, die Sicherheitsarchitektur so aufstellen, dass wir in Summe konsolidiert resilient sind, um dem allen zu begegnen und sich dann gleichzeitig das Thema APT-Schutz anzugucken. Wie können wir gegen solche Hochwertangriffe geschützt sein? Hier geht es um Waffensysteme. Wie können die gehärtet werden? Wie kann man sich mit nationalen Schlüsseltechnologien aufstellen? Das sind hier die Stichwörter.

Das zweite Thema hatte ich auch schon erwähnt, ist gesamtstaatliche Cyberfähigkeit. Wir müssen ressortübergreifend eng kooperieren, uns hier einbringen und auch darüber nachdenken, wie wir Cybercluster mit Wirtschaft, mit Wissenschaft und auch mit neuen Partnern bilden können.

Drittes Thema. Struktur. Hier spreche ich über eine Großorganisation mit ca. 250 000 bis 280 000 IT-Nutzern. Das heißt, wir haben eine Großorganisation, die es gilt, so aufzustellen, dass wir all diesen Schutz, all dieses überhaupt erreichen können. Es war auch im Tagesbefehl der Ministerin, den sie angesprochen hatten, erwähnt, dass wir uns primär auch neu aufstellen wollen, um die Kräfte und die wenigen Ressourcen, die wir haben, die solche Fähigkeiten haben, zu bündeln und gleichzeitig auch sicherzustellen, dass man Sicherheitsstrukturen implementieren kann. Das heißt, es geht sozusagen auch darum, die Strukturen in place zu bekommen.

Viertes Thema. Personal. Das liegt mir persönlich fast am meisten am Herzen. Wir reden hier ja auch oft von Spitzenpersonal, das solche Architekturfähigkeiten hat, das sich mit IT auskennt. Die Frage ist, wie können wir es für das BMVg, für die Bundeswehr, aber in Summe auch für den Staat und auch für die Wirtschaft schaffen, Spitzenpersonal zu rekrutieren, auszubilden, zu halten, das sich gemeinschaftlich dieser Problematik widmet. Das als Schlusssatz: Ich bin da der Überzeugung, dass sich die Bundeswehr und im Grunde wir alle uns gesamtstaatlich anders aufstellen müssen, auch mit anderen Partnern. Wir müssen uns öffnen, um diesen Herausforderungen gewachsen zu sein.

SV **Dr. Thomas Kremer** (Vorstandsmitglied Deutsche Telekom AG - Datenschutz, Recht und Compliance): Vielen Dank, Herr Vorsitzender! Sehr geehrte Damen und Herren Abgeordnete! Sehr geehrte Frau Staatssekretärin! Sehr geehrter Herr Staatssekretär! Meine Damen und Herren! Lassen Sie mich vielleicht zu Beginn eines einmal feststellen: Es gibt heutzutage keinen internationalen Konflikt mehr, der nicht auch virtuell, das heißt im Cyberraum ausgetragen wird – von Propaganda zu gezielter Desinformation bis hin zu Cyberangriffen auf Infrastrukturen, die ja, wie wir alle wissen, die Lebensadern jeder Gesellschaft sind. Beispiele sind die Angriffe auf die Elektrizitätswerke der Ukraine im Dezember 2015 und natürlich auch die jüngsten Veröffentlichungen zum Angriff auf die iranischen Infrastrukturen. Hinzu kommt, wir stecken mittendrin in der Digitalisierung unserer Wirtschaft und unserer Gesellschaft. Menschen, Maschinen und Geräte werden miteinander vernetzt und kommunizieren untereinander. Es entsteht eine Vielzahl von neuen Geschäftsmodellen und neuen Nutzungsmöglichkeiten. Damit entstehen auch neue Bedrohungsszenarien aus dem Cyberraum; das haben meine Vorredner auch beide erwähnt.

Nach meiner Einschätzung ist auch die Bundeswehr von dieser Entwicklung betroffen. Im globalen Cyberraum verschwimmen nationalstaatliche Grenzen, Zeitzonen verlieren an Bedeutungen und die Differenzierungen von Freund und Feind wird zunehmend schwieriger, teilweise gar unmöglich. Die Bundeswehr muss sich auf diese neue Bedrohungslage einstellen. Auch sie selbst kann natürlich Ziel von Cyberangriffen werden.

Wir als Deutsche Telekom identifizieren frühzeitig Angriffe auf unsere Infrastruktur und die dabei verwendeten Methoden. Unsere Sensoren im Netz, wir nennen sie Honeypots oder Honigtöpfe, registrieren derzeit bis zu 4 Mio. automatisierte Angriffe täglich. Individuelle Cyberattacken werden immer professioneller. Wir haben Fälle gesehen, in denen Angreifer in genau 6 Minuten das Zielsystem in voller Kontrolle übernommen haben. Und auch die Bürger erleben diese Gefahr aus dem Cyberraum immer konkreter. Laut einer aktuellen Umfrage von TNS Emnid im Auftrag der Deutschen Telekom ist fast jeder zweite Deutsche Opfer von Cyberkriminalität geworden. Weitere Fakten habe ich in meiner schriftlichen Stellungnahme für Sie aufgeführt.

Meine Damen und Herren! Für Cyberangriffe werden spezifische Programme verwendet, um bestehende Sicherheitslücken in IT-Systemen, also in Software, auszunutzen. Über diese Sicherheitslücken dringt ein Angreifer unbemerkt in die Systeme seines Zielobjekts ein. Dort kann er sensible Informationen abgreifen oder die kompromittierten Systeme so manipulieren, dass sie nicht mehr funktionieren. So ist es zuletzt Hackern gelungen, ganze Krankenhäuser lahm zu legen. Dies ist übrigens nicht nur in Deutschland, sondern auch in den USA passiert. Hinzu kommt, das Tarnen, Täuschen und auch spurlose Verschwinden ist in der globalisierten digitalen Welt vielfach einfacher als in der analogen. Militärische Cyberwaffen werden von Cyberkriminellen wiederverwendet. Ein Beispiel dafür ist die Schadsoftware Stuxnet. Mutmaßlich für Angriffe auf das iranische Atomprogramm entwickelt wurde sie nach der Entdeckung durch Cyberkriminelle abgeändert und für deren Zwecke eingesetzt. Und so geschieht es auch noch heute.

Meine Damen und Herren! Anders als bei der konventionellen Kriegsführung stehen im Cyberraum bisher vor allem zivile Ziele und hier insbesondere kritische Infrastrukturen im Fokus. Daher müssen sich Betreiber von kritischen Infrastrukturen besonders gegen virtuelle Angriffe schützen. Nur wer die Strategien und Methoden des digitalen Angreifers kennt, kann sich wirksam verteidigen. Die Bundeswehr steht dabei vor ähnlichen Herausforderungen wie die Privatwirtschaft. Zunächst einmal sind für einen wirksamen Schutz die allgemein bekannten Sicherheitsmaßnahmen erforderlich, das heißt Schutz vor Computerviren, Firewallsysteme, eingespielte Softwareupdates und natürlich Sicherheitstests. War ein Angriff erfolgreich, das heißt, ist ein Angreifer in das System seines Opfers eingedrungen, bedarf es analytischer Fähigkeiten, um die Ursache und Wirkung eines individuellen Angriffs zu erkennen; nur so können maßgeschneiderte Gegenmaßnahmen eingeleitet werden. Bei uns heißen die Leute Hunter Teams. Für mehr IT-Sicherheit braucht es allerdings Fachkräfte, die heute am Markt kaum verfügbar sind. Die Telekom hat daher damit begonnen, selbst Cybersecurity-Experten auszubilden. Auch die Bundeswehr könnte hier nach unserer Überzeugung mit ihren renommierten Hochschulen zum Beispiel mit der Schaffung eines Cybersecurity-Clusters viel erreichen. Zudem sollte die Forschungsförderung im Bereich der Cybersicherheit intensiviert und entsprechende Budgets bereitgestellt werden.

Lassen Sie mich noch einmal zusammenfassen: Es gibt keine Sicherheit, wenn wir die zunehmende virtuelle Bedrohung ignorieren. Sicherheit muss heute auch immer digital gedacht werden und dazu benötigen wir im Wesentlichen vier Dinge: Erstens. Wir brauchen EU-weite und nationale Regeln, die für hohe Standards bei IT-Sicherheit und Datenschutz sorgen. Es muss die gesamte digitale Wertschöpfungskette betrachtet werden: vom Netzbetreiber über die Hard- und Softwarelieferanten bis hin zu den Over-the-Top-Playern.

Zweitens. Wir brauchen eine hohe Sicherheit der IT-Systeme von Staat und Wirtschaft. Es darf keine Abhängigkeit von einzelnen Zulieferern geben und wir brauchen unabhängige Testcenter für Komponenten, die in kritischen Infrastrukturen eingesetzt werden.

Drittens. Wir brauchen gut vernetzte Expertenteams zur Cyberabwehr in Unternehmen und bei staatlichen Institutionen, die sich als Partner gegenseitig über neue Gefahren informieren. Wir brauchen Transparenz über Cyberangriffe, um die Lage einschätzen zu können. Eine enge Zusammenarbeit von Unternehmen und Behörden untereinander und übergreifend, wie sie zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik und die Deutsche Telekom praktizieren, sind sehr wünschenswert. Durch einen intensiven Informationsaustausch kann sichergestellt werden, dass Sicherheitsvorkehrungen schneller getroffen werden.

Und viertens. Einfache Lösungen für einen wirksamen Schutz von Informationen sind erforderlich. Dazu gehören insbesondere die wirksame Ende-zu-Ende-Verschlüsselung sowie datenschutzfreundliche und sichere Lösungen im Bereich der neuen Geschäftsmodelle. Sicher ist eines: Cybersecurity gibt es nicht zum Nulltarif. Verbraucher, Unternehmen und der Staat werden sich darauf einstellen müssen, für die virtuelle Sicherheit in Zukunft deutlich mehr Geld ausgeben zu müssen als in der Vergangenheit. Auch das ist Teil unserer digitalen Verantwortung.

SV Prof. **Dr. Thomas Rid** (King's College London): Danke! Ich fange mit den rechtlichen Rahmenbedingungen an, die Sie in Ihrem Fragekatalog in das Zentrum gerückt haben. Bis heute gibt es keinen Computernetzwerkangriff, bei dem etwa internationales Humanitäres Recht zu tragen gekommen wäre. Die Autoren des Tallinn-Manuals – das ist ein NATO-Handbuch zum Internationalen Recht in Anwendung auf Cyberwarfare, wie Sie schreiben – konnten sich nicht darauf einigen, ob der Stuxnet-Angriff gegen das iranische Nuklearanreicherungsprogramm in Natanz überhaupt als bewaffneter Angriff gelten könnte. Also wenn selbst das extremste Beispiel, das wir haben, nicht eindeutig genug ist, dann ist es für mich ein Zeichen dafür, dass der Rahmen, die Theorie, die wir hier versuchen anzuwenden, nicht so richtig passt. Daher heute ganz kurz zwei Fragen. Erstens. Was passiert eigentlich bereits, wie können wir das begreifen? Und zweitens. Was bedeutet das für Deutschland und was bedeutet es für die Bundeswehr?

Ich bin jetzt in den Beispielen noch konkreter als meine Vorredner. Was wir heute schon sehen sind zwei Dinge: Spionage – entweder Industriespionage oder politische Spionage – oder Sabotageakte. Herr Dr. Kremer hat die Stromausfälle in der Ukraine erwähnt; Sabotageakte ersten Ranges – übrigens operativ sehr beeindruckend. Der Trend der letzten 20 Jahre – und das ist ja kein neues Problem, das wir hier vor Augen haben; beispielsweise haben wir ab 1996 in den USA den ersten Advanced Persistend Thread gegen amerikanische Ziele gesehen – zeigt eindeutig, es geht hier um nachrichtendienstliche Tätigkeiten. Das sind vor allem Nachrichtendienste, die aktiv sind, und heute auch in hohem Maße die organisierte Kriminalität. Keine Streitkräfte. Alle großen Operationen, die wir erwähnt haben, sind die Arbeit von Nachrichtendiensten, nicht von Streitkräften.

Also konkrete Beispiele: Wir sehen in den letzten Jahren insbesondere gegen europäische Ziele zunehmend aggressives Verhalten. Warum? Weil die Snowden-Leaks, von denen Sie sonst sehr viel hören, ein Wettrüsten unter Nachrichtendiensten ausgelöst haben. In den USA und Großbritannien, wo ich arbeite, findet die nachrichtendienstliche Aktivität in einem viel restriktiveren Rahmen statt – politisch, wie Sie sich vorstellen können. Aber das Gegenteil trifft in Russland und China zu, wo wir einen viel höheres operatives Tempo sehen sowie aggressiveres Vorgehen und mehr Investitionen. Mir hat ein chinesischer Nachrichtendienstmitarbeiter in Peking direkt ins Gesicht gesagt: Snowden hat uns eine Fähigkeitslücke vor Augen geführt. – Im Klartext übersetzt: Wir wollen sowas auch haben.

Also konkret: Was haben wir gesehen? Gesteigertes operatives Tempo! Vor etwa zwei Wochen gab es im Spiegel eine hoch interessante Geschichte. Eine kurze Meldung darüber, dass laut einer Quelle aus deutschen Regierungskreisen der Hack des Bundestages, der letztes Jahr im Mai in die Öffentlichkeit kam – sie waren zum Teil, nehme ich an, betroffen, das macht es persönlich – die Arbeit – Zitat – „eines russischen Militärnachrichtendienstes" war. Also im Klartext heißt das: GRU. Das hier ist ein bedeutender Hinweis. Und übrigens – wichtig – muss man hier sehen: Eines der Themen, wo es in den letzten Jahren ganz klar einen Fortschritt gibt, ist Attribution. Attribution, also „wer war es" oder „den Täter zu finden", ist ganz klar möglich, und die Methoden, den Täter zu finden, haben sich sehr gut verbessert. In dem Fall haben wir eine hohe Sicherheit, dass es sich in der Tat um diesen Akteur handelt.

Frankreich: Der gleiche Akteur hat TV5 Monde wenige Monate vor dem Bundestag auch angegriffen; auch ein Beispiel von Sabotage in dem Fall. Noch ein drittes Beispiel aus Europa, das bisher nicht öffentlich bekannt ist. Der gleiche Akteur hat bereits im späten 2014 die italienische Marine gehackt und zwar – Zitat – „tief und hart", mit hoher Wahrscheinlichkeit bis in die klassifizierten Systeme vorgreifend. Wir sehen hier ein operatives Tempo, das sehr stark hoch geht, deswegen ironischerweise auch leichter zu identifizieren. Wir haben gleiche Muster russischer Machart gegen andere europäische Ziele in NATO-Staaten gesehen, insbesondere gegen militärische Ziele und Rüstungsunternehmen.

Ein kurzes Wort zum Stromausfall in der Ukraine, am 23. September 2015 bekanntgeworden. Wir reden hier auch von einer Schadsoftware und einem Vorgehensmuster, das sich ebenfalls auf russische Akteure zurückführen lässt. Das ist relativ klar. Nicht ganz klar ist, ob es der gleiche russische Akteur ist wie im Bundestagsfall, aber das Vorgehen und die Schadsoftware BlackEnergy 3 sind hier zumindest Zeichen. Und auch ein deutsches Beispiel. Sie haben sicherlich von dem Thyssen Stahlwerk gehört, das 2014 in einem BSI-Bericht als Beispiel erwähnt wurde und das nach gleichem Muster wie der Ukraineangriff gehackt wurde. Also ganz konkret: Wir reden hier nicht von abstrakten Problemen, sondern von wirklich sehr aggressivem Vorgehen.

Was heißt das also nun für die Bundeswehr und für Deutschland? Wenn Sie sich diese Operationen genau anschauen, dann können wir drei Dinge feststellen: Erstens. Die sind sehr aufklärungsintensiv. Es geht sehr stark um Zielaufklärung. So hohe Zahlen wie vier Millionen Angriffe pro Tag sind sehr irreführend, denn es handelt sich hier nur um Scans, nicht um nachrichtendienstlich betriebene, maßgeschneiderte Angriffe, die das eigentlich große Problem darstellen. Weil sie so nachrichtendienstlich intensiv sind, gehören aus meiner Sicht sowohl die Abwehr als auch die Aufgabe, sowas gelegentlich durchzuführen, ganz klar in den nachrichtendienstlichen Bereich und nicht so sehr in den der Streitkräfte.

Zweitens. Ein Thema, das auch bereits aufgegriffen wurde, sind Skills, auf Deutsch Fachkräfte. Die Erfahrung aus den USA und England und anderorts zeigt, dass Streitkräfte aufgrund des Rotationssystems, der Karrierestrukturen innerhalb der Streitkräfte ein großes Problem haben, die Skills intern zu entwickeln. Das ist ein Problem, mit dem sehr schwierig umzugehen ist. Auch die US-Streitkräfte haben damit große Probleme. Die Nachrichtendienste sind da von der Karriereförderung her viel besser aufgestellt. Nur ein Problem, das ich andeuten möchte.

Lassen Sie mich mit der Beobachtung schließen, dass ich es für sehr unwahrscheinlich halte, dass wir in der mittelfristigen Zukunft einen Fall sehen, bei dem der politische und rechtliche Kontext klar genug ist, um einen offensiven Einsatz dieser Fähigkeiten der Bundeswehr überhaupt möglich zu machen. Defensiv? Absolut! Offensiv? Sehr schwierig, weil es per Definitionem hybride Situationen in diesem Graubereich sind. Ich halte es dagegen für extrem wahrscheinlich, dass wir von einer weiteren Eskalation in einem nachrichtendienstlichen Bereich ausgehen müssen; das passiert jetzt schon. Und Deutschland hinkt – ich hoffe, ich kann mir dieser Beobachtung erlauben – hier an der Stelle hinterher.

Ich mache es für Sie hier noch mal persönlich. Der Bundestags-Hack, der offensichtlich hier in diesem Hause stattgefunden hat: Wissen Sie, wie der Verfassungsschutz überhaupt herausgefunden hat, dass es ein Problem innerhalb der Bundestagsrechner gibt? Weil ein britisches Unternehmen den Verfassungsschutz angerufen hat und gesagt hat: Schauen Sie doch mal bitte in den Bundestag rein, es könnte da ein Problem geben. Es war ein britisches Unternehmen, kein britischer Nachrichtendienst. Denn die Quelle dieser Informationen war, dass ein anderes Unternehmen, ein Kunde dieses britischen Unternehmens, als Exfiltrierer benutzt wurde. Deswegen haben die sich natürlich gewundert, woher diese deutschen Daten auf deren eigenen Servern kommen.

Der Punkt ist hier der deutsche Privatsektor. Es gibt kaum nennenswerte Unternehmen, die sich im Bereich Incident Response oder – noch wichtiger – Threat Intelligence einen Namen gemacht haben. Es gibt hier einfach keine großen deutschen Player. Ich denke, das ist etwas, dem man mit gezielter Förderung entgegenwirken kann.

SV **Prof. Dr. Gabi Dreo Rodosek** (Universität der Bundeswehr München): Sehr geehrte Damen und Herren! Ich möchte mich zunächst für die freundliche Einladung bedanken. Vieles haben meine Vorredner schon gesagt. Ich möchte vier Themen etwas näher beleuchten. Erstens. Wir wissen alle, dass Cybersicherheit die Schlüsselrolle einer digitalen Gesellschaft ist. Die Informations- und Kommunikationstechnologie ist heute in allen Bereichen der Gesellschaft von zentraler Bedeutung: im Gesundheitswesen, in der Produktion, in der Logistik, im Finanzwesen, in der Versorgung mit Energie und Wasser sowie auch in militärisch vernetzen Operationen. Die digitale Transformation verändert bereits heute unser soziales, gesellschaftliches und berufliches Leben. Hierbei kommt der Frage der IT-Sicherheit eine Schlüsselrolle zu. Eine vertrauenswürdige IT-Infrastruktur ist die Grundvoraussetzung für das Funktionieren in unserer heutigen, aber insbesondere auch zukünftigen digitalen Welt. Vertrauen und Sicherheit sind daher Kernbegriffe im Diskurs über Chancen und Risiken der digitalen Welt.

Zweitens. Hochqualifiziertes IT-Personal ist der Schlüsselfaktor. Die Beherrschbarkeit der IKT wird durch das außerordentliche Wachstum der Anzahl der internetfähigen Geräte – wir reden hier bis 2020 von um die 50 Mrd. vernetzte Geräte –, die hohen Bandbreiten, Multi-Terabit und mehr sowie durch die Entwicklung neuer Technologien – Software-Defined Everything, Inter-Cloud – immer schwieriger. Die Technologie wird immer „smarter" – u.a. Smart Homes, Smart Meters, Smart Car – und die Systeme immer vernetzter sowie auch autonomer. Hierzu kommt eine enorme Menge von Daten, der sogenannte „Rohstoff" der digitalen Welt. Eine effiziente Cyberabwehr oder -verteidigung kann nur gewährleistet werden, wenn aus der Flut der Daten die relevanten Informationen extrahiert werden. Das alles erfordert aber hochqualifiziertes IT-Personal, stetige Aus- und Weiterbildung und digitale Kompetenz auf allen Ebenen, von der Leitungsebene angefangen.

Drittens. Wir haben schon gehört: Cyberattacken werden immer ausgefeilter, sind zielgerichtet, persistent, komplex, steuerbar. APTs oder sogenannte Smart Attacks sind sehr schwierig zu detektieren. Laut Bitkom ist gut die Hälfte aller Unternehmen in Deutschland in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage und Datendiebstahl geworden. Die Anzahl zum einen und auch die Ungewissheit über das tatsächliche Ziel der Cyberattacke – ist sie nun zivil, ist sie nun militärisch – zum anderen fordern eine enge Kooperation zwischen den Sicherheitsbehörden. Die Verteidigung eines IT-Systems erfordert die Schließung aller Sicherheitslücken. Das heißt, der Verteidiger muss alle Lücken schließen, der Angreifer muss nur eine Lücke ausnutzen. Die Konsequenz ist, dass für einen Angreifer eine Vielzahl von Verteidigern notwendig ist, obwohl es natürlich illusorisch ist zu denken, dass wir alle Lücken schließen können.

Viertens. Es wurde schon die enge Zusammenarbeit angesprochen. Die Etablierung eines Cybersicherheit-Clusters des Bundes und der Bundeswehr wäre hier zu empfehlen. Es ist notwendig, die Kompetenzbündelung für sicherheitskri-

tische Forschung im Rahmen so eines Clusters, in dem die Forschung mit der Industrie und Behörden entlang der gesamten Wertschöpfungskette kooperiert, für die speziellen Belange des Bundes und der Bundeswehr mit substanziellen Forschungsmitteln zu etablieren. Die entwickelten Lösungen im Rahmen des Clusters sollen hierbei einen dualen Charakter haben. Das heißt, dass sie sowohl für den Schutz von militärischen als auch zivilen Einrichtungen bzw. Systemen Verwendung finden können. Um den stetigen Bedarf an hochqualifizierten IT-Nachwuchskräften sicherzustellen, ist es ferner notwendig, die Studienrichtung Cybersicherheit, aufbauend auf den Grundlagen der Informatik, zu stärken. Die Universität der Bundeswehr München mit dem Forschungszentrum CODE ist hier bestens geeignet – etwas Eigenwerbung – den Nukleus eines solchen Cybersicherheitsclusters sowohl in der Forschung, als auch in der Aus- und Weiterbildung zu stellen.

SV **Prof. em. Dr. Michael Bothe**: Vielen Dank, Herr Vorsitzender! Meine Damen und Herren! Die Nutzung von Computernetzwerken zur Schädigung fremder Staaten – das ist das, was wir unter Cyberangriff verstehen – besitzt ein hohes Schadenspotenzial, das eine Klärung seiner rechtlichen Schranken erfordert. Dieses neue Phänomen ist keineswegs rechtliches Niemandsland, in dem alles neu geregelt werden müsste. Vielmehr kann und muss bestehendes Recht sinnvoll darauf angewandt werden. Und wenn ich richtig sehe, ist das der Ansatz sowohl der Bundesregierung als auch Ihrer Kritiker.

Zunächst zum Völkerrecht. Hier möchte ich mit dem Friedensvölkerrecht beginnen, weil wir in dem Bereich bewaffneter Konflikte noch nicht so richtig wissen, was da eigentlich alles geschieht oder geschehen kann, während es im Frieden schon geschieht. Das wurde ja eben schon richtig gesagt. Auf den Cyberangriff, auf grenzüberschreitende Cyberangriffe ist eine alte allgemeine völkerrechtliche Grundregel anzuwenden, die es Staaten verbietet, andere Staaten zu schädigen, und den Staaten gebietet, mit der gebotenen Sorgfalt – wir sprechen von due diligence – zu verhindern, dass von ihrem Territorium Schaden auf dem Gebiet anderer Staaten verursacht wird. Das ist die sogenannte No Harm Rule. Sie gilt für ganz unterschiedliche Bereiche; sie gilt auch für den Cyberspace. Dabei ist dann allerdings fraglich, welche Kontrollpflichten ein Staat im Sinne dieser due diligence eigentlich erfüllen muss. Und wenn wir von Kontrolle reden, dann sind wir natürlich in einem äußerst kontroversen Bereich. Wir haben auf der einen Seite den Wunsch nach Kontrolle und auf der anderen Seite die Förderung des Free Flow of Information. Das geht nicht immer gut zusammen. Ein weiteres Problem in diesem Bereich ist die Rückverfolgbarkeit von Angriffen – nach dem guten alten Prinzip „Die Nürnberger hängen keinen, sie hätten ihn denn!". Ich habe eben mit großem Vergnügen vernommen, dass sich die Möglichkeiten der Bestimmung von Ursprüngen von Schadstiftung verbessert haben. Aber da besteht natürlich ein großer Bedarf, und Haftung ist eben ohne Zurechnung nicht möglich.

Damit komme ich nun vom Frieden in den Krieg. Das ist ja ein viel diskutiertes Phänomen und darauf muss auch irgendwie planend eingegangen werden. Das heißt, man muss zunächst einmal bestimmen, welche Schadstiftung eigentlich das völkerrechtliche Gewaltverbot verletzt oder gar als ein bewaffneter Angriff angesehen werden kann, der dann das Recht auf Selbstverteidigung nach Artikel 51 der Satzung der Vereinten Nationen auslöst. Da haben wir eine herrschende Meinung im internationalen Diskurs, die sich entwickelt: Es kommt auf die Wirkung der Schadstiftung an, nicht auf das Mittel. Wenn es auf das Mittel ankäme, dann wäre der Computerangriff eben niemals ein Waffeneinsatz. Aber wenn man auf die Wirkung abstellt, dann kann das genauso schlimm sein wie kinetische Waffen. Das, glaube ich, ist inzwischen herrschende Lehre, was nicht bedeutet, dass dieses Kriterium der Vergleichbarkeit physischer Schäden mit den Schäden, die durch traditionelle kinetischen Angriffe verursacht werden, etwas schwierig zu handhaben ist. Wichtig ist, dass wenn wir ein hohes Maß an physischen Schäden haben, dann ist der Schluss erlaubt, dass die Verursachung dieser Schäden ein bewaffneter Angriff ist, der zum militärischen Gegenschlag berechtigt, der

übrigens auch dann den Artikel 5 des NATO-Vertrages – die Beistandspflichten oder die Prüfung der Beistandspflichten – zur Folge hat. Hier bestehen ganz sicher Interpretationsspielräume. Und solche Interpretationsspielräume – das weiß der Beobachter der internationalen Szene – haben ein hohes Missbrauchspotenzial in dem Sinne, dass hier falsche Rechtfertigungen militärischer Gegengewalt stattfinden können.

Die Selbstverteidigung ist bei Militärpolitikern ein sehr beliebter Rechtfertigungsgrund und ist darum seit Jahrzehnten eine Herausforderung für völkerrechtliche Phantasien. Selbstverteidigung ist nur gegen den Staat zulässig, der die Erstgewalt ausgeübt hat, dem also ein erster Cyberangriff nachweisbar zuzurechnen ist. Das ist ein wichtiger Gesichtspunkt. Selbstverteidigung auf Verdacht geht gar nicht. Das ist eine Regel, die trotz der Schwierigkeiten der Zurechnung von Cyberangriffen zu beachten ist. Stellen Sie sich bitte nur vor, Iran hätte den Stuxnet als einen bewaffneten Angriff qualifiziert, interpretiert und dann gesagt: Die Israelis waren es, also greifen wir sie in Selbstverteidigung an.

Ein Wort zu dem hier viel beschworenen Prinzip der Abwehr, der Sicherheit. Von der Selbstverteidigung im Sinne eines Gegenschlags gegen einen Angreifer ist natürlich die passive Schutz- und Abwehrmaßnahme zu unterscheiden; die ist immer zulässig, auch wenn die Unterscheidung nicht immer einfach sein mag. Wenn denn ein bewaffneter Konflikt einmal entstanden ist, so gilt auch für Cyberangriffe das allgemeine geltende Humanitäre Völkerrecht über die Zulässigkeit von Schädigungshandlungen im Kriege. Auf Einzelheiten kann ich hier nicht eingehen, da haben die Verfasser dieses schon zitierten Tallinn-Manuals eine sehr große Phantasie walten lassen.

Ich komme zum Schuss zum Verfassungsrecht. Zwei Aspekte. Einmal: Nach Artikel 26 des Grundgesetzes ist die Bundesrepublik verfassungsrechtlich verpflichtet, keine Angriffe, auch keine Cyberangriffe auszuführen oder sich an ihnen zu beteiligen, die den Tatbestand des Gewaltverbots erfüllen und nicht durch Selbstverteidigung gerechtfertigt sind. Und das ist eine Selbstverständlichkeit, die man aber ruhig mal ab und zu wiederholen kann.

Ich komme zu dem, soweit ich sehe, bis jetzt überhaupt noch nicht in der Diskussion befindlichen Problem der parlamentarischen Zustimmung. Es gelten hier die gleichen Regeln wie sonst beim Einsatz von Streitkräften. Wenn also die Bundeswehr Cyberangriffe mit Wirkung im Ausland tätigt, dann gelten die allgemeinen Regeln über die Notwendigkeit parlamentarischer Zustimmung. Das gilt selbstverständlich nur, wenn es sich um eine isolierte Cyberoperation handelt und nicht um eine Cyberoperation im Rahmen einer ohnehin bestehenden bewaffneten Auseinandersetzung. Auch hier ist die Mindestschwelle der Zustimmungsbedürftigkeit das, was ich schon vorgestellt habe, nämlich die Wirkung. Wenn also solche Cyberoperationen erhebliche physische Schäden verursachen, sind sie zustimmungsbedürftig.

Viel spannender ist die Frage, was sonst noch zustimmungsbedürftig ist. Denn nach der Rechtsprechung des Bundesverfassungsgerichts in dem grundlegenden Urteil von 1994, wo das vom Bundesverfassungsgericht entwickelt worden ist, ist eben nicht nur von militärischen Zwangsmaßnahmen, die der Zustimmung bedürfen, die Rede, sondern von Einbezug in militärische Operationen. Was heißt das im Zusammenhang mit Cyberaktivitäten? Ich könnte mich jetzt einfach zurücklehnen und sagen, das überlasse ich jetzt erstmal den IT-Leuten, die da Szenarien entwickeln. Ich möchte aber trotzdem ein Beispiel nennen, das mir durch den Kopf gegangen ist. Wenn denn völlig zu Recht der Tornado-Einsatz, der nur der Aufklärung zu dienen hat – die schießen ja nicht, die schießen nur Bilder – zustimmungsbedürftig ist – und das ist sicherlich zustimmungsbedürftig, ist ja auch so behandelt worden –, dann kann man sich schon vorstellen, dass entsprechende Aufklärungsmaßnahmen, Eindringen in die militärische Cyberinfrastruktur eines Gegners, dann auch das Zustimmungserfordernis auslösen. Wir sehen auch an dem Tornadobespiel, dass man sich so solche Aktionen

durchaus isoliert in Kooperation mit Maßnahmen anderer Staaten vorstellen kann.

Schließlich ein weiteres Problem, das das Bundesverfassungsgericht nur angedeutet hat, was aber jetzt in der Praxis eine Rolle spielt, nämlich das Zustimmungserfordernis für geheimhaltungsbedürftige Maßnahmen. Das soll jetzt wohl für geheimhaltungsbedürftige Einsätze von Streitkräften mit einem besonderen Verfahren in das Gesetz aufgenommen werden; so jedenfalls der Entwurf, wenn ich das richtig gesehen habe. Für Cybereinsätze ist so etwas sicherlich zu prüfen. Das heißt aber, dass die Geheimhaltung nicht einfach das Erfordernis der parlamentarischen Zustimmung ausschließt, sondern dass für diese eben besondere Verfahren entwickelt werden können und müssen.

Zum Schluss. Was jetzt ? Was tun? Haben wir hier genügend Unklarheiten, dass neue völkerrechtliche Regeln entwickelt werden sollten und müssten? Das wird vielfach gefordert, daran arbeiten auch die Vereinten Nationen. Die Frage staatlicher Kontrollpflichten, die ich kurz angerissen habe, ist sicherlich etwas, wo mehr Klarheit sinnvoll wäre. Allerdings ist das eben auch Gegenstand des Streits. Dazu kommt etwas, was sich aus dem allgemeinen Klima der internationalen Beziehungen ablesen lässt: Die Chancen für völkerrechtliche Neuregelungen im militärischen Bereich sind im gegenwärtigen Klima der internationalen Beziehungen eher schlecht.

SV **Dr. Marcel Dickow** (Stiftung Wissenschaft und Politik Berlin): Vielen Dank, Herr Vorsitzender! Sehr geehrte Mitglieder des Deutschen Bundestages! Liebe Kolleginnen und Kollegen! Sehr geehrte Damen und Herren! Sie wissen, ich leite die Forschungsgruppe Sicherheitspolitik an der Stiftung Wissenschaft und Politik. Deswegen möchte ich mich auf drei zentrale sicherheitspolitische Implikationen für die Bundeswehr und für die Cyberfähigkeiten der Bundeswehr einlassen.

Erstens. Die Bundeswehr braucht die Fähigkeit, ihre IT-Systeme und -Netze im Friedensfall wie auch im Konflikt- bzw. Verteidigungsfall sowie in Auslandseinsätzen wirksam zu schützen. Ich plädiere allerdings im Friedensfall für eine enge Beschränkung dieses Auftrages auf die eigenen Netze. Für den Schutz ziviler IT-Infrastruktur in der Bundesrepublik bedarf es ziviler unabhängiger Stellen, die institutionell in keinen Interessenkonflikt mit möglichen offensiven Fähigkeiten geraten können. Hardware und Software ist immer von Menschen entwickelt und damit fehleranfällig. Zum Schutz der eigenen Systeme müssen solche Schwachstellen möglichst schnell entdeckt und geschlossen werden. Angreifer sammeln und nutzen das Wissen um solche Verwundbarkeiten, um in gegnerische Systeme eindringen zu können. Ungepatchte Schwachstellen, sogenannte Zero Days, stellen zusammen mit systematischen Verwundbarkeiten, zum Beispiel unsichere Hardware, das Haupteinfallstor dar.

Der eigene Schutz von Infrastruktur bietet aber nur relative Sicherheit. Wie in der zu schützenden Systemarchitektur können auch in der Sicherheitsarchitektur Schwachstellen und Lücken klaffen. Dies ist statistisch gesehen bei komplexen Systemen sogar unvermeidbar. Entnetzung, Abschottung oder systematische logische Begrenzung innerhalb der Netze können deshalb das Schutzniveau verbessern. Diese Maßnahmen können dauerhaft oder nur temporär, zum Beispiel während eines Angriffs oder Eindringens, eingesetzt werden. Solange sie auf die eigene Infrastruktur begrenzt bleiben, entstehen keine völkerrechtlichen Grauzonen. Hierzu ein kleiner Exkurs: Es gibt allerdings konzeptionelle Überlegungen, die Verteidigung gegen Angriffe bereits in die vorgelagerten Netze anderer zu tragen, wenn die eigenen Schutzsysteme nicht wirksam erscheinen oder technische Parameter dort höhere Erfolgsaussichten nahelegen, also Verteidigung schon in den Netzen anderer. Konsequent zu Ende gedacht bedeutet eine solche Strategie, den Angreifer in seinem eigenen System anzugreifen, während dieser von dort aus gerade operiert oder die Vorbereitungen dazu trifft. Dies stellt keine Verteidigung – Selbstverteidigung – im engeren Sinne dar und ist wenigstens im

Friedensfall nicht vom Auftrag der Bundeswehr abgedeckt.

Zweitens. Denkbare Angriffe im Zuge einer aktiven Verteidigung auf rein militärische Systeme des Gegners, zum Beispiel die Sabotage von angreifenden Flugzeugen oder ihrer Command-and-Control-Infrastruktur durch Schadcode, im Rahmen einer größeren konventionellen Auseinandersetzung können wirksam und angemessen sein, bergen jedoch immer Eskalations- und Proliferationrisiken. Eine solche Verteidigung wäre ohne intensive Vorbereitung nicht möglich und stellt de facto die Entwicklung von offensiven Cyberangriffsfähigkeiten dar. Auch in diesem Fall erscheint ein Verzicht bezüglich der Entwicklung dieser Einsatzmittel vor dem Hintergrund größerer politischer Interessen, auf die ich noch zu sprechen kommen, geboten.

Drittens. Über die Generierung von Wissen zum Schutz der eigenen Infrastruktur hinaus erscheint es sinnvoll, generell keine offensiven Fähigkeiten im Cyberraum für die Bundeswehr zu entwickeln oder entwickeln zu lassen. Ich möchte dafür drei Gründe anführen. Erstens. Offensive Fähigkeiten im Cyberraum bedürfen offener Sicherheitslücken in Software, die im Allgemeinen auch eigene zivile und militärische Systeme betreffen. Diese gezielt nicht zu schließen, vergrößert die Risiken und unterminiert die internationale Cybersicherheit. Zudem würde die Bundeswehr den globalen kommerziellen Handel mit diesen sogenannten Zero Days weiter befeuern. Zweitens. Vorbereitende Maßnahmen zum Entwickeln und für das Platzieren von Schadcode in gegnerischen Systemen führen auf einen Pfad, der beinhaltet, fremde Systeme generell als legitime Ziele aufzufassen und routinemäßig anzugreifen, um für den Ernstfall vorbereitet zu sein. Diese Kolonialisierung des Netzes widerspricht der deutschen Kultur der militärischen Zurückhaltung und trägt große Eskalationsrisiken in sich, wenn sich dies als Staatenpraxis durchsetzt. Und drittens. Die Entwicklung von offensiven Cyberangriffsfähigkeiten in und durch die Bundeswehr würde die Glaubwürdigkeit deutscher Cyberaußenpolitik vor allem in den Politikbereichen Internet Governance, Völkerrecht des Netzes und Menschenrechte online massiv einschränken und damit gegen fundamentale ökonomische und menschenrechtspolitische Interessen der Bundesrepublik Deutschland verstoßen.

Zum Schluss. Die Cyberfähigkeiten der Bundeswehr stehen also in einem größeren politischen Kontext von globaler Cybersicherheit. Eine klare militärische Beschränkung auf defensive Fähigkeiten vermeidet das Risiko, politische Opportunitätskosten beim Verlust von außenpolitischer Glaubwürdigkeit und in einem von Deutschland mitgetragenen Wettrüsten im Cyberraum tragen zu müssen.

Vors. **Wolfgang Hellmich (SPD):** Vielen Dank! Das ist eine breite Plattform für eine umfassende Debatte technischer politischer Rahmenbedingungen vom Völkerrecht bis zu militärischen Fähigkeiten und es obliegt nun den Fraktionen in den anschließenden Diskussionsrunden und Fragerunden, dieses weiter voranzutreiben. Als erstes hat die Fraktion der CDU/CSU das Wort.

Abg. **Henning Otte** (CDU/CSU): Herr Vorsitzender! Herzlichen Dank, liebe Kolleginnen und Kollegen! Herzlichen Dank im Namen der CDU/CSU-Fraktion an Sie, meine Damen und Herren Sachverständige, für Ihre Bereitschaft, heute zu diesem wichtigen Thema zu sprechen. Es wurde mehr als deutlich, dass die digitale Revolution alle Lebensbereiche durchsetzt. Und dem Stichwort „Industrie 4.0" in der Wirtschaft müssen wir meines Erachtens einen Begriff „Sicherheitspolitik 4.0" entgegenstellen. Das Bundesverteidigungsministerium hat bisher sowohl mit den strategischen Leitlinien als auch mit dem Prozess des Weißbuches diesen Begriff Cyber umfassend aufgenommen. Aber wenn wir rein militärisch denken, wird es so sein, dass in Zukunft ganze Gefechtsfelder digital abgebildet werden; die Industrie muss solche medialen Bilder auch abbilden können. Und überall müssen wir einen Schutzschirm haben. Das ist eine große Herausforderung.

Deswegen gehen meine ersten beiden Fragen an

Herrn Dr. Kremer. Sie haben auch den Inhalt der Cyberabwehr eindrucksvoll dargestellt. Ich möchte einmal um eine Einschätzung der Zuständigkeit von Schutz und Abwehr aus Ihrer Sicht bitten, ob Unternehmen selbst zuständig sind, ob der Staat im Rahmen der Diskussion um innere und äußere Sicherheit zuständig ist, insbesondere unter Berücksichtigung, dass beispielsweise ein Staat wie Nordkorea 2014 das Sony-Unternehmen angegriffen hat.

Und die zweite Frage geht an Frau Staatssekretärin Dr. Suder. Wir haben intensiv die Diskussion über Schlüsseltechnologien geführt und aus Ihrem Haus wurde sehr deutlich und sehr frühzeitig signalisiert, dass Router, Netzwerk und Kryptologie ein ganz wichtiges Beispiel für nationale Schlüsseltechnologien abbilden. Nun ist es so, dass wir sowohl national als auch europäisch kaum die industriellen Fähigkeiten dafür haben, sondern oftmals außereuropäisch auf Kräfte zurückgreifen müssen. Wie können wir diese Schlüsseltechnologien aus nationaler Sicht sicherstellen, um Deutschland Souveränität zu gewährleisten? Des Weiteren möchte ich an meinen Kollegen Dr. Brandl abgeben.

SV **Dr. Thomas Kremer** (Telekom AG): Die Frage der Zuständigkeit. Was haben wir gelernt, was entscheidend ist? Entscheidend bei einer effizienten Cyberabwehr sind die Zusammenarbeit und der Austausch. Weder eine Behörde noch ein großes Unternehmen allein hat den Überblick darüber, was tatsächlich im Cyberraum an Angriffen gerade passiert. Das sind immer nur Teilsichten. Das heißt, wenn man es effizient machen will, muss man kooperieren. Das gilt für Behörden untereinander, das gilt für Unternehmen untereinander und das gilt im Verhältnis von Behörden zu Unternehmen. Das ist aus meiner Sicht der ganz, ganz entscheidende Punkt bei der Frage der Zusammenarbeit. Transparenz, Informationsfluss und das möglichst schnell und effizient, das stärkt am meisten unsere Cyberabwehr. Das gilt sowohl für die Wirtschaft als nach meiner Einschätzung auch für die öffentliche Seite und die Bundeswehr.

SV Stsin **Dr. Katrin Suder** (BMVg): Herr Otte! Zu Ihrer Frage: „Wie können wir Schlüsseltechnologien sicherstellen?“ Wenn wir uns den IT-Stack ankommend angucken, also von unten, von der Hardware kommend, also Router und spezielle Schutzzeichen und Technologien, bis nach oben zur Anwendungsseite, stimmt es, dass wir gerade diese Fertigungstechniken in den Hardwaretechnologien in Deutschland, in Europa so nicht mehr haben. Das stimmt, das ist so. Und jetzt ist die Frage, wie man damit umgeht. Ich bin der Auffassung, dass das wahrscheinlich auch nicht wieder herstellbar sein wird, also das heißt, wir werden nicht wieder großflächig in diese Technologien investieren. Deshalb müssen wir uns damit beschäftigen, dass wir in höheren Schichten dann so etwas wie eine Hülle darum bauen. Das machen wir ja gerade auch bei unserem eigenen Netzwerk, wo wir im Grunde versuchen, mit Kryptotechnologien eine Hülle um die entsprechenden Router zu bauen.

Damit sind wir beim Thema Krypto. Dort gibt es in Deutschland durchaus die eine oder andere Firma, die auch sehr gute Fähigkeiten hat, wenn auch sicher nicht in der Größe und dem Kaliber. Und ich glaube, hier gilt es jetzt, genau darauf aufzubauen und zu sagen, es ist Schlüsseltechnologie und wie können wir auch wieder gesamtstaatlich, wie können wir als Cluster über alle verschiedenen Institutionen hinweg genau in diese Schlüsseltechnologien, die wir alle brauchen, auch wieder investieren. Das war ja auch etwas, was verschiedentlich schon angesprochen worden ist. Das heißt, wir müssen gucken, wie wir den Markt bündeln können, damit wir dann auch die entsprechende Markthoheit haben. Wir müssen überlegen, wie können wir auch Prozesse dafür, also Testprozesse, Beschaffungsprozesse – – Wie können wir agiler werden, um das zu befördern und uns letztendlich dort auch ganz klar dazu zu bekennen und die auch einzusetzen. Insofern sehe ich da schon Mittel und Wege. Aber was auch klar ist: Wir werden nicht mehr über den gesamten IT-Stack hinweg Schlüsseltechnologien haben können.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Herzlichen Dank! Ich würde meine Fragen nacheinan-

der an einzelne Experten stellen und dies dementsprechend auch so adressieren. Meine ersten Fragen gehen ebenfalls an Herrn Dr. Kremer. Wir haben gerade vorher, auch in Ihrem Statement, von den APT-Angriffen gehört. Meine Frage wäre, wie sich aus Sicht der Deutschen Telekom diese Bedrohung in den letzten Jahren entwickelt hat? Auch vielleicht im Verhältnis zum Thema Cybercrime, das ja einen kriminellen Hintergrund hat, während APT eher den nachrichtendienstlichen Hintergrund hat. Die zweite Frage: Sind solche APT-Angriffe auch eine Bedrohung für die Wirtschaft? Wir haben natürlich vor allem den Staat im Blick – wir bekommen Berichte über staatliche Angriffe auf staatliche Institutionen –, haben aber weniger Blick auf die Wirtschaft. Da würde mich Ihre Einschätzung interessieren. Und das dritte ist: Was würden Sie von der Bundesregierung – es sind zwei Staatssekretäre vom BMI und vom BMVg anwesend – erwarten, was sie konkret zur Erhöhung der Cybersicherheit in Deutschland beiträgt?

SV **Dr. Thomas Kremer** (Telekom AG): Wie haben sich die APT-Angriffe entwickelt? Da kann man sicherlich sagen, wenn ich in die letzten Jahre zurückgucke, die sind deutlich gestiegen. Wir sehen sehr viel Social Engineering darum herum, das heißt, die Angreifer überlegen sich sehr genau, wen sie im Unternehmen adressieren, zum Beispiel mit einer Mail mit welchem Inhalt und mit welcher getarnten Anlage, die dann Malware verseucht ist. Das ist das Erste. Das Zweite ist: Wir sehen auch, dass nicht nur ein Mitarbeiter im Unternehmen adressiert wird, um eine Malware zu installieren, sondern eine ganze Vielzahl. Der Angreifer hat ja schon dann Erfolg, wenn er 40 Leute mit einer E-Mail versorgt, wenn nur einer von denen das öffnet. Die 39 anderen, die Falle erkennen und vorsichtig sind und löschen, haben im Ergebnis dann doch nicht geholfen, weil es einen gegeben hat, der sich anders verhalten hat. Also das ist eine durchaus sehr, sehr reale Gefahr, die sich da auftut.

Ist das auch eine Bedrohung für die Wirtschaft? Selbstverständlich! Denn auch hier, gerade bei kritischen Infrastrukturen haben wir natürlich eine Verwundbarkeit. Und das Thema Wirtschaftsspionage, das muss ich natürlich hier in diesem Kreise auch nicht weiter ausführen, kann gerade über dieses Mittel aus Sicht der Täter sehr gut vorangetrieben werden. Das Thema Nachrichtendienste und Cybercrime ist für uns als Wirtschaftsunternehmen ein sehr komplexes, weil ich es nicht erkennen kann. Ich kann einem Angriff nicht ansehen, ob er von einem Nachrichtendienst oder einem Cyberkriminellen gemacht wird. Beispiel Stuxnet. Dieses Tool, diese Waffe, die wird von Kriminellen immer wieder im Ganzen oder in Teilen verwandt, verändert und dann für ihre Zwecke eingesetzt. Sie können also dem Tool selber und der Angriffsart nicht entnehmen, ob es sich um einen Nachrichtendienst, einen feindlichen Staat oder um Kriminelle handelt.

Thema Bundesregierung. Was kann sie tun? Ich glaube mit dem IT-Sicherheitsgesetz von 2015 ist eine ganze Menge getan worden. Aber hier ist mir insbesondere wichtig, dass jetzt die Möglichkeit, besteht auch die Software-Hersteller und Hardware-Hersteller in die Verpflichtung zur Bereinigung von Schwachstellen, also in das Thema Patchen, einzubeziehen, damit Lücken wirklich geschlossen werden können. Denn es gibt im Wesentlichen drei Ursachen für Cyberangriffe und drei Ziele: Das erste ist Software, das zweite ist Software und das dritte ist Software! Und wenn wir da anfangen und da ansetzen, ist es, glaube ich, genau das richtige. Zweiter Punkt ist: Wir müssen sehen, dass wir auf europäischer Ebene gleichziehen. Da ist die NIS Directive gerade in der Diskussion, kurz vor Ende. Da haben wir das Thema Soft- und Hardware-Hersteller allerdings nicht drin; ein aus meiner Sicht großer Mangel, an dem wir in der Zukunft arbeiten und versuchen müssen, da noch eine Nachbesserung zu erreichen.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich hätte die nächste Frage an Herrn Dickow. Ich habe mir Ihre Stellungnahme, die Sie uns dankenswerterweise auch zugesandt haben, noch einmal durchgelesen. Die erste Frage. Sie sprechen von Cyberangriffswaffen. Meine Frage wäre: Was ist eigentlich für Sie eine Waffe oder welche Definition von Waffe legen sie zugrunde? Die zweite Frage

wäre bezogen auf das Thema Attribution. Gibt es eigentlich eine Pflicht oder eine völkerrechtliche Norm, die besagt, dass ein Angriff in einem bewaffneten Konflikt bei einer Konfliktpartei zugeordnet sein muss, jenseits vom Cyberraum, wo es schwierig ist? Was ist die rechtliche Frage dazu?

SV **Dr. Marcel Dickow** (SWP): Es gibt natürlich keine völkerrechtlich verbindliche Definition einer Cyberwaffe. Ich persönlich würde jeglichen Schadcode, der dazu da ist, sozusagen größeren, möglicherweise auch physischen, aber eben auch immateriellen Schaden beim Gegner anzurichten, als eine solche bezeichnen. Aber es ist ein Begriff. Also, wir können auch einfach über Schadcode sprechen. Das, was wir APT nennen, kommt dem sicherlich sehr nahe. Es sind eben ausgefeilte technische Funktionalitäten, die sich nicht nur darauf beschränken in ein System, in ein gegnerisches System, einzudringen, sondern dort eben auch zu wirken, wie man in der Bundeswehrsprache sagt. Ich bin Ihnen auch sehr dankbar für die Frage nach der Attribution. Ich glaube, dass das nach wie vor ein ungelöstes Problem ist. Es gibt tatsächlich einige Fälle, die darauf hindeuten, dass man in bestimmten Situationen Angriffe attributieren kann. Ich sehe keinerlei Systematik, die nahelegt, dass man das immer tun kann. Selbst wenn man über quasi alle Fähigkeiten verfügt, ist es extrem schwierig nachzuweisen, wer tatsächlich hinter einem Angriff steht. Die einzige Fallkonstruktion, die ich mir vorstelle, ist eben, dass man sich bereits im System des Angreifers befindet und dort live mitverfolgt, was derjenige dann tut. Aber die Konsequenzen eines solchen Vorgehens habe ich eben angedeutet.

Wann darf man angreifen bzw. sich selbst verteidigen? Ich bin kein Völkerrechtsexperte, ich bin nicht einmal Jurist. Die Bedingung der Selbstverteidigung ist nicht einfach so gegeben, wenn man angegriffen ist, sondern sie muss sozusagen im direkten Zusammenhang mit dem Angriff stehen. Also, man kann nicht beliebig lange warten, nachdem man angegriffen wurde, um dann zurückzuschlagen. Es muss einen kausalen Zusammenhang geben und eben auch einen zeitlichen Zusammenhang. Wenn man das jetzt kombiniert mit Computerforensik, mit der Frage, wie man attributiert, woher ein Angriff kommt, dann kann es sein, dass man am Ende herausfindet, es war dieser oder jener Akteur, aber es kann eben Monate, manchmal sogar länger dauern, bis man das heraus findet. Das ist ein Fall, in dem das Selbstverteidigungsrecht nach der Meinung vieler Völkerrechtler nicht mehr zieht. Aber wie gesagt: Ich bin kein Völkerrechtler.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Herzlichen Dank. Meine nächste Frage richtet sich an die Frau Dr. Suder. Ich habe zwei Fragen. Wir haben einmal das Thema der Cyberangriffswaffen – ich verwende jetzt mal diesen Begriff – angesprochen. Wir haben vorher auch schon das Thema Proliferation gehabt. Meine erste Frage an Sie ist: Wie wollen Sie die Proliferation von Cyberangriffswaffen verhindern oder eindämmen? Und meine zweite Frage an Sie ist: Welche Maßnahmen ergreifen Sie, um ihre eigenen Waffensysteme der Bundeswehr resilient zu machen?

SV Stsin **Dr. Katrin Suder** (BMVg): Proliferation verhindern. Die erste Frage. Also zum einen, wenn wir uns das nochmal technologisch angucken; wir hatten es im Grunde gerade herausgearbeitet: Es geht um Software, aber es geht vor allem auch um Fähigkeiten. Und vorhin war ja der Begriff vor allem auch der Fähigkeiten; sie hatten den auch verwendet. Das heißt, dass ich mich ein bisschen schwer damit tue, denn vor allem sind das ja Programmierfähigkeiten. Wenn wir uns angucken, was ein APT ist, ist der im Wesentlichen eine Programmierfähigkeit, das heißt, er findet auch zum großen Teil in den Gehirnen statt. Und auch Software ist im Gegensatz zu einem Waffensystem und insbesondere zu einem Großwaffensystem auch etwas, was ich nicht so gut anfassen kann. Das heißt, wir müssen uns unbedingt damit beschäftigen. Sie hatten vorhin auch das Problem der Kontrolle angesprochen, Herr Prof. Bothe. Das heißt, die Frage ist: Wie kann ich sozusagen das Weitergeben von Gehirninformationen verhindern? Das ist ja ein extrem kompliziertes Thema. Ich wollte es nur deshalb erklären, weil ich glaube, dass die Fähigkeiten, die dahinter stehen, eben genau einen Unterschied zur Waffe darstellen, weil sie nicht so gut angreifbar sind. Trotzdem ist das definitiv

ein Thema, was uns beschäftigt. Und ich denke, man muss das auch unbedingt adressieren.

Es wurde ja auch schon mehrfach angesprochen: Wie können wir eigentlich auf zwischenstaatlicher Ebene zu Normen kommen? Wie können wir zu Regelungen kommen? Und hier ist ja, gerade auch in diesem Jahr, das ganze Thema OSZE, vertrauensbildende Maßnahmen, wie können wir darüber reden. Da gibt es ja diese Gouvernemental Group of Experts, die sich ja auch auf der Vereinten-Nationen-Ebene damit beschäftigt. Die haben versucht einen ersten Normengebungsprozess zu beginnen. Der ist schwierig, aber Herr Prof Bothe hat das klar angesprochen, warum der auch schwierig ist. Definitiv müssen wir das aber tun. Und dort engagieren wir uns jetzt auch wieder in Summe als Bundesregierung, denn dort ist natürlich auch das Auswärtige Amt ganz klar mit in der Verantwortung. Also, es gibt ein inhaltliches technologisches Problem in meinen Augen, aber wir müssen definitiv da was tun, und wir engagieren uns auch sehr stark. Das hat auch etwas mit Transparenz und vertrauensbildenden Maßnahmen zu tun.

Zweitens. Was tun wir selber, um uns selber und vor allem unsere Waffensysteme resilient zu machen? Das ist ein sehr wichtiges und zentrales Thema. Im Wesentlichen gibt es eine ganze Kette von Maßnahmen. Wenn wir nochmal zurückgreifen; wie können wir eigentlich sicherstellen, dass wir das, was wir bekommen, was auch „drin" ist – in Anführungsstrichen – im Input, in den Chips, in der Hardware, in der Software – erstmal über den Input der Komponenten kontrollieren. Das war ja auch die Frage von Ihnen, Herr Otte. Auch dort gibt es wieder mehrere Unterpunkte. Der eine ist: Wir haben unsere Zulieferer und dort müssen wir über Testcenter sprechen. Wir müssen über Zertifizierung sprechen. Das heißt, hier stützen wir uns auch auf die gesamten Instrumente ab, die es gesamtstaatlich gibt. Das andere ist, dass wir selber auch testen und selber auch uns damit beschäftigen. Das reicht aber nicht. Das heißt, wir kontrollieren zum einen die Zulieferer auch über ganz klare Vorschriften und Normen und wie wir mit denen umgehen. Und das andere ist: Wenn wir dann selber unser Waffensystem haben, dass wir das wiederum testen, dass wir hier auch einen sehr klaren Prozess haben – wer darf überhaupt was mit diesem System machen.

Und der letzte Aspekt noch. Wir haben ja unser eigenes CERT, also unser eigenes Response Team, das auch regelmäßig unsere Waffensysteme testet, um zu gucken, ob wir Schwachstellen haben oder nicht. Das findet regelmäßig statt. Hier sehen wir im Moment, dass wir ganz gut dastehen. Ich möchte jetzt nochmal auch wieder in meiner Rolle als Expertin einen Einblick nach oben oder nach außen geben. Ich weiß, dass eine andere Nation mal versucht hat, einen Fighter Jet auseinanderzubauen, um zu überlegen, wenn wir ihn komplett wieder nach Cybersicherheitsregeln mit eigenen Komponenten usw. zusammenbauen würden, würde man wahrscheinlich dasselbe Geld nochmal ausgeben müssen, was man einmal investiert hat. Ich glaube, der Weg wird es nicht sein. Das heißt, wir müssen Prozesssicherheit herstellen, wir müssen über Zertifizierung nachdenken, wir müssen über Testcenter reden und dann unsere eigenen Tests machen.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich hätte eine Nachfrage an Frau Suder. Sie haben nämlich den Faktor Mensch in Ihrer Stellungnahme angesprochen; ich glaube, Sie haben das Wort Hirn verwendet. Was tut eigentlich die Bundeswehr, um das notwendige hochqualifizierte Personal für diesen Bereich zu gewinnen?

SV Stsin **Dr. Katrin Suder** (BMVg): Also auch hier vielleicht wieder in der Struktur: Mehreres! Das eine ist, wie es die Ministerin ja in ihrem Tagesbefehl gesagt hat: Wir fangen erstmal an und ziehen das ganze Thema zusammen. Das hat ja auch etwas mit Sichtbarkeit zu tun. Das hat auch etwas mit Anerkennung und Bedeutung des Themas zu tun und damit auch wieder mit Attraktivität für Leute, die kommen. Das heißt, wir werden ja im nachgeordneten Bereich einen eigenen Bereich zum Thema schaffen und auch auf der Ministeriumsebene das ganze Thema IT und Cyber deutlicher bündeln und hervorheben. Das bedeutet zum einen Sichtbarkeit und auch Be-

tonung, aber eben auch, dass wir jetzt anfangen können, auch eigene Karrieren, auch Fachkarrieren einzuführen; ein Thema, das die Wirtschaft, mit Verlaub und mit Respekt, ja auch lange beschäftigt hat. Wie können wir Fachkarrieren herstellen, die auch jenseits von Führungskarrieren sind? Das ist das Eine, also erstmal die Voraussetzungen überhaupt zu schaffen, dass wir Menschen gewinnen können und dann auch binden können.

Und dann sind wir beim Thema Gewinnung. Da gab es ja auch schon gute Ideen. Die Kollegin hat es ja auch gesagt. Welche Rolle spielen also sozusagen ein eigener Studiengang, eine eigene Ausbildung? Und das ist definitiv ein Weg, den wir gehen wollen und werden. Das heißt, dass wir selber Leute ausbilden, selber auch dafür Studiengänge anbieten, um die Leute frühzeitig zu gewinnen und zu binden; das muss ich letztendlich sagen; das hatte ich auch in meinem Statement gesagt. Das alles müssen wir tun, das alles ist jetzt in der Planung, das alles werden wir tun. Aber ich glaube, das wird in Summe nicht reichen. Wir müssen uns Gedanken machen, wie wir in gewisser Weise aussteigen, in diesen Kampf um die klugen Köpfe, denn das ist ja eine Herausforderung, die uns alle angeht, und dann muss man auch zu anderen Zusammenarbeitsmodellen kommen – das Stichwort Cybercluster ist ja mehrfach genannt worden –, um nicht zu konkurrieren um diese Fähigkeiten, sondern miteinander zu überlegen wie wir die Probleme lösen können.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meine nächste Frage geht an den Staatssekretär Vitt. Wir haben jetzt gerade vorher ja vom Risiko von Angriffen auf kritische Infrastrukturen gehört, haben Beispiele gehört. Wie wären eigentlich der Ablauf, die Verteidigung, die Zuständigkeiten, die Informationskette im Falle eines Angriffes auf eine kritische Infrastruktur in Deutschland, beispielsweise in ein Elektrizitätswerk? Wie würde von staatlicher Seite darauf reagiert werden? Würde überhaupt reagiert werden?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Wir haben ja mit dem IT-Sicherheitsgesetz zwei Elemente definiert. Einmal die Mindestanforderung und dann der Fall, den Sie beschrieben haben: ein Angriff auf eine kritische Infrastruktur. Ich unterstelle jetzt, es ist ein kritischer Sicherheitsvorfall. Dann wird dieser kritische Sicherheitsvorfall dem BSI, das sich zusammensetzt, gemeldet, wird erkannt, wird bewertet, wird beurteilt. Dann läuft ein Strang ab, das wäre das Cyber-Abwehrzentrum. Da würde die Lage diskutiert, wird überlegt, was kann man tun. Parallel dazu würden die anderen Betreiber von kritischen Infrastrukturen über diesen Vorfall informiert mit der Bewertung und so, dass die rechtzeitig Maßnahmen ergreifen können, damit sozusagen dieser Angriff bei Ihnen erst gar keinen Erfolg hat. Je nachdem über welche Fassade es geht, ist der nächste Schritt, dass das BSI den Betreiber kritischer Infrastrukturen unterstützen würde. Nehmen mal an, zu einem späteren Zeitpunkt würde der rechtliche Aspekt analysiert. Dann würde das Bundeskriminalamt eingeschaltet, um dann den Staatsanwalt oder wen auch immer zu unterstützen. So ungefähr wäre der Ablauf.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Dann hätte ich eine Frage an die Frau Prof. Dreo Rodosek. Tut mir leid, dass sie jetzt nur drei Minuten haben, aber die Frage ist: APT-Angriffe. Welche systematischen Möglichkeiten haben Unternehmen, große Organisationen, staatliche Einrichtungen, sich überhaupt gegen solche Angriffe zu schützen? Kann man sich schützen?

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Wir sehen in der letzten Zeit eine immense Steigerung nicht nur der Quantität, sondern insbesondere der Qualität der APT-Angriffe. Können sich einzelne Institutionen schützen? Eigentlich nur, wie schon gesagt, durch Austausch und ein gemeinsames Vorgehen. Denn jede Institution sieht nur einen bestimmten Bereich der IT-Infrastruktur, die zu überwachen ist. Das heißt, nur durch effektive Zusammenarbeit kann erkannt werden, dass ein APT überhaupt läuft, und durch Live-Forensik und unterschiedliche andere Maßnahmen kann analysiert werden, was im System passiert. Das heißt, nur durch Zusammenarbeit

und natürlich durch die Entwicklung der Fähigkeiten, die wir dazu benötigen.

Vors. **Wolfgang Hellmich** (SPD): Zwei Minuten verbleiben.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich gebe die an die Opposition ab, das ist ein erhöhter Oppositionszuschlag von mir.

Vors. **Wolfgang Hellmich** (SPD): Aber jetzt ist die SPD dran. Das ist nicht die Opposition.

Abg. **Rainer Arnold** (SPD): Herr Vorsitzender! Liebe Kolleginnen und Kollegen! Werte Gäste! Auch von unserer Seite zunächst einmal ein Dankeschön an all die Experten, die hier sind, aber auch an die Vielen, die Interesse an diesem Thema haben. Ich glaube, es ist ein guter Ansatz, dass wir Verteidigungspolitiker das Thema, das uns insgesamt politisch und gesellschaftlich breit beschäftigt, heute mal auf den Bereich der Streitkräfte fokussieren. Uns beschäftigen drei Themenbereiche, zu denen ich auch einleitend fragen möchte. Natürlich das Thema Schutz. Das zweite Thema. Wie ist es ethisch, rechtlich, technologisch mit Angriffsfähigkeiten? Und drittens auch die Frage: Sind wir im Öffentlichen Dienst mit unserem Gehaltsgefüge überhaupt so aufgestellt, dass wir das Personal für die großen Herausforderungen finden?

Ich fange mal mit dem Thema „Angriffskönnen" an. Meine erste Frage dazu an Herrn Dr. Dickow; es können vielleicht auch andere darauf eingehen. Mein Verständnis ist, wenn man abwehren kann, entwickelt man zwangsläufig auch die Fähigkeit und das Wissen, angreifen zu können. Dies lässt sich nicht trennen. Wenn dem so ist, dann greife ich mal Ihr starkes Plädoyer dafür auf, dies selbst nicht zu tun. Gleichzeitig gehe ich davon aus, dass Streitkräfte aber für den Ernstfall natürlich alle Szenarien der möglichen Angriffe beherrschen müssen. Haben sie das so gemeint, dass Sie die Fähigkeiten erst gar nicht entwickeln, oder entwickeln Sie die Fähigkeiten für die Schublade, die Sie dann ggf. im Kriegsfall öffnen?

SV **Dr. Marcel Dickow** (SWP): Das ist eine sehr interessante Differenzierung. Sie haben völlig Recht. Man entwickelt die Fähigkeiten dadurch, dass man seine eigenen Systeme zum Eigenschutz testet. Das heißt, man versteht dann sehr genau, wo die eigenen Schwachstellen sind, und man versteht auch sehr genau, wo strukturelle Schwachstellen von IT-Systemen auftreten können. Das ist das eine. Das andere ist, daraus eine Angriffsfähigkeit zu entwickeln, das heißt, sie zum Beispiel in einen Schadcode umzusetzen. Und es ist ja nicht nur das eine, in das System eines Gegners einzudringen, sondern es geht ja auch darum, dann im System dort etwas zu machen, also dort unentdeckt zu bleiben, dort Informationen auszuleiten, dort Manipulationen vorzunehmen, von dort aus woanders hin, zum Beispiel zu den eigentlichen Command-and-Control-Servern zu kommunizieren. All diese Dinge muss man nicht ausbuchstabieren, muss man nicht ausentwickeln, wenn man sich auf den Eigenschutz beschränkt. Es gibt sozusagen technische Hürden, die das eine ermöglichen, nämlich den Eigenschutz, und das andere – sagen wir mal so – zumindest nicht befördern. Aber das Wissen ist natürlich da. Wenn man Angreifer im eigenen Netz studiert, erkennt man natürlich, wie sie vorgehen.

Es bleibt die Frage, ob man dieses Wissen umsetzt. Wenn man das tun will, zum Beispiel weil man in einem bewaffneten Konflikt, im Verteidigungsfall, auch in die Netze anderer wirken will, dann muss man diese Netze der anderen, die IT-Systeme der anderen, sei es militärische oder zivile oder Dual-Use-Systeme, vorher genau studieren. Und das tut man technisch gesehen, nicht politisch gesehen am besten von innen. Das heißt, wenn man dort angreifen oder sich dort verteidigen will, muss man vorher ziemlich genau wissen, auf was man sich vorbereiten muss. Und ob man diesen Schritt gehen will, sich also im Vorfeld in die Systeme der potentiellen Gegner begeben will, um dort herauszufinden, was einen erwartet und was man dann dort unternehmen kann, da habe ich meine Zweifel, dass man das tun sollte.

Abg. **Rainer Arnold** (SPD): Ich möchte daran

anknüpfen und die Vertreterin des Verteidigungsministeriums, Frau Dr. Suder, befragen. Liegt es nicht doch ein Stück weit in der Logik, dass Streitkräfte für den eventuellen Fall, alle Daten, die sie bekommen können, auch sammeln? Ich gehe mal von Cyber weg. Wir haben uns aus Vorbereitungsgründen immer darum bemüht, über das Segment Aufklärung Radarstationen auf der halben Welt zu kartieren. Wird im Zuge des Weißbuches nicht ein Klärungsprozess notwendig sein, dass die Bundeswehr solche Fähigkeiten aufbaut bzw. vorhält? Und wie ist dies dann mit den geheimdienstlichen Spionageaufgaben noch einigermaßen trennscharf handhabbar?

SV Stsin **Dr. Katrin Suder** (BMVg): Im Grunde war ja vieles bereits im Statement und da kann ich nur sagen: Ja! Ja, das ist etwas, was im Weißbuchprozess ist. Es geht genau darum, der Politik ein breites Spektrum von Fähigkeiten anzubieten. Und diese Fähigkeiten muss ich dann beüben und vorhalten. Insofern ist das meines Erachtens nach schon etwas. Um das auch nochmal ganz klar zu sagen: Dann unterliegen sie natürlich ganz klaren rechtlichen Randbedingungen, die auch mehrfach genannt worden sind, aufgegliedert von Völkerrecht bis hin zum Parlamentsbeteiligungsrecht; das haben wir ja auch sehr genau in dem Vortrag gehört. Aber ja, in meinen Augen geht es darum. Und das ist genau das, was mit CNO ja auch passiert, dass es dort um Fähigkeiten geht.

Die Abgrenzung. CNO hat natürlich eine Aufklärungs- und eine Wirkungskomponente. Das ist aber klar abzugrenzen von den nachrichtendienstlichen Aufgaben, denn die liegen nicht dort. CNO sind knapp 60 Leute; das ist ja auch etwas, was wir bereits gesagt haben. Ich glaube, wir müssen jetzt auch vorsichtig sein, dass wir nicht sagen: die ganze Welt und alle Netze und alles kartografieren. Wir haben ja auch gesagt, das was wir jetzt tun, tun wir auch sehr stark, damit wir uns erstmal konsolidieren, schützen und dann aufstellen, um überhaupt die Angebote machen zu können.

Abg. **Rainer Arnold** (SPD): Dann anknüpfend an Herrn Prof. Rid. Ist es überhaupt ein denkbares Szenario, dass man auf die Entwicklung von Fähigkeiten auch zum Angriff, zum Spionieren, irgendwann vielleicht auch zum Sabotieren, falls man in ein militärisches Szenario käme, – – Würden wir nicht dadurch eine extreme Asymmetrie erzeugen? Wenn wir nur mit hohem Aufwand abwehren und der Angreifer mit relativ geringem Aufwand die Möglichkeiten hat, müssten wir nicht schon aus Symmetriegründen – und ich frage dann auch den Völkerrechtler –, um überhaupt ein Bewusstsein für Rüstungskontrolle in dem Sinne „Wenn die Guten nichts tun, gewinnen die Bösen auch in diesen Fragen" zu schaffen, auch Symmetrie herstellen, damit eine Notwendigkeit für eine Rüstungskontrolle überhaupt erkannt wird?

SV **Prof. Dr. Thomas Rid** (King's College London): Ja, hochinteressante Frage. Vielleicht nochmal kurz zu dem „Angriffskönnen" – so haben Sie es, glaube ich, gerade schon in der Frage vorher genannt –, das notwendig ist, um militärische Effekte erzielen zu können. Insbesondere wenn das Ziel hochkomplexe Systeme sind – Elektrizitätswerk war ein Beispiel, Stuxnet, dieses Nuklearanreicherungsbeispiel, ein anderes –, dann ist gewissermaßen die Payload, die man entwickeln muss, also der Teil der Schadsoftware, der das System beeinflusst, entsprechend auf das System, für das Ziel zugeschnitten wie ein Maßanzug. Das heißt, man kann diesen Maßanzug nicht auf alle möglichen Ziele wiederverwenden. Der Arbeitseinsatz in die Payload ist sozusagen nicht einfach auf ein anderes Ziel einsetzbar. Das ist eine ganz wichtige Erkenntnis, weil die gewissermaßen die Offensive viel schwieriger macht. Das sind quasi Ein-Schuss-Waffen, die auf ein Ziel entwickelt sind. Stuxnet wurde auch nicht so oft wiederverwendet, weil die Payload sich überhaupt nur in Natanz aktivieren konnte.

Aber zu der Frage nach der Symmetrie, die sie ansprechen. Da müsste man jetzt lange ausholen. Viele der Fähigkeiten, die notwendig sind, um in entsprechend komplexe und gut geschützte Zielsysteme reinzukommen, haben mit Verwundbarkeiten zu tun, die nicht so leicht auf-

findbar sind. Dafür gibt es Schwarzmärkte. Die kann man auch selbst entwickeln. Und da stellen sich dann sehr schwierige Fragen, die auch schon zur Sprache kamen, zum Beispiel inwiefern man für alle letztlich ein unsicheres Umfeld erzeugt, wenn man diese Verwundbarkeiten selber hortet, entwickelt oder kauft. Diese Proliferationsdynamiken sind in diesem Bereich sehr komplex.

Abg. **Rainer Arnold** (SPD): Letzte Frage von mir an Herrn Dr. Kremer, dann macht Kollege Klingbeil weiter. Es ist das Stichwort Entnetzung gefallen. Wir haben ja in den letzten zehn Jahren das Gegenteil getan: möglichst Standardsoftware, alles IP basiert. Wie realistisch ist es aus heutiger Sicht noch, insbesondere militärische Führungssysteme durch Entnetzung dicht zu machen?

SV **Dr. Thomas Kremer** (Telekom AG): Jetzt muss ich um Nachsicht bitten, dass ich kein Experte für militärische Führungssysteme bin. Ich kann Ihnen in der Tat nur allgemein sagen, dass es sich extrem empfiehlt, dass man in dem Thema Vernetzung vorher eine Risikoanalyse macht, sich mal genau überlegt, ob ich eigentlich eine Vernetzung von bestimmten Geräten miteinander brauche. Es gehört eigentlich zu Cyberabwehr mit dazu, dass ich mir das zumindest überlege. Das kann in vielen Fällen dazu führen, dass ich diese Vernetzung brauche. Daneben kann ich nur auf die normalen Cyberabwehrthemen eingehen. Es fängt mit den Firewalls an bis zu den verhaltensbasierten Abwehrmethoden. Diese Dinge sind dann immanent. Ich kann nur sehr empfehlen, dass man sich das Thema „Was vernetze ich mit wem?“ zumindest überlegt, bevor man es gedankenlos installiert. Das findet man jedenfalls im industriellen Bereich doch schon an der einen oder anderen Stelle.

Abg. **Lars Klingbeil** (SPD): Ich übernehme für die SPD-Fraktion und will gleich bei einem Punkt, der gerade schon angesprochen wurde, nochmal nachhaken. Die Frage Offensivfähigkeiten. Ich weiß nicht, ob Herr Prof. Rid, Frau Prof. Dreo Rodosek oder Herr Dr. Dickow das beantworten können. Aber mich würde da die klare Abgrenzung nochmal interessieren. Kann man eigentlich ganz klar sagen, was defensiv und was offensiv ist? Wenn eine Attacke läuft und ich mich vielleicht dagegen schützen kann; wenn ich dann noch versuche, gegen die Rechner, die mich gerade angreifen, vorzugehen, ist das dann eine Offensivfähigkeit oder nicht? Da würde mich einfach eine klare Trennlinie, wie sie das aus der Wissenschaft bewerten, interessieren.

Und an Herrn Prof. Rid noch eine zweite Frage. Sie haben vorhin dargestellt, dass die Snowden-Enthüllungen quasi zu einer Aufrüstungsspirale im Cyberraum geführt haben. Das würde mich interessieren. Wenn sie das noch ein bisschen genauer darstellen können, was sie für Beobachtungen haben.

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Dann versuche ich mal anzufangen. Offensive Fähigkeiten, defensive Fähigkeiten. Man muss sich überlegen, was heißt offensiv und was heißt defensiv oder was ist Verteidigung, was ist Angriff? Die besten Verteidiger sind immer die besten Angreifer, weil sie genau die Schwachstellen kennen, wie sie in die Systeme hineingelangen und wie sie die Systeme kompromittieren können. Deswegen ist es schwierig zu erkennen, was im Prinzip defensive Fähigkeiten sind. Ich baue fünf Mauern um meine Kronjuwelen und wenn das nicht reicht – Stichwort Layered Security –, dann baue ich noch eine sechste Mauer und hoffe, dass der Angreifer, wenn er dann wirklich an die innerste Mauer kommt, aufgibt. Die Frage, die sich dann stellt, ist natürlich, ob ich denn erstmal den Angreifer identifizieren kann. Ich würde da nicht sagen, dass man den Angreifer immer identifizieren kann. Ganz im Gegenteil. Die Angreifer können sich tarnen und kennen sich sehr gut mit Techniken wie dem Tor-Anonymisierungsnetz oder Spoofing-Ansätzen sowie dem Verschleiern aus.

SV **Prof. Dr. Thomas Rid** (King's College London): Die Unterscheidung zwischen Offensive und Defensive ist in der Tat sogar im Fallbeispiel selbst manchmal extrem schwierig. Ein konkretes Beispiel, auch für Attribution, wäre hilfreich. Die

NSA wollte ungefähr im Jahr 2007 eine Attribution einer großen Kampagne chinesischen Ursprungs vornehmen. Das wissen wir aus den Leaks. Und was die NSA gemacht hat, war, in die chinesischen Äquivalente der Telekom einzubrechen und die IP-Adressen, die für den Angriff verwendet wurden, letztlich dem Kunden des Telekommunikationsunternehmens zuzuordnen. Und der Kunde war zu dem entsprechenden Zeitpunkt der Benutzung eben die nachrichtendienstliche Abteilung der PLA. Also in dem Fall eine einwandfreie Attribution. War das jetzt eine Offensive auf Seiten der NSA oder war es eine Defensive? Ich glaube, das ist eine interessante Frage an der Stelle, die gar nicht so leicht zu beantworten ist.

Ganz kurz vielleicht auf ihre Frage hin: NSA? Wettrüsten durch die Snowden-Leaks ausgelöst? Das Wichtige an der Stelle ist, dass man versteht, dass es extrem schwierig ist, auch zum Beispiel für mich als Wissenschaftler, die Snowden-Dokumente richtig zu beurteilen. Viele von Ihnen werden das Problem aus eigener Erfahrung kennen. Denn viele von den Dokumenten wurden unter hohem Zeitdruck gemacht, weil jemand mehr Geld für sein Projekt brauchte, weil jemand eine Beförderung wollte oder weil jemand einen Betriebsausflug zu einer Konferenz nach Barcelona machen wollte. Man hat die mit einer inneren Motivation gemacht, was es sehr schwierig macht. Es sind sehr viele Fehler und sehr viele Overstatements drin. Und diese werden nicht immer von anderen Nachrichtendiensten verstanden. Das heißt, das Einschätzen dessen, was auf Seiten der NSA und des GCHQ wirklich passiert und auch erfolgreich ist, ist extrem schwierig. Daher gibt es überschätzende Fähigkeiten.

SV **Dr. Marcel Dickow** (SWP): Dann ergänze ich noch an einer Stelle. Prof. Rid hat es eben gesagt und ich glaube, das ist ein wesentlicher Punkt. Wenn man versucht herauszufinden, wer einen angreift, wird man zwangsläufig Dritte involvieren. Denn Angreifer werden nie einen Angriff direkt fahren, sondern sie werden immer Proxies, technisch gesehen, benutzen – andere Server, andere Netze usw. So lange die nicht alle quasi im selben Augenblick mit einem kooperieren, hat man nur zwei Möglichkeiten: sie selbst anzugreifen, um den Proxy und den nächsten Schritt dahinter zu sehen, oder es eben sein zu lassen. Das heißt, wir haben es hier völkerrechtlich immer mit dem Problem zu tun, dass all die ganzen False-Flag Proxyoperationen, die da stattfinden, Dritte involvieren – und das ist die Regel – und dass der Verteidiger dazu gezwungen ist, sozusagen den selben Pfad zurückzugehen, den der Angreifer vorher hingegangen ist. Ich halte das auf jeden Fall völkerrechtlich, technisch sowieso für ein extrem problematisches Feld, auf das man sich begibt, wenn man sagt, dass man seine eigenen Systeme nicht nur dadurch schützt, dass man sie schützt, sondern, indem man sozusagen auch die Angreifer direkt vor Ort, wo auch immer das sein mag, bekämpfen will.

Vors. **Wolfgang Hellmich** (SPD): Danke sehr! Dann ist die Fraktion DIE LINKE. dran. Zehn Minuten plus eine Minute geschenkt.

Abg. **Dr. Alexander S. Neu** (DIE LINKE.): Vielen Dank für die bislang gemachten Ausführungen! Manche Fragen, die ich stellen wollte, sind bereits gestellt worden. Aber man kann nochmal nachhaken, um vielleicht zu präzisieren. Beispiel: Terroristen nutzen einen Staat als Safe Haven, um von dort Angriffe gegen Staat X zu fahren. Wenn ein Cyberangriff von einem nichtstaatlichen Akteur auf dem Territorium eines anderen Staates gemacht wird greift dann in dem Fall auch die sogenannte Safe-Haven-Theorie, wie sie 2001 im Umfeld des Afghanistan-Angriffes als Argument herangeführt wurde? Die Taliban waren seinerzeit die Gastgeber von Bin Laden und wurden dafür in Haftung genommen. Greift das auch in der Cyberwelt? Diese Frage geht an Prof. Bothe.

Wenn ein Staat die Verantwortung dafür hat, dass von seinem Territorium keine Cyberangriffe gefahren werden, welche rechtlichen und praktischen Konsequenzen hat das eigentlich für die Internetfreiheit, zum Beispiel in Deutschland? Ist das eine weitgehende Einschränkung oder wie muss man sich das vorstellen? Diese Frage ist an Staatssekretär Vitt gerichtet.

Frau Suder! Sie und, ich glaube, auch Herr Vitt hatten gerade darauf hingewiesen, dass äußere und innere Sicherheit in der Cyberwelt nicht mehr wirklich trennbar seien, dass sie weitgehend zusammenfallen. Wenn ich mir jetzt den Artikel 35 Grundgesetz „Amtshilfe" anschaue, komme ich da auf einen Punkt, dass die Amtshilfe ja möglich ist, dass die Bundeswehr also auch Landes- und Bundesbehörden aushelfen kann und vermutlich auch Unternehmen aushelfen kann. Hat die Amtshilfe nur einen temporären oder einen permanenten Charakter? Ich habe das so verstanden, dass die Amtshilfe nur einen temporären Charakter hat. Und wenn Ihrer Meinung nach ein Zusammenfallen von äußerer und innerer Sicherheit gegeben ist, muss das Ihrer Einschätzung nach eine Änderung, eine Anpassung des Artikels 35 Grundgesetz bedeuten?

Dann der Punkt Cyberangriffe bei Drittstaaten. Das wurde gerade schon einmal angesprochen. Ich möchte dennoch nochmal darauf eingehen. Cyberforensik. Angenommen man glaubt nachweisen zu können, dass aus dem Staat X ein Angriff gegen den Staat Y gefahren wird, ist sich aber noch nicht ganz sicher, weil der Angriff tatsächlich vom Staat Z über den Staat X ausgeht, also sozusagen ein Durchgangsstaat genutzt wurde. Wie sicher ist die Cyberforensik in dieser Frage? Wenn man das wie zum Beispiel im Bundestag, wo es weitgehend nachgewiesen ist, wie ich das verstanden habe, nach einem halben oder nach einem dreiviertel Jahr nachweisen kann, inwiefern ist dann noch nach so einem Zeitraum ein Vergeltungsschlag, also der Verteidigungsaspekt, tragfähig? Gibt es eine Definition, wie lange das Verteidigungsrecht besteht? Diese Frage wurde auch schon einmal aufgeworfen; Herr Dr. Dickow hatte versucht, das zu beantworten. Vielleicht von daher nochmal an Herrn Prof. Bothe.

Dann wurde von Vorneverteidigung gesprochen. Sie haben es sehr amüsant gesagt, Frau Prof. Dreo Rodosek: „Angriff ist die beste Verteidigung." Es ist natürlich ein bisschen schwierig, wenn man das den Chinesen zuschreibt. Wenn sie uns angreifen, verteidigen sie sich. So eine Argumentation finde ich etwas schwierig. Aber gut. Wenn die Vorneverteidigung, also eine Erweiterung des Verteidigungsbegriffs, die ja damit stattfinden würde – –. Meine Frage an Frau Dr. Suder. Hat es solche Maßnahmen, also gewissermaßen Vorneverteidigung, seitens der Bundeswehr bereits gegeben? Und Herr Prof. Bothe! Wie ist eine Vorneverteidigung aus der Sicht eines Völkerrechtlers zu bewerten?

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Ich möchte nur etwas klarstellen. Sie haben gesagt: „Angriff ist die beste Verteidigung". Das habe ich nicht gesagt. Ich habe die Schwachstellen gemeint. Wenn ich im System weiß, welche Schwachstellen es gibt, kann ich die auf einer Seite schließen, auf der anderen Seite kann ich sie aber auch ausnutzen. Das heißt, was ich genau kennen muss, ist die Schwachstellenanalyse. Welche Hardware und Software habe ich in meinem System. Mit was haben wir es zu tun? Wie weit ist unsere digitale Souveränität in dem Punkt? Wie können Lösungen entwickelt werden, die in einer per se unsicheren IT-Welt eine sichere Nutzung der IT unterstützen? Das heißt, es ging diesbezüglich wirklich nur um die Schwachstellen. Das wollte ich zur Klarstellung sagen.

SV **Prof. em. Dr. Michael Bothe**: Es ist natürlich ein guter Sport, alles, was im Allgemeinen unsicher und streitig ist, dann noch dadurch zu verkomplizieren, dass man es in den IT-Bereich bringt. Die Geschichte mit dem Safe Haven ist ja nun auch sonst nicht gerade unumstritten. Und zu sagen, die Operation Enduring Freedom in Afghanistan war deswegen zulässig, weil die Taliban al-Qaida einen Safe Haven geboten haben, das ist, sagen wir mal, zumindest eine ziemlich leichtsinnige Vereinfachung. So einfach ist das nicht. Auf der anderen Seite ist es sicherlich auch nicht so einfach, dass man sagt, wenn ein Angriff einer anerkannten Regierung eines Staates nicht zuzurechnen ist, dann ist das Territorium dieses Staates absolut geschützt – Souveränität, keine Selbstverteidigung!

Beide Positionen sind sicherlich in dieser Allgemeinheit nicht tragfähig. Ich komme gleich auf IT, aber Sie haben eben dieses Beispiel mit dem

Safe Haven gebracht, und das ist nicht zuletzt in Bezug auf Afghanistan entwickelt worden. Gerade in Bezug auf Afghanistan ist aber bis heute umstritten, wie die Rechtslage eigentlich ist. Und ich persönlich habe mich eher auf den Standpunkt gestellt, dass die Taliban letzten Endes damals die zwar nicht anerkannte, aber effektive Regierung Afghanistans und hinreichend in das involviert waren, was al-Qaida da getan hat, und dass Enduring Freedom von daher die Rechtfertigung als Selbstverteidigung erfahren hat. Das heißt, wir müssen genau hinsehen, und das gilt sowohl allgemein als auch für den IT-Bereich. Es gibt zwei Gründe, warum der militärische Gegenschlag zulässig sein kann. Das eine ist, dass wir genauer bei der Zurechnung schauen. Das muss man genauer tun. Ich habe vorhin gesagt, Selbstverteidigung auf Verdacht geht nicht, und Zurechnung auf Verdacht geht auch nicht. Die andere Möglichkeit der Rechtfertigung geht dahin, dass man sagt, hier hat die effektive Regierung eines Staates völlig ihre Macht verloren und darum ist hier ein neuer Akteur entstanden, gegen den dann Selbstverteidigung zulässig ist. Mein Beispiel ist der IS. Ich weiß, auch das ist umstritten. Angriffe gegen den IS erfolgen auf syrischem Gebiet in Gebieten, in denen eine effektive syrische Herrschaft einfach nicht mehr besteht. Dieses Szenario auf die IT zu übertragen, scheint mir etwas problematisch und schwierig zu sein. Hier haben wir Bereiche, die so von staatlicher Einflussmöglichkeit entkoppelt sind, dass sie sozusagen ihre eigene Welt darstellen.

Das bringt mich zu dem zweiten Problem. Nachweis und Abwarten. Selbstverteidigung ist Verteidigung gegen einen gegenwärtigen Angriff. Und irgendwann wird aus der Selbstverteidigung eine unzulässige gewaltsame Repressalie. Wann genau ist schwer zu bestimmen. Das ist eine Denkfigur, die für den eigentlichen militärischen Bereich, Umgang mit kinetischen Waffen usw., theoretisch ebenso unbestritten wie in der praktischen Anwendung schwierig ist. Dieser Gedankengang, dass der Angriff noch irgendwo gegenwärtig sein muss, um Selbstverteidigung zu rechtfertigen, ist für IT natürlich ausgesprochen schwierig. Eines ist sicher. Es geht nicht an, einfach unüberlegt zu sagen: Ich habe keine Zeit mehr, mir zu überlegen, wer es eigentlich war, also schieße ich auf Verdacht. Zu lange zu warten, kann andererseits zu einer Situation führen, wo wir dann andere rechtliche Maßstäbe haben. Und aufgrund all dieser Unsicherheiten habe ich auch in dem letzten Satz meines Statements geschrieben, die Entwicklung von Schutzmechanismen bleibt wichtiger als die Frage, wann ich eigentlich wie angreifen kann.

Die Frage der völkerrechtlichen Verneverteidigung. Was Verneverteidigung völkerrechtlich ist, weiß ich nicht. Wir haben verschiedene Spielarten von Selbstverteidigung, die umstritten sind. Es gibt die vorbeugende Selbstverteidigung gegen einen unmittelbar drohenden Angriff. Das ist die Frage, ob etwas nun unmittelbar drohend ist. Da haben wir große Probleme, ob wir einen Cyberangriff durch das Eindringen in andere Systeme wirklich als etwas, was unmittelbar bevorsteht, identifizieren können. Wenn da hinreichende Sicherheiten bestehen, dann ist natürlich auch eine Verteidigungsmaßnahme zulässig. Was nicht geht, ist die präventive Selbstverteidigung. Wir hatten mal eine amerikanische Militärstrategie, die so etwas eingeführt hat wie Verteidigung nach dem Vorsorgegrundsatz: Man kann ja nicht wissen, also tun wir was. – Das geht natürlich nicht. Das gilt allgemein und das gilt auch und gerade für den IT-Bereich.

Vors. **Wolfgang Hellmich** (SPD): Danke sehr! Jetzt nehmen wir aber die beiden Antworten – Sie müssen sich die Fragen jetzt merken – in die nächste Runde der 10 Minuten der Fraktion DIE LINKE. mit rüber, weil die Zeit um ist. Also ist die Fraktion BÜNDNIS 90/DIE GRÜNEN dran. Ebenfalls zehn Minuten plus eine.

Abg. **Agnieszka Brugger** (BÜNDNIS 90/DIE GRÜNEN): Auch von unsere Seite nochmal herzlichen Dank für die Statements, die Sie uns gegeben haben, die, glaube ich, auch wieder eine Reihe von neuen Fragen aufgeworfen haben. Ich will versuchen, mich auf ein paar zu beschränken, damit Sie auch Gelegenheit haben zu antworten.

Frau Staatssekretärin, Herr Staatssekretär! Sie haben ja in Ihren Statements jeweils beschrieben, wieviel an der Cyberwelt neu ist, von der Frage Trennung innerer und äußerer Sicherheit, von dem Punkt, dass man zwischen defensiv und offensiv eigentlich nicht wirklich unterschieden kann bis hin zu den Grenzen, die es eben in diesem Bereich nicht mehr gibt. Gleichzeitig haben Sie beide in Ihren Statements gesagt, die rechtlichen Regelungen, die wir haben, und die Grenzen auch der Aufgabenteilung zwischen Bundeswehr und Nachrichtendiensten sind ganz klar. Das passt auf den ersten Blick nicht unbedingt zusammen. Auch bei den Völkerrechtlern gibt es die Diskussion in dem Bereich. Inwiefern sehen Sie irgendwo noch Klärungsbedarf? Gerade wenn es um das Wirken in fremden Netzen geht, können Sie nochmal beschreiben, wo eigentlich in Zukunft die Nachrichtendienste zuständig sein sollen und wo genau die Bundeswehr und wie die rechtlichen Regelungen dafür aussehen?

Dann das Thema reine Cyberoperationen. Das Stichwort ist schon gefallen. Ich glaube, wir können uns alle vorstellen, wie ein Cyberangriff im Rahmen eines sozusagen normalen militärischen Einsatzes aussieht, und die Mandatierungspflicht kennen wir auch, ebenso wie die Rechtsprechung des Bundesverfassungsgerichtes. Wie sieht es aber in dem Fall bei reinen Cyberoperationen aus? Würde man ein Mandat bekommen, in dem nur der reine Cyberangriff geplant ist?

Herr Prof. Rid! Sie haben gesagt, Attribution sei viel einfacher geworden und man sei viel vorangekommen. Können Sie das vielleicht noch einmal ausführen, was für konkrete Maßnahmen Sie da meinen? Kann man eigentlich nicht immer die Herkunft verschleiern? Den Staaten ist es auch nicht immer direkt zuzuordnen. Es ist auch eine ganz entscheidende Frage ist, ob es staatlich in Auftrag gegeben wurde oder nicht.

Von Frau Dr. Suder würde mich interessieren: Herr Dr. Dickow hat die Glaubwürdigkeitsproblematik angesprochen, wenn es um das Wirken in fremden Netzen geht, auch im Vergleich zu den außenpolitischen Initiativen der Bundesregierung. Wo müssten da aus Ihrer Sicht die Grenzen für die Tätigkeit der Bundeswehr sein? Sehen Sie dieses Glaubwürdigkeitsproblem, das erwähnt wurde auch und inwiefern kann man dann etwas tun, um die Proliferation, die auch schon angesprochen und ausgeführt wurde, einzudämmen?

Noch an Herrn Dr. Dickow und Herrn Prof. Rid eine Frage. Vertrauensbildende Maßnahmen, Rüstungskontrolle, Regulierung – was sehen Sie da an Möglichkeiten im Cyberraum? Denn ein Teil der Staaten sagt zwar immer, man möchte da mehr Sicherheit, mehr Regeln, baut aber auf der anderen Seite selber Kapazitäten auf, um genau diese zu umgehen und zu verletzen.

SV Stsin **Dr. Katrin Suder** (BMVg): Ich fasse einfach mal die ganzen Themen zusammen. Was ist unklar, was ist klar? Ich glaube, es herrscht doch relativ viel Klarheit. Wahrscheinlich wollten Sie auch darauf eingehen, was die Teilung im Inneren anbelangt, was ja auch so ein bisschen in Richtung der Frage geht, die wir uns für die nächste Runde aufbewahrt haben, was ist sozusagen mit Amtshilfe. Hier ist in meinen Augen sehr viel Klarheit und die sollte man auch nicht zu sehr versuchen zu verwischen. Es gibt offene Fragen, die hatten wir ja gerade schon gehört, die vor allem mit der verfassungsrechtlichen Ebene zusammen hängen. Teile der Genfer Konvention: ich glaube, 1977 und 1949 sind Teile des Völkerrechts entstanden. Dort gab es das Internet ja so noch nicht. Und dort gab es ja so natürlich auch noch nicht bestimmte Detailregelungen. Das heißt, man muss sich natürlich überlegen, wie das Gesetz und wie Rechte auf die moderne Zeit bezogen ausgelegt werden. Aber ich glaube, das ist eine Aufgabe der Juristen, und ich bin keine Juristin, sondern Physikerin. Das würde ich jetzt auch anderen überlassen wollen. Aber insofern glaube ich, gibt es Dinge, die sehr klar sind, gerade auch wie das Wechselspiel im Inneren aussehen kann.

Glaubwürdigkeitsproblematik. Wir haben allein schon zwei Thesen dazu gehört. Herr Arnold hatte ja auch eine Gegenthese aufgestellt, was die

Glaubwürdigkeitsproblematik anbelangt. Insofern möchte ich da jetzt nicht eine dritte hinzufügen. Aber wir haben allein zwei gehört. Ich möchte nochmal darauf eingehen, was es konkret für uns, für die Bundeswehr bedeutet. Zum einen, was die Proliferation von unseren eigenen Werkzeugen und Tools anbelangt, die können wir natürlich sehr gut kontrollieren und die haben wir auch im Griff und selbstverständlich tragen wir auch nicht dazu bei, dass es darum geht, dass man Zero-Days sozusagen künstlich vorhält. Das kann nicht Sinn und Zweck der Sache sein. Ich habe es vorhin gesagt, ich möchte es aber nochmal bekräftigen: Ich glaube aber, natürlich ist das Thema – und da sind es nicht wir, sondern da sind es vor allen Dingen auch andere – absolut wichtig, dass wir uns mit Proliferation, mit vertrauensbildenden Maßnahmen – – und dass wir das Thema gesamtheitlich und gesamtstaatlich adressieren. Das tun wir auch sehr aktiv. Wir sind ja in den verschiedenen Expertengruppen – Auswärtiges Amt, aber auch wir stellen Leute dazu ab – sehr aktiv. Das halte ich für absolut notwendig, das zu tun. Insofern ist es eines, was wir mit unseren Dingen machen. Dort haben wir natürlich eine gewisse Kontrolle und können das natürlich auch tun, aber nicht gesamtstaatlich. Dort geht es darum, zwischenstaatliche und überstaatliche Prozesse unbedingt zu befördern.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Vielleicht kann ich das noch kurz ergänzen. Ich hatte hier im Rahmen der Cybersicherheitsstrategie ja dargestellt, dass wir versuchen, diese Herausforderung durch die Bündelung der Kompetenzen hinzubekommen. Dann ist die Bündelung der Kompetenzen erstmal auf der Basis von den heute rechtlichen Regelungen. Wenn wir da an die Grenzen stoßen, käme dann der nächste Schritt. Aber wir machen das erstmal in dem Rahmen der heutigen rechtlichen Möglichkeiten.

SV **Prof. Dr. Thomas Rid** (King's College London): Ganz kurz auf Ihre Attributionsfrage geantwortet. Unter Fachleuten ist heute die Frage, die man diskutiert, nicht: Ist Attribution möglich, ja oder nein?, sondern: Wie können wir die Qualität steigern und die Qualitätsevidenz hochfahren? Grob gesagt: Wie gut Attribution ist, ist eine Funktion der Ressourcen, die Sie für ein bestimmtes Problem einsetzen. Eine Zeit, die Sie haben, um die Frage zu beantworten. Und natürlich auch, wie gut der Gegner ist, wie gut die antiforensischen Fähigkeiten des Gegners sind. Da muss man einfach ganz nah an den Fallbeispielen argumentieren. Es gibt sehr viele Beispiele, wo wir Attribution mit sehr hohem Grad erreichen können. Viele davon sind öffentlich. Ich halte mich ganz kurz und verweise hier auf die Studie, die derzeit in der Debatte führt: „Attributing Cyber Attacs". Sorry, ich habe Sie zufällig mit einen Kollegen zusammen geschrieben. Die wird in mehreren Behörden auch verwendet, um Attribution zu betreiben. Sorry, das war jetzt very un-British on my part.

Zweiter Punkt, ganz kurz nur. Vertrauensbildung an der Stelle. Ich verfolge die Debatte hier in Deutschland über die Nachrichtendienste, NSA-Untersuchungsausschuss etc. mit etwas Unbehagen, denn was ich sehe, ist nämlich ein sehr stark unterminiertes Vertrauen in Erkenntnisse von Fachleuten. Und leider sind die Fachleute in dem Bereich vor allem in den Nachrichtendiensten. Wenn Sie genau hinhören, sind zum Beispiel in der Encryption-, in der Verschlüsselungstechnologiedebatte, die ganz offensichtlich gerade mit Apple versus FBI sehr hohe Wellen schlägt – – auch letzte Woche in München bei der Sicherheitskonferenz, dann hören Sie von den Leuten aus den Nachrichtendiensten, sehr nuancierte, sehr vorsichtige Statements und oft von den Leuten aus den Polizeibehörden der USA etwa und auch aus Innenministerien viel restriktivere und problematischere Statements. Man muss da ganz genau hinhören. Es gibt jetzt auch sehr viel öffentlich zugängliche Informationen aus den Nachrichtendiensten aus dem englischsprachigen Raum.

SV **Dr. Marcel Dickow** (SWP): Dann habe ich wahrscheinlich die schwierigste Frage abbekommen. Was gibt es eigentlich für Möglichkeiten für Vertrauensbildung und auch für Rüstungskontrolle? Wir haben dazu ein bisschen was im sogenannten Ausblick der SWP aus dem Januar diesen Jahres geschrieben. Ich glaube, wir

müssen uns von klassischen Konzepten insoweit verabschieden, dass wir neue Akteure für solche bislang auf staatlicher Ebene ablaufenden Prozesse zulassen müssen. Wo wir früher Rüstungskontrolle zwischen Streitkräften und Staaten gemacht haben, habe wir jetzt überwiegend private, kommerzielle Akteure, die wir da irgendwie einbeziehen müssen. Und das wirft unser Konzept mehr oder weniger über den Haufen. Das trifft aber auch auf andere Felder, wie zum Beispiel die Robotik, zu. Das macht es jetzt nicht einfacher und das ist auch keine Antwort auf die Frage, welche vertrauensbildenden Maßnahmen wir machen können.

Mein Vorschlag ist immer, wir sollten da ansetzen, wo wir die größten Sicherheitsprobleme haben. Und die größten Sicherheitsprobleme haben wir in der Software. Also wenn wir es irgendwie schaffen, dass die Software sicherer wird, dann werden wir auch in irgendeiner Form Vertrauen schaffen. Deswegen sollte alles, was dazu dient, Unsicherheit zu schaffen und Unsicherheit aufrechtzuerhalten, im Sinne von Vertrauensbildung reduziert werden. Mein konkreter Vorschlag wäre, dass sich Staaten zum Beispiel darauf verpflichten, Sicherheitslücken grundsätzlich nur zu schließen und sie nicht auszunutzen. Ich weiß, dass das mit den Amerikanern im Moment nicht zu verhandeln ist – völlig klar. Und da gibt es sicherlich auch noch einige andere europäische Staaten, die das so sehen. Die Sicherheitslücken sind aber das zentrale Problem, mit dem wir irgendwie umgehen müssen.

Abg. **Agnieszka Brugger** (BÜNDNIS 90/DIE GRÜNEN): Dann nochmal die Frage der Mandatspflichtigkeit bei reinen Cyberoperationen, denn ich glaube, dass es eine ganz entscheidende ist, weil die bisherige Rechtsprechung des Bundesverfassungsgerichtes hier offensichtlich mit den Kriterien, die sie aufgibt, an ihre Grenzen stößt.

SV Stsin **Dr. Katrin Suder** (BMVg): Wenn wir von offensiv, von offensiven Fähigkeiten reden, ob sie Aufklärung – Führung, Unterstützung ist hier nicht ganz so relevant – oder Wirkung sind, dann ist es mandatierungspflichtig.

SV **Prof. em. Dr. Michael Bothe**: Vielleicht etwas grundsätzlicher. Natürlich hat das Bundesverfassungsgericht zu Beginn der 90er Jahre nicht daran gedacht. Ich habe damals für die damalige Opposition vor dem Bundesverfassungsgericht plädiert und ich kann Ihnen sagen, ich habe auch nicht dran gedacht. Ich konnte mir das gar nicht vorstellen. Aber nach dem guten alten juristischen Grundsatz, dass man neue Probleme auch mit gesunden, alten Prinzipien behandeln kann, ein kurzer Rückblick. Für das Bundesverfassungsgericht war das Wesentliche, dass die Bundeswehr ein Parlamentsheer ist. So steht das in dem Urteil drin. Infolgedessen muss man von diesem Zweck her denken und eben sagen, heute haben wir militärische Operationen im Cyberraum, die sind echte militärische Operationen, das sind nicht zivile. Nach dem Sinn und Zweck der Parlamentsbeteiligung müssen die unter das Zustimmungserfordernis fallen. Was beispielsweise nicht darunter fällt, ist, wenn einfach nur geübt und geforscht wird. Wenn aber Aktion gegenüber einem anderen Staat oder einem fremden Privatunternehmen da ist, dann sind wir in diesem Bereich, den man als „Einbezug in militärische Operationen" ansehen kann. Das ist Originalton Bundesverfassungsgericht. Also zurück zu den Grundsätzen und von da aus wieder nach vorne.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich knüpfe an die letzte Antwort von Frau Prof. Dreo Rodosek an. Sie haben betont, dass der Schutz und die Abwehr von APT-Angriffen vor allem durch Zusammenarbeit erfolgen können. Ebenfalls haben wir haben aus den Antworten von Dr. Kremer und Staatssekretär Vitt gelernt, dass die Zusammenarbeit sowohl den privatstaatlichen als auch den innerstaatlichen Sektor umfassen muss. Ich würde jetzt meinen Frageblock zunächst auf das Thema Innerstaatliche Zusammenarbeit fokussieren, also das zwischen staatlichen Behörden, und die Frage in den Mittelpunkt stellen, wie die Bundeswehr zu einer Erhöhung der gesamtstaatlichen IT-Sicherheit beitragen kann, ohne ihren verfassungsgemäßen Auftrag in irgendeiner Form zu verletzen. Ich

würde auch das Thema Offensivkräfte erst einmal kurz beiseitelassen. Um auch mal eine Größenordnung zu haben, ist die Einstiegsfrage an die beiden Staatssekretäre: Welche Ressourcen stehen in Ihren beiden Geschäftsbereichen eigentlich im Bereich Cybersicherheit zur Verfügung? Ich denke da speziell an die Frage von CERT, das sie vorher schon kurz angesprochen haben, und an die Frage IT-Forensiker. Können Sie das ungefähr skizzieren, damit wir und die Zuhörer im Blick haben, was im BMVg und was im BMI heute vorhanden ist, bevor wir dann weiter auf die Möglichkeiten der Zusammenarbeit eingehen?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ich würde gerne nochmal ganz kurz auf APT-Schutz und -Abwehr eingehen. Ich würde dazu noch zwei Aspekte erwähnen. Auf der einen Seite ist es natürlich wichtig, dass man solche Angriffe abwehrt oder früh erkennt. Das wird man nicht zu 100 Prozent schaffen. Wenn so ein Schadprogramm eingedrungen ist, ist das Nächste, was dann gemacht werden muss, dass man die Auswirkungen sehr begrenzt hält. Das sind so zwei Themen, die man fokussieren muss. Warum habe ich das jetzt dargestellt? Weil das dann Mindestanforderungen an die IT-Sicherheit sind, die wir in unseren eigenen IT-Einheiten auf der Ebene der Bundesverwaltungen benötigen. Das ist mit der Grund, warum wir die IT-Konsolidierung vornehmen und warum wir die Rechenzentren und die Netze konsolidieren.

Die Frage war, wie wir zusammenarbeiten. Da würde ich erstmal sagen: Um diesen Grundschutz zu erlangen, also frühzeitig zu erkennen und darauf hinzuwirken, dass der Schaden begrenzt wird, wenn der Eindringling drin ist, haben wir dort mit der Bundeswehr, mit dem BMVg eine enge Zusammenarbeit bei der Konsolidierung der Netze. Wie machen wir das? Indem wir uns unsere Netz- und Sicherheitsarchitekturen gegenseitig betrachten und überlegen, wie wir die gemeinsam auf ein vernünftiges Niveau heben können. Da war die nächste Fragestellung. Wie könnte die innerliche Zusammenarbeit bezogen auf die Sicherheit aussehen? Da würden wir uns erstmal ansehen, welche Kompetenzen wir haben und zu welchem Zeitpunkt wir welche Kompetenz bezogen auf die Angriffsszenarien, die da sind, einsetzen würden.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich habe noch nach den Ressourcen gefragt.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ressourcen. Wenn ich jetzt mal bei uns einzeln durchgehe. Ich nehme das BSI, das hat hier den Bereich CERT und Forensik. Im CERT sind beim BSI 17 und bezogen auf Forensik sind es 81 Mitarbeiter. Bei der Bundespolizei haben wir eine Größenordnung von CERT BPOL von 23 Mitarbeitern. Heute sind es 11. Zielsetzung ist 23. Bezogen auf Forensik sind es in den unterschiedlichen Aufgabengebieten ungefähr 100 Mitarbeiter. Im Bundeskriminalamt sind es in Summe 245. Die teilen sich aber auf die unterschiedlichen Aufgabengebiete auf. Ich nenne mal ein paar wie Cybercrime, Cyberspionage oder IT-Forensik. Das wäre ganz grob die Größenordnung.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): In Summe entspricht das etwa 500?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Etwas drunter.

SV Stsin **Dr. Katrin Suder** (BMVg): Auch bei uns die Zahlen. Ich würde jetzt nicht auf die komplette IT-Sicherheitsorganisation eingehen. – die ist natürlich sehr viel größer; so habe ich die Frage auch nicht verstanden –, sondern vor allem auf die CERTs. Im Wesentlichen haben wir hier zwei CERTs. Wir haben das CERT der Bundeswehr. Ich habe es jetzt nicht tages- und FTEscharf dabei, aber es sind ungefähr 50 bis 60 Mitarbeiter. Dann haben wir nochmal das CERT der BWI. Dort sind es etwas weniger. Hier ist vieles auch über einen Dienstleistungsvertrag geregelt. Es sind vielleicht 35 bis 40, wobei das grobe Zahlen sind. Die Forensiker bilden eine kleine Minderheit daraus mit ungefähr zehn Prozent. Das ist jetzt aufs CERT bezogen. Wir haben natürlich eine größere Sicherheitsorganisation, aber so habe ich die Frage verstanden.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Habe ich Sie jetzt richtig verstanden, Sie haben quasi drei CERTs in Ihren Geschäftsbereichen. Zwei der Bundeswehr und eines des BMI.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Wir haben zwei. Einmal das BSI und einmal in der Bundespolizei.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Frau Staatssekretärin! Sie haben gerade schon die BWI angesprochen. Die BWI ist eine Tochter und im Moment noch in öffentlich-privater Partnerschaft. Sie geht Ende des Jahres vollständig in das Eigentum des Bundes über. Damit verfügt die Bundeswehr über eine GmbH, einen IT-Dienstleister. Könnten Sie kurz darstellen, wie die BWI aufgestellt ist, und dann drauf eingehen, welche Aufgaben die BWI in Zukunft sowohl im Bereich des BMVg als auch für andere Bereiche innerhalb der Bundesverwaltung übernehmen soll?

SV Stsin **Dr. Katrin Suder** (BMVg): Die BWI ist, wenn man so will, ein IT-Systemhaus. Das heißt, sie ist nicht als Provider auf das Angebot einzelner Fähigkeiten spezialisiert, sondern sie kann im Grunde als Systemhaus über den kompletten IT-Stack Dienstleistungen zur Verfügung stellen. Sie tut das nicht alles mit eigenen Kräften, sondern sie bindet auch Externe über Unterauftragsnehmerleistungen mit ein. Aber grundsätzlich ist sie ein Systemhaus, das heißt, sie besitzt die Fähigkeit, IT umfassend als Provider zur Verfügung zu stellen. Das ist im Wesentlichen das, was die BWI ist. Sie wird in der Tat eine Inhouse-Gesellschaft. Wir haben gesagt, die Zukunft ist im Grunde zweierlei. Das eine ist, sie wird das zentrale IT-Systemhaus der Bundeswehr. Das ist sie, das wird sie sein und auch bleiben. Sie soll für bestimmte Aufgaben auch mehr Verantwortung bekommen. Das ist das Stichwort, was wir auch schon mehrfach diskutiert haben, wie „grüne" und „weiße" IT in dem Sinne auch zusammenkommen können, weil sie teilweise durch unterschiedliche Kräfte betrieben werden, was nicht unbedingt Sinn macht, weil das Ganze ja sowieso inzwischen größtenteils technologisch verschmolzen ist. Das heißt, die BWI ist und bleibt ein zentraler Anbieter der Bundeswehr, des BMVg für IT-Leistungen.

Zweite Frage. Wie kann das auch anderen zur Verfügung gestellt werden? Wir sind über den IT-Rat und in enger Abstimmung mit dem BMI auch ein Dienstleister des Bundes. Wir wollen, wenn wir denn dann den Übergang in die Inhouse-Gesellschaft geschafft haben, was ein großer Schritt ist, – – Denn man muss sich ja vorstellen, dass eine komplette Gesellschaft mit allen Mitarbeiterinnen und Mitarbeitern jetzt in eine Bundes-Inhouse-Gesellschaft übergeht. Da sind verschiedenste rechtliche und technische Übergänge zu bewerkstelligen. Wenn das hoffentlich erfolgreich geleistet worden ist, dann wollen wir auch die Dienste anderen anbieten. Wir sind hier in enger Abstimmung, was das sein könnte. Das könnten zum Beispiel dezentrale Leistungen sein, denn die Bundeswehr und damit auch die BWI ist in Deutschland eine Flächenorganisation. Das heißt, wir haben hier viele Standorte und damit die Möglichkeit, auch dezentral IT-Leistungen und netzwerknahe Leistungen anzubieten. Das ist eine Fähigkeit, die wir brauchen, die wir haben und die man zum Beispiel auch anderen dezentralen Organisationen anbieten könnte.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Sie haben die beiden großen IT-Projekte der Bundesregierung gerade schon angesprochen. Da ist das Thema IT-Konsolidierung, das sich auf das Thema der Rechenzentren bezieht, und das ist das Thema Netze des Bundes, das sich auf das Thema Weitverkehrsnetze im Wesentlichen bezieht. Mich würde interessieren, welche Rolle die Bundeswehr und das BMVg bei diesen beiden Projekten spielt, insbesondere auch mit dem Blick auf das heutige Thema Erhöhung der Cybersicherheit? Zum Beispiel könnte ich mir vorstellen, dass gerade im Bereich der Netze – und Cyberangreifer kommen ja über Netze – möglicherweise eine intensivere Zusammenarbeit zwischen der Bundeswehr (BWI) und dem BMI mit den anderen Behörden sinnvoll wäre. Sie könnten eine Einschätzung zu dieser Frage abgeben. Dann hätten wir auch nicht das Problem mit Einsätzen usw. und Angriffen, weil das stationäre Netze sind, die in Deutschland irgendwo

unter der Erde liegen. In dem Bereich sehe ich jetzt persönlich eine Zusammenarbeit zwischen BWI und Bundeswehr sowie dem BMI als für unproblematisch an. Wenn da jetzt jemand anderer Meinung ist, kann das auch artikuliert werden. Das war das Thema Netze des Bundes.

Das zweite ist das Thema IT-Konsolidierung. Auch das ist großes Projekt. Macht es da Sinn, in dem Sinne zusammenzuarbeiten, dass die BWI auch ein großer Rechenzentrumsanbieter ist und die Bundeswehr große Ressourcen hat, diese auch der restlichen Bundesregierung teilweise mit zur Verfügung stellt und dafür sorgt, dass das Niveau an Cybersicherheit dann innerhalb der Bundesregierung insgesamt erhöht wird – Stichwort: Kampf um die knappe Ressource Mensch, Fachkräfte werden überall gesucht.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ich fange mit dem Thema Netze des Bundes an. Da haben wir eine enge Zusammenarbeit mit dem BMVg. Wir haben heute unterschiedliche Netze und Netzarchitekturen. Wenn ich mal die Netze des Bundes kurz betrachte, haben wir zurzeit drei Bundesnetze, die wir im ersten Schritt zu einem Netz konsolidieren. Wir wollen mit dem eine neue Technologie haben und eine höhere Sicherheitsgewährleistung. Danach gibt es noch 40 weitere Netze auf der Bundesebene, die wir dann auch konsolidieren.

Die Bundeswehr hat ein eigenes Netz mit einer anderen Netzarchitektur und mit anderen Herausforderungen. Was wir zurzeit machen, ist, dass wir das sehr eng abstimmen. Es gibt ein gemeinsames Architekturboard, wo wir sozusagen diese beiden Architekturen zusammenlegen und dann überlegen, was die beste Lösung ist, um die Netzarchitekturen soweit wie irgend möglich anzunähern und zu einen späteren Zeitpunkt auch Synergien zu heben. Das wird aber ein Prozess über die nächsten Jahre sein.

Bei der IT-Konsolidierung Bund haben wir auch eine enge Zusammenarbeit. Das ist ein Projekt, das aus sechs Teilprojekten besteht. Ein Teilprojekt verantwortet das BMVg. Das ist die Rechtsform von dem zukünftigen Dienstleistungszentrum. Es gibt aber noch weitere Aktivitäten, wo wir eng zusammenarbeiten, zum Beispiel bei der Einführung der elektronischen Akte. Da haben wir uns so abgestimmt, dass wir uns die Produkte auch vom Markt ansehen und die Bundeswehr der Pilot dafür sein wird. Auch bei der Sicherheitskonzepteplattform bei dem Dienstleister des Bundes werden wir unsere Architekturen abgleichen, um zu schauen, was wir tun können, um auf beiden Seiten eine hohes Sicherheitsniveau zu haben.

SV Stsin **Dr. Katrin Suder** (BMVg): Da gibt es jetzt wenig hinzuzufügen. Wenn ich vielleicht noch einmal versuche, das, was wir eigentlich tun, mit einer Systematik zu unterlegen, dann versuchen wir, dass wir Standards gemeinsam miteinander diskutieren und dann ausrollen und durchsetzen. Ich glaube, dass ein großes Sicherheitsproblem – – Und jetzt rede ich tatsächlich nochmal sehr viel stärker auch in meiner Expertenrolle mit meiner Vorerfahrung. Es sind weniger die großen Rechenzentren oder die großen IT-Dienstleister. Die haben ein sehr hohes Sicherheitsniveau, weil es sehr viel zentralisiert und dann auch sehr viel einfacher ist, in Schutz zu gehen – mit all den Schwierigkeiten, aber relativ gesehen. Wenn man dezentrale IT hat, ist das Hauptproblem eigentlich immer der berühmte Server oder, besser gesagt, der Rechner irgendwo unterm Schreibtisch. Das ist genau die Schwachstelle. Das Ganze hier einzusammeln und sicherzustellen, dass wir dort stark konsolidieren, das ist, glaube ich, eine große Herausforderung. Wir bringen da auch unsere Expertise ein und sind da sehr eng abgestimmt, auch in Standardisierungsfragen zu gehen, um zu gucken, dass wir das in Summe vorwärts bekommen.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich möchte nochmal auf die Zusammenarbeit auch im Sicherheitsbereich eingehen. Die Kollegen werden sich erinnern: Wir hatten bei dem Thema WANBw in der letzten Legislaturperiode eine große Diskussion über die BSI-Zertifizierung des WANBw, die nicht erfolgt ist. Vielleicht können Sie uns kurz einen Blick geben, ob das und wie es

auf Ihrer Agenda steht. Vielleicht Frau Dr. Suder oder Herr Vitt – suchen Sie sich es aus.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Da die Zertifizierung bei uns liegt, kurze Darstellung. Ich hatte das eben schon erwähnt, dass die beiden Netze, einmal die Netze des Bundes und dann das Netz der Bundeswehr, eine unterschiedliche Architektur haben. Dort hat es bis jetzt noch keine Zertifizierung durch das BSI gegeben. Es gibt jetzt eine Möglichkeit, diese Zertifizierung durchzuführen, indem man ganz spezielle Verschlüsselungswerkzeuge von deutschen Lieferanten in Ergänzung zu den Routern, die von der Firma Cisco da sind, einsetzt. Heute läuft die Verschlüsselung über Cisco. Da wird eine separate Komponente integriert, sodass die Verschlüsselung in der Hand der Bundeswehr und bei einem IT-Dienstleister aus Deutschland ist. Es laufen gerade die Aktivitäten und die Abstimmung und ich gehe davon aus, dass wir über den Weg die Zertifizierung hinbekommen.

SV Stsin **Dr. Katrin Suder** (BMVg): Keine Ergänzung!

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Dann möchte ich nochmal auch auf das Thema offensive Fähigkeiten zurückkommen. Die erste Frage geht nochmal an Frau Suder. Wir haben diese CNO-Kräfte. Es wäre aus meiner Sicht eigentlich naheliegend zu sagen, wir nutzen diese CNO-Kräfte in Friedenszeiten einfach dafür, als SWAT-Teams zu testen, ob unsere eigene Infrastrukturen und die eigenen Infrastrukturen der Bundeswehr sicher sind. Das heißt, dass man sagt, man baut ein Waffensystem auf, nutzt die eigenen offensiven Fähigkeiten, die man im Bereich der CNO hat, und versucht, in der eigenen Infrastruktur Sicherheitslücken zu finden. Wäre sowas aus Ihrer Sicht denkbar?

SV Stsin **Dr. Katrin Suder** (BMVg): Denkbar ist immer Vieles. Heute haben wir es anders organisiert. Die CERTs sind diejenigen, die die Penetrationstests machen und die sozusagen die Sicherheit in den Waffensystemen usw. herstellen. Dort liegt heute die Verantwortung und dort wird das Ganze ausgeübt. Die CNO-Kräfte agieren in ihren eigenen geschlossenen Netzwerken.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Dann hätte ich zwei Fragen an Herrn Dr. Dickow. Sie haben ja in Ihrem Papier und in Ihrem Statement eine klare Rollenverteilung, was Aufgabe der Bundeswehr und was Aufgabe der restlichen Regierung sein sollte. Jetzt nehmen wir mal den Fall an, eine deutsche kritische Infrastruktur würde von mehreren Servern aus angegriffen, sei es mit Denial of Service, seien es gezielte APT-Angriffe. Man weiß jetzt nicht genau, wo es herkommt. Das Problem der Attribution haben wir immer. Man kennt aber den Server. Jetzt ist der Server vielleicht in einem Umfeld, wo er nicht direkt physisch greifbar ist. Es stellt sich die Frage, ob wir jetzt den Server mit Hilfe eines Cyberangriffs ausschalten und damit den unmittelbaren Angriff unterbinden sollen. Frage an Sie: Wer soll das Ihrer Meinung nach innerhalb der Bundesregierung machen? Soll die Bundesregierung es überhaupt machen?

SV **Dr. Marcel Dickow** (SWP): Meine Präferenz wäre, eher den Angriff zu unterbinden, indem man das Netzt abklemmt, aus dem man angegriffen wird, bzw. die Angriffe technisch auszufiltern, was man in den meisten Fällen relativ gut kann, insbesondere bei DDoS-Attacken. Die Frage ist dann natürlich, welches Ausmaß der Angriff hat, wie stark die eigene kritische Infrastruktur betroffen ist. Ist sie groß betroffen, denke ich, wäre der erste Schritt zu überprüfen, inwieweit das Land, in dem der Server steht, einem auf der Basis von polizeilicher Zusammenarbeit weiter helfen kann. Das ist das, was in der Regel getan wird. Das BKA geht an die entsprechende Stelle oder man geht über EUROPOL oder INTERPOL und versucht das zu machen. Denn es ist ja völlig klar, dass man, wenn man jetzt den Server in diesem Land lahm legt, da auf jeden Fall erstmal die Infrastruktur in einem anderen Land angreift. Völkerrechtlich kann ich das nicht bewerten, aber ich hätte zumindest als Sicherheitspolitiker große Zweifel, dass das die richtige Herangehensweise ist.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Nochmal eine Frage an Sie. Sie sprechen in Ihrem Papier auch über das Attributionsparadigma und ich sehe das als ernsthaftes Problem. Was ich noch nicht ganz verstanden habe, ist, wie Sie Cyberwaffen von Nicht-Cyberwaffen unterscheiden, wie Sie die Trennlinie auch in Bezug auf die Anforderungen bezüglich Attribution ziehen. Wir haben zum Beispiel im Bereich EloKa auch schon immer mal wieder Angriffe mittels elektromagnetischer Wellen, an denen auch kein Absenderschild hängt. Wir haben auch bei anderen Waffen nicht unbedingt immer das Absenderschild auch gleich da. Ich weiß, dass das bei Cyber ein Problem ist, aber bei anderen ist dieses Abgrenzen auch ein Problem. Sie führen dann in Ihrem Papier als Kriterium die Frage der juristischen Verwertbarkeit an: „Dieser Ansatz macht den Angegriffen zum Angreifer und gefährdet die juristische Verwertbarkeit der so erlangten Beweismittel." Meine Frage an Sie wäre, in welchem Szenario jetzt diese juristische Verwertbarkeit unter welchen Kriterien und vor welchen Gerichten und sowas gefährdet wäre? An was denken Sie da?

SV **Dr. Marcel Dickow** (SWP): Es sind natürlich zwei unterschiedliche Fälle. Das eine ist sozusagen die Frage des Völkerrechts und ob man sich auf das Recht der Selbstverteidigung berufen kann. Das andere sind zivilrechtliche bzw. strafrechtliche Verfahren. In letzterem Bereich ist das so, dass forensisch gesammelte Beweise nur dann akzeptiert werden, wenn man einwandfrei nachweisen kann, dass man das System nicht manipuliert hat, während man die Beweise sammelt. Deswegen kopieren Strafverfolgungsbehörden erstmal alle Datenträger, die sie bekommen, grundsätzlich schreibgeschützt und machen dann ihre Forensik, sodass sie belegen können, dass sie Daten auf den erbeuteten Datenträgern nicht manipuliert haben.

In der Vorwärtsverteidigung, wenn ich ein System angreife, von dem ich denke, dass ich von dort aus angegriffen werde, und dort Beweismaterial sammele, was ich völkerrechtlich einsetzen will, um mein Recht auf Selbstverteidigung vorzuführen, wird das natürlich schwierig. Wie gesagt, es gibt dort eine andere Beweislastpflicht. Prof. Bothe wird das noch besser ausführen können als ich. Da ist Völkerrecht und Strafrecht nicht miteinander vergleichbar. Aber das Prinzip bleibt, dass solche Beweise von anderen angegriffen werden können, weil man nicht einwandfrei belegen kann, dass man nur gesammelt, nur beobachtet und nicht selbst auch verändert hat. Wenn man sich in die Systheme anderer begibt, um dort Selbstverteidigung, Vorwärtsverteidigung, Verneverteidigung oder wie man das nennen mag, ausüben will, heißt das heißt letztlich, dass man sich immer in den Konflikt begibt, dass man völkerrechtlich nicht einwandfrei beweisen und belegen kann, dass man von dort aus auch wirklich angegriffen worden ist. Das Problem der Attribution bleibt, selbst wenn man sich in dem System befindet. Zumindest strafrechtlich ist das dann eben nicht verwertbar. Ob es völkerrechtlich hilft? Den Fall hatten wir noch nicht. Ich kenne einen Fall wo wir vermuten müssen, dass eine solche Beweisführung erfolgt ist. Das ist nämlich der Sony-Hack, der angeblich von Nordkorea durchgeführt worden ist. Meine Vermutung ist, dass amerikanische Sicherheitsbehörden das nur wissen können, weil sie sich zum Zeitpunkt des Angriffs bereits im nordkoreanischen System befunden haben. Wir haben keine Details darüber. Das ist nachrichtendienstliche Tätigkeit. Aber das ist die einzige Erklärung, die ich dafür habe.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Die Frage ist, vor welchem Gericht und gibt es das Problem der Attributierbarkeit?

SV **Dr. Marcel Dickow** (SWP): Es gibt natürlich de facto kein ständiges Gericht dafür. Das sind Sachen, die man im Zweifelsfalle dann vor den Vereinten Nationen, insbesondere vor den Sicherheitsrat, bringen muss. Vielleicht müssen wir dafür noch ein Gericht schaffen, aber das kann ich nicht beurteilen. Um auf Ihre andere Frage zurückzukommen: Die Attribution ist tatsächlich immer ein Problem. Das ist in der digitalen Welt vielleicht besonders auffällig. Das gibt es in der konventionellen Kriegsführung auch, nur sind da unsere forensischen Möglichkeiten, die Möglichkeit unserer Aufklärung besser ausgereift,

weil wir uns eben nicht über so global umfassende, umspannende Netze unterhalten, wie das in der IT-Welt der Fall ist. Natürlich können wir zum Beispiel mit Hilfe von Radar beobachten, wenn Flugzeuge in den feindlichen Luftraum eindringen. Solche Mittel stehen uns zumindest in der Güte in der IT-Welt in den Netzen nicht zur Verfügung. Es gibt den theoretischen Ansatz, dass man den gesamten Netzverkehr beobachtet, mitschneidet und dadurch Beweise sammelt, aber das ist sicherlich kein Ansatz, den demokratische westliche Staaten verfolgen wollen, weil das eben bedeutet, dass man die Informationskontrolle über das Internet übernehmen will.

Abg. **Lars Klingbeil** (SPD): Frau Dr. Suder! Ich habe ein paar Fragen zum Thema Personal. Das sehe ich als einen der großen Punkte, wenn wir die Fähigkeiten im Bereich der Bundeswehr besser aufstellen wollen. Es ist damals gesagt worden, es sind bisher knapp 15 000 Dienstposten, die es in der Bundeswehr gibt. Ich würde von Ihnen gerne mal eine Bewertung haben, ob Sie sagen, das ist ausreichend oder ob sie schon Zahlen erarbeitet haben, wohin sich das Ganze entwickeln müsste?

Dann würde ich gerne zum Bereich Personalgewinnung nochmal nachfragen. Sie haben vorhin angedeutet, dass man da was machen muss. Ich würde gerne konkreter wissen, welche Überlegungen es gibt? Wie ist das mit Reservisten und wie ist das mit der Zusammenarbeit mit der Wirtschaft und mit der eigenen Ausbildung? Vielleicht kann auch Frau Prof. Dreo Rodosek für die Bundeswehruniversität dazu was sagen. Das würde mich interessieren. Wenn Sie dazu ein paar Ausführungen machen können.

SV Stsin **Dr. Katrin Suder** (BMVg): Zum Personal war die erste Frage, ob das in der Gesamtheit reicht. Wir haben ja mal in einer Antwort gesagt, wir haben 15 000 Kräfte, die sich mit IT im Weitesten oder in irgendeinem Zusammenhang beschäftigen – ohne die Mannschaftsdienstgrade, sonst wären es 21 000. Diese Zahl ist, glaube ich, in dieser absoluten Höhe grob die richtige. Das ist nicht der Punkt. Sondern der Punkt ist, dass ich vorhin ja gefragt wurde, wieviel IT-Forensiker wir haben. Wenn ich sage vom CERT mit ungefähr 50 Leuten 10 Prozent, dann sind das 5. Da sicher zu sagen, wenn wir von 5 auf 15 gehen, dann wäre das eine Verdreifachung. In der Gesamtheit der Leute sind das aber natürlich nicht unbedingt sehr viele. Worauf ich hinaus will: Ich glaube, spezielle Hochwertfähigkeiten haben wir nicht genug und brauchen wir mehr. Da sind auch solche Dinge dabei wie IT-Architektur. Denn ich habe ja davon gesprochen, dass Schutz ein oberstes Gebot ist. Das ist ganz wichtig und wir alle waren uns einig. Dazu braucht man vor allem auch Architekten – Leute, die verstehen, wo in unserem Netz eigentlich Schwachstellen ganz einfacher Natur sind, wo ich Server habe, die noch gar nicht integriert sind, wo ich Netzübergänge nach außen habe. Dafür brauche ich Leute, die diese IT-Fähigkeiten haben. Insofern reicht das in der Gesamtzahl. Das ist, glaube ich, jetzt nicht unbedingt das Thema. Das fällt da nicht ins Gewicht. Aber reicht das bei den einzelnen Fähigkeiten? Da würde ich sagen: definitiv nicht.

Danke auch für die Gelegenheit, nochmal was zur Personalgewinnung zu sagen. Ich glaube, es gibt nicht *die* eine Maßnahme, mit der man das Qualifizierungsproblem lösen kann. Das gibt es definitiv nicht. Deshalb müssen wir über die Gewinnung und dann aber auch über das Halten der Leute auch mit neuen Mitteln nachdenken. Die Gewinnung ist auch wieder ein Konglomerat. Das hat was mit der Agenda Attraktivität zu tun, die schon vor lange Zeit aufgesetzt worden ist und die genau da reingeht, um zu überlegen, wie wir als Bundeswehr ein attraktiver Arbeitgeber werden können – alles, was damit zusammenhängt. Dann Gewinnung durch eigene Ausbildung und durch eigene Studiengänge. Da würde ich dann gerne auch nochmal den Handover machen wollen. Auch hier müssen wir unbedingt ran, zumal ja auch gerade im militärischen die Regeneration häufig über die eigene Ausbildung und das eigene Studium funktioniert. Insofern Einiges zur Gewinnung.

Dann aber auch Halten. Da ist speziell das Thema Fachkarrieren, was ich vorhin schon mal am Rande erwähnt habe, für mich ein ganz wichtiges.

Was heißt das eigentlich? Fachkarrieren meint, dass auch Menschen, die sich vor allem durch Expertise und Erfahrung auszeichnen, auch eine gewisse Laufbahn haben, wenn sie vielleicht nicht immer in der Führungsverantwortung sind. Denn das ist in Unternehmen immer ein großes Thema; das kenne ich schon aus meiner Vorverwendung. Wenn ich nicht gleichzeitig breite Führungsverantwortung trage, kann ich keine Karriere machen, kann ich nicht aufsteigen. Mit Verlaub und Respekt den Kollegen gegenüber, und ich habe ja selber auch mal programmiert: Gerade in der IT sind es nicht immer unbedingt die, die auch die breiteste Führungsverantwortung haben; sie haben oft komplementäre Skills. Wir brauchen unbedingt Fachkarrieren, um die auch zu halten, auszubilden und denen eine attraktive gute Perspektive bieten zu können.

Das alles wird aber immer noch nicht reichen. Jetzt sind wir bei dem Thema, wie wir eigentlich mit anderen zusammenarbeiten können. Das ist das Thema Reserve. Die Bundeswehr bildet in Summe sehr gute Fähigkeiten, Werte und Menschen aus, die dann auch irgendwann wieder in die Wirtschaft gehen. Das ist auch so ein Drehtürprinzip. Allerdings haben wir natürlich das Reservistenthema nicht mehr so wie früher, als es noch die Wehrpflicht gab. Das heißt, die Anzahl schrumpft. Jetzt geht es, glaube ich, darum zu überlegen, wie von denjenigen, die die Bundeswehr verlassen, weil sie Soldaten auf Zeit sind oder auch aus anderen Gründen, einige bindet, wie man auch speziell solche Reserve auch wieder ausbildet und wie man darüber mit der Wirtschaft und auch mit Universitäten nachdenken kann, anders zusammenzuarbeiten. Ich habe das vorhin schon mal am Rande erwähnt: Das betrifft ja nicht nur uns, das betrifft ja auch das BMI, das betrifft alle anderen. Es würde sich wahrscheinlich mal ein eigenes Expertenpanel dazu lohnen, weil die Frage ja ist, wie wir eigentlich im Staat in Summe die Fachkräfte gewinnen können, ohne dass wir uns die alle immer gegenseitig wegnehmen und in so einen Kampf um die Köpfe kommen. Das ist immer noch nicht umfassend, aber vielleicht habe ich so ein paar Aspekte genannt.

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Ich darf etwas zu den Tendenzen ausführen, die wir an der Universität der Bundeswehr in München erkennen. Es war schon angeklungen, dass wir einen neuen Master Cyber-Security, natürlich aufbauend auf das Informatikstudium, einführen wollen. Die Frage ist jetzt, warum Studierende zu uns kommen sollten. Das Ziel ist, die besten Köpfe, das heißt exzellente Lehre mit exzellenter Forschung zu verbinden und somit die erste Adresse für Cybersicherheit in der Aus- und Weiterbildung zu werden. Wenn wir die besten Professoren gewinnen wollen, beinhaltet das, dass wir auch entsprechende Forschungsmöglichkeiten wie Forschungslabs oder Testlabs haben und dass wir auch zusammen, nicht nur in der Forschung, sondern auch mit der Industrie entlang der gesamten Wertschöpfungskette innovative Sicherheitslösungen entwickeln können.

Abg. **Lars Klingbeil** (SPD): Eine weitere Frage an Frau Dr. Suder. Die Waffensysteme, die wir bisher haben, sind hochgradig technologisch unterwegs. Da wäre meine Frage eigentlich, ob es eine Bestandsaufnahme gibt, wie stark die geschützt sind, bzw. ob es eine Analyse darüber gibt, wieviel Kosten auf uns zu kommen, wenn wir jetzt nachträglich noch alles schützen wollen, um uns technologisch besser abwehren und schützen zu können?

SV Stsin **Dr. Katrin Suder** (BMVg): Ich kenne eine solche umfassende Analyse aktuell nicht. Ich weiß auch nicht, ob sie so einfach durchführbar ist. Denn die Frage ist, welches Schutzniveau ich wie erreichen möchte. Ich habe vorhin schon einmal gesagt, ich weiß von einem anderen Land, das mal versucht hat, so einen Jet auseinander zu bauen und wieder neu zusammenzusetzen, um zu gucken, was man dann eigentlich tun müsste, wenn man ihn wirklich sozusagen from the scratch wieder zusammensetzt. Das sind exorbitante Kosten. Man muss natürlich in gewisser Weise gucken, wie man über die verschiedenen Hebel ran geht. Ich habe es versucht, vorhin zu sagen. Ich glaube, ein zentraler Hebel liegt darin, dass wir nicht immer alles bis ins letzte Detail analysieren und testen können. Das wird so nicht gehen. Wir müssen uns auf Zertifizierungen ver-

lassen können. Wir müssen Mechanismen finden, wo wir auch dort wieder shared resources bilden, seien das zum Beispiel die von Herrn Dr. Kremer angesprochenen Testcenter. Wir sind darauf aus, dass wir das gemeinschaftlich machen und nicht jeder für sich alleine immer wieder dieselben Fragen stellt, denn Computerchips sind ja überall drin. Die sind nicht nur in unseren Waffensystemen drin, sondern auch in Autos, die sind ja überall. Die Frage ist, wie wir damit gesamtgesellschaftlich umgehen. Wir haben für uns das bislang so beantwortet, was ich vorhin grob skizziert habe, indem wir sowohl also über die Zulieferstrukturen gehen, dort auch bestimmte Standards festschreiben, das aber auch selber testen, dann im Ganzen selber über die Prozesse gehen und anschließend auch noch mal Penetrationstests machen. Ich kenne keine Kostenabschätzung. Ich sehe auch eine gewisse analytische Herausforderung, das komplett anzugehen, weil wir natürlich auch das Thema haben mit den unknown unknowns – das sind ja genau wieder die APTs –, wo ich gar nicht genau weiß, wie man das letztendlich quantifizieren sollte. Aber vielleicht das erstmal als Antwort.

Abg. **Lars Klingbeil** (SPD): Dann eine Frage an Herrn Prof. Rid und Herrn Dr. Dickow. Wenn man sagt, man verzichtet auf Offensivfähigkeiten, dann rückt auch der Bereich Abschreckung unmittelbar stärker in den Fokus. Da wäre meine Frage an Sie, welche Instrumente der Abschreckung Sie auch aus anderen Ländern kennen und was Sie an Fähigkeiten empfehlen würden?

SV **Prof. Dr. Thomas Rid** (King's College London): Die Frage der Abschreckung ist ganz eng mit der Frage der Attribution verknüpft, also des Herausfindens, wer dahinter steckt. Und es ist einfach wichtig an der Stelle nahe an den technischen Realitäten zu bleiben. Attribution findet, wie ich schon sagte, sehr oft in der Praxis statt. Wir haben Reports mit sehr hoher Sicherheit, Beispiel APT1, in dem zuerst eine amerikanische Firma und später das Justizministerium sowie das FBI ganz klar eine chinesische PLA-Unit mit dem Titel 61398 identifiziert haben, was nicht mal die Chinesen zum jetzigen Zeitpunkt in Frage stellen. Wichtig ist, wenn man sich anschaut, wie sich bestimmte APT-Operationen entwickeln, nachdem sie öffentlich gemacht wurden, dann sehen wir verschiedene Reaktionsmuster – manchmal nur die Operation selber, ohne ein Land zu nennen. Aber das ist Teil der Abschreckung. Die Operation wird öffentlich gemacht, dann gibt es in der Regel eine upfile. Es gibt viele Beispiele, die ich konkret nennen könnte. Abschreckung ist hier eher wie Abschreckung von Kriminalität zu sehen, wo wir davon ausgehen, dass danach – nicht wie im Kalten Krieg; Abschreckung: keinen Nuklearkrieg – – Sondern hier heißt Abschreckung, dass man Aktivitätsniveaus beeinflussen kann, leicht runter drücken kann, aber mit Sicherheit nicht komplett auf null drücken kann.

SV **Dr. Marcel Dickow** (SWP): Ich bin skeptisch, was das Thema Abschreckung angeht. Denn selbst wenn wir nachträglich Attribution in einigen Fällen erlangen, – – Wir sehen ja die Angriffe, wir sehen auch immer neue, und wir wissen, dass wir zumindest bei den bekannten Fällen im Schnitt 200 Tage brauchen, um überhaupt zu identifizieren, dass wir angegriffen wurden. Die Tatsache, dass man sich so gut verbergen kann, dass man sich solange in gegnerischen Systemen aufhalten kann, ohne entdeckt zu werden, ist so für alle Seiten, by the way, attraktiv, dass Abschreckung offensichtlich nicht funktioniert. Ja, natürlich werden die Angriffe dann nach der Entdeckung zurückgefahren. Aber das heißt nicht, dass man nicht in der nächsten Woche, im nächsten Monat, im nächsten Jahr einen neuen Angriff startet, der eben anders funktioniert, der noch nicht entdeckt ist. Also ich sehe nicht, dass Staaten erfolgreich andere Staaten davon abgehalten haben, im Cyberbereich anzugreifen, wenigstens nicht auf nachrichtendienstlicher Ebene. Es ist halt ein offenes Spielfeld und wenn man entdeckt wird, dann wechselt man den Spieler aus und wechselt einen neuen ein.

Abg. **Lars Klingbeil** (SPD): Sehen Sie eine Notwendigkeit völkerrechtlich Änderungen vorzunehmen oder Verabredungen zu treffen?

SV **Dr. Marcel Dickow** (SWP): Da bin ich schon

wieder als der Nicht-Völkerrechtler gefragt. Ich bin geneigt zu sagen, dass wir mit dem bestehenden Völkerrecht nicht alle Probleme tatsächlich erschlagen können. Wir haben gewisse Phänomene, die in der klassischen Welt eben vorhanden sind, die aber in der digitalen Welt anders aussehen. Ich bin mir nicht hundertprozentig sicher, ob wir dann wirklich ein neues Völkerrecht oder eine Anpassung dafür brauchen. Ich sehe halt, dass wir uns mit bestimmten Phänomenen wie eben der Attribution oder dem Problem der Selbstverteidigung einfach sehr schwer tun. Aber ich habe keine Idee, wie ein neues Völkerrecht aussehen könnte.

Abg. **Lars Klingbeil** (SPD): Ich würde die Frage nochmal an Prof. Bothe weitergeben.

SV **Prof. em. Dr. Michael Bothe**: Die Frage ist gerade in einer Arbeitsgruppe der Generalversammlung der Vereinten Nationen diskutiert worden, wo sich die Befürworter einer stärkeren staatlichen Kontrolle und stärkerer Kontrollpflichten und die Befürworter eines free flow of information noch gegenüberstehen. Die völkerrechtliche Lösung liegt dann letzten Endes in der Entwicklung von Strukturen der Zusammenarbeit der Staaten, die dann letzten Endes gemeinsam solcher Probleme Herr werden müssen. Und da gibt es in der Tat Möglichkeiten und Bedarf an neuen Regelungen. Denn es ist so, dass die Möglichkeit, einem anderen zu schaden, ja was Attraktives an sich hat. So ist die Welt. Auf der anderen Seite ist es so, dass auch jeder selbst betroffen ist. Aus dieser Ambivalenz der Interessen – und das ist nun keine IT-Spezialität – ergibt sich dann auch häufig die Möglichkeit, doch zusammenzuarbeiten, insbesondere bei einem Zurückdrängen von krimineller und privater Aktivität, wo letzten Endes ein gemeinsames Interesse der Staaten da ist, dieses zu kontrollieren und zurückzudrängen. Kurz gesagt: neues Völkerrecht – ja, schon. Aber angesichts der Gegensätze, die wir da haben, wird das eher in Richtung von Zusammenarbeit gehen müssen.

Abg. **Rainer Arnold** (SPD): Ich würde gerne Staatssekretär Vitt nochmal zu Personalgewinnung fragen. Gibt es Überlegungen, die Personalstruktur, sprich Eingruppierungen im Bereich IT-Spezialisten, perspektivisch anzupassen oder zu verändern, um wettbewerbsfähig zu sein?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Es gibt jetzt keine konkreten Überlegungen. Ich versuche mal das Thema von einer anderen Seite zu beleuchten. Frau Dr. Suder hat das vorher erwähnt. Die IT-Konsolidierung, die wir in den Rechenzentren vornehmen, hat unterschiedliche Aspekte, zum Beispiel die Erhöhung des Sicherheitsniveaus und ein attraktiver Arbeitgeber zu sein. Wenn ich heute eine IT-Fachkraft vom Markt bekommen möchte, muss ich ein paar Voraussetzungen erfüllen. Eine Voraussetzung ist, dass der Arbeitgeber attraktiv ist. Wann ist ein IT-Arbeitgeber attraktiv? Wenn er innovativ und groß ist, so dass ich mich spezialisieren kann. Das nächste Thema was wichtig ist, ist Vereinbarkeit von Familie und Beruf. Dies hat gerade in den letzten zwei Jahren einen unheimlich hohen Stellenwert bekommen. Dann eine realistische Einschätzung, weil ich beide Welten kenne. Bezogen auf IT-Spezialisten und -Fachkräfte werden wir im öffentlichen Bereich, nicht das Gehaltsniveau erreichen, wie in der Wirtschaft. Wenn das so ist, muss man schauen, welche anderen Möglichkeiten es gibt, um attraktiv zu sein. Da gibt es unterschiedliche Möglichkeiten, Frau Dr. Suder hat das bei der Personalgewinnung dargestellt: Enge Zusammenarbeit mit Universitäten und möglichst frühes Binden von IT-Fachkräften an die Organisation. Das sind die Möglichkeiten.

Abg. **Dr. Alexander S. Neu** (DIE LINKE.): Die beiden Fragen von vorhin stehen ja noch im Raum. Ich möchte sie aber noch um zwei Fragen ergänzen. Das eine ist, als Opposition hat man natürlich kein grenzenloses Vertrauen in die Regierung und auch nicht in das BMVg. Und wenn wir von isolierten Cyberangriffen reden – ob das nun in der Realität seitens der Bundeswehr stattfindet oder ob das nur eine Option ist, sei mal dahingestellt – ist es ja nicht so, dass man das kontrollieren kann. Es ist nicht so, dass ein Flugzeug über die Grenze fliegt, dass Truppen verlegt werden, was irgendwo kontrollierbar,

feststellbar ist. Das kann man eben im Cyberraum nicht. Das heißt also, die Parlamentarier können nicht von sich aus feststellen, ob die Bundeswehr einen Cyberangriff fährt oder nicht. Welche Maßnahmen sind gewissermaßen denkbar, um da die Kontrollfähigkeit des Bundestages, des Verteidigungsausschusses gegenüber dem BMVg zu erhöhen? Wäre da zum Beispiel die Möglichkeit von „Red Card Holdern" gegeben, also dass man jemanden in Rheinbach installiert, der mit darauf achtet, dass da nichts passiert, was nicht passieren darf? Welche Überlegungen gibt es dazu? Gibt es dazu überhaupt Überlegungen? Es ist schon von großem Interesse, dass wir da als Parlamentarier bei isolierten Cyberangriffen, wenn sie denn stattfinden sollten, auch eine Kontrollmöglichkeit haben. Das ist die eine Ergänzungsfrage.

Die andere geht nochmal zurück auf die Frage Verteidigung. Herr Prof. Bothe hat von vorbeugenden, also präventiven Maßnahmen gesprochen. Das ist völkerrechtswidrig, sagt er. Präemptiv ist nochmal eine andere Geschichte. Präemptives, unmittelbares Zuvorkommen ist im Völkerrecht weitgehend anerkannt. Herr Prof. Bothe! Ist das Sich-Einnisten in fremde Netze eine präventive oder eher eine präemptive Maßnahme? Kann man das in diesem Falle genau differenzieren? Und hat das bereits seitens der Bundeswehr stattgefunden, Frau Dr. Suder? Gibt es also schon Fälle, wo die Bundeswehr sich dementsprechend in fremde Netze eingehackt hat, um dort präventiv oder präemptiv, wie auch immer, zu agieren? Wie bewerten Sie das vor dem verfassungs- und völkerrechtlichen Aspekt? Danke.

SV **Dr. Katrin Suder** (BMVg): Offen war, glaube ich, noch das Thema äußere und innere Sicherheit sowie Amtshilfe. Zum einen ist Amtshilfe in diesem Sinne temporär angelegt, was vor allem für diejenigen, die Amtshilfe leisten, etwas bedeutet. In diesem Falle wären wir dies. Das bedeutet, dass wir das nicht strukturell vorhalten. Der Begriff „temporär" kann dann aber auch durchaus länger sein. Soweit ich weiß, ist der jetzt nicht mit einem Zeitstamp versehen, aber da bewege ich mich jetzt auf Glatteis.

Grundgesetz anpassen. Herr Vitt hatte darauf, glaube ich, schon geantwortet. Im Moment sehen wir das nicht, diskutieren das auch nicht, aber natürlich kann es sein, dass man zu Punkten kommt. Ich persönlich glaube es jetzt nicht; ich bin aber Physikerin, keine Juristin. Denn bei der Amtshilfe, was wir ja gesagt haben, oder auch beim gemeinsamen Schutz kritischer Infrastrukturen, wie wir es auch am Beispiel der Sicherheit im Luftraum haben, sehen wir ja, dass wir das auch nicht benötigt haben. Insofern wäre meine Antwort darauf: Nein.

Jetzt war noch vom letzten Mal das Thema Vorneverteidigung offen. Und dazu würden wir dann gleich nochmal gemeinschaftlich antworten, Herr Bothe. Zum einen ist das hier eine öffentliche Anhörung. Ich bin hier als Expertin und nicht, um Details der taktischen oder sonstigen Operationsführung der Bundeswehr zu diskutieren. Davon würde ich jetzt Abstand nehmen wollen. Ich will aber trotzdem die Frage auf einer Ebene höher beantworten wollen. Das Konzept heißt dann eher nicht Vorneverteidigung, sondern Active Defence, ist aber wahrscheinlich ungefähr dasselbe. Es gibt ja auch hier eine große Sprachverwirrung, weil wir im Neuland sind und dann gibt es immer Sprachverwirrungen. Das ist zurzeit keine Planung. Das ist auch nicht das, was wir vorsehen. Es gibt aber eine Studie dazu, die ihnen ja, glaube ich, auch zugegangen ist. Insofern gibt es natürlich immer wieder Gedanken darüber, dass man auch ständig überprüft, was eigentlich zulässig, was technisch möglich ist und wie sich dieser Raum zu gestalten hat.

Also das waren jetzt, glaube ich, alle Fragen vom letzten Mal und eingewoben das, was sie mich jetzt noch zusätzlich gefragt haben. Wenn wir jetzt zum Thema Kontrollfähigkeit kommen. Wir sind ja auch rechtlich, juristisch kontrolliert. CNO ist das. Sie haben mich gefragt, ob das denkbar ist. Denkbar ist immer vieles, das habe ich vorhin schon gesagt. Aber ich denke, es gibt hier ja auch schon ganz konkrete Methoden. Das passiert ja alles nicht im rechtsfreien Raum. Insofern kann ich es jetzt nur so sagen. Alle weiteren Modelle kann ich mir gerade nicht konkret vorstellen, das müsste man alles erstmal rechtlich

prüfen. Aber es ist ja nicht so, dass das rechtsfrei ist und dass da nicht auch Juristen und Rechtsberater und alles Mögliche dabei sind. Es ist ja nicht so, dass da einfach irgendwelche Menschen sitzen, die irgendetwas tun.

SV **Prof. em. Dr. Michael Bothe**: Vielleicht gerade im Anschluss daran. Kontrollfähigkeit. Da geht es ja auch um Kontrollwilligkeit im Sinne der Bereitschaft, kontrolliert zu werden. Meine Erfahrung aus der Beobachtung unseres politischen Systems ist eher, dass Mogeln letzten Endes wenig Erfolg versprechend ist und dass darum, so sehe ich das, durchaus schon immer Bereitschaft bestanden hat, egal welche Partei die Regierung innehatte, mit der Opposition im Sinne einer Kontrolle und der Fähigkeit, Kontrolle herzustellen, zusammenzuarbeiten. Das ist immer mal auch unter Beachtung von Geheimschutz gemacht worden und teilweise auch mittels persönlicher Kontakte von Mitgliedern der Regierung mit Funktionsträgern der Opposition getan worden. Ich glaube, das ist eine gute Tradition. Da wäre ich nicht so pessimistisch.

Mein Hauptpunkt ist: Sprachverwirrung. Es gibt zum einen, technisch gesehen, Selbstverteidigung im Sinne des Artikels 51 der Satzung der Vereinten Nationen. Die ganzen Beispiele, die hier diskutiert wurden, haben damit nichts, aber auch gar nichts zu tun. Hier geht es dagegen um gegenseitige „Unnettigkeiten", die völkerrechtlich nicht egal sind. Wenn sich ein Staat in das Regierungs-IT-System eines anderen Staates einnistet, so stellt sich hier die Frage des Respekts der Souveränität dieses anderen Staates und das ist, ich sage mal, jedenfalls rechtlich problematisch. Ich würde es in der Regel als einen unzulässigen Eingriff in die staatliche Souveränität des anderen Staates und damit als ein völkerrechtliches Delikt ansehen. Dieses völkerrechtliche Delikt löst nicht ein Recht auf Selbstverteidigung mittels militärischen Gegenschlags gemäß Artikel 51 der Satzung der Vereinten Nationen aus, sondern etwas anderes, nämlich ein Recht auf Gegenmaßnahmen, auf Maßnahmen, die an sich rechtswidrig wären, die aber als Antwort auf ein vorheriges Unrecht mit dem Ziel gerechtfertigt sind, dafür zu sorgen, dass dieses Unrecht abgestellt wird. So lautet die relevante Vorschrift der Artikel, die die International Law Commission der Vereinten Nationen zur Frage der Staatenverantwortlichkeit entwickelt hat. Diese Gegenmaßnahmen sind zulässig. Sie stehen unter einem ganz wesentlichen Vorbehalt, nämlich dem Vorbehalt der Verhältnismäßigkeit. Solche Gegenmaßnahmen sind Antwort auf vorheriges Unrecht. Das ist also die erste Frage, wo man dann natürlich auch Beweisschwierigkeiten hat. Dazu komme ich gleich. Ein vorheriges Unrecht ist also die erste Voraussetzung. Und dieses Sich-Einnisten wird in der Regel ein solches Unrecht sein. Zweitens das Ziel, dafür zu sorgen, dass das Unrecht abgestellt wird. Und drittens die Verhältnismäßigkeit.

Um dann auf die Frage der Streitregelungen und der damit verbundenen Beweisschwierigkeiten zu kommen. Niemand wird es zugeben, nicht wahr. Damit sind wir bei der Streitregelung und in einem etwas pathologischen Bereich der internationalen Beziehungen. Es gibt Staaten, die die obligatorische Zuständigkeit des Internationalen Gerichtshofes gegenüber allen Staaten, die das gleiche getan haben, anerkannt haben. Die Bundesrepublik gehört dazu. Wenn dieser Streit zwischen Großbritannien oder Italien und der Bundesrepublik entstehen würde, dann könnten wir vor den Internationalen Gerichtshof ziehen und umgekehrt. Die Zahl dieser Erklärungen liegt so bei 70. Es gibt also viele Staaten, bei denen dieser Weg nicht funktioniert. Da gibt es alle möglichen anderen Wege wie internationale Streitschlichtung; da sind der Phantasie recht wenig Grenzen gesetzt.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Ich möchte nochmal auf meine erste Frage von vorhin zurückkommen, diese an sie, Herr Staatssekretär, nochmal stellen, und ein bisschen präzisieren. Wenn ich jetzt die Äußerungen der letzten Monate, gerade aus dem BMVg, lese und höre – nicht alles offen, einiges eingestuft –, dann habe ich schon den Eindruck, dass beispielsweise bei der Frage nach dem Schutz kritischer Infrastruktur doch nicht so ganz klar zu trennen ist, wann eigentlich das BMI und wann das BMVg mit den jeweiligen Behörden federführend zu-

ständig ist. Denn es gibt natürlich militärische Hard- und Softwares und es gibt zivile Software, die sowohl militärisch, als auch zivil genutzt wird. Für welche kritische Infrastruktur ist denn jetzt das BMI und für welche Bereiche das BMVg zuständig? Und ist das alles wirklich so klar oder gibt es hier nicht doch an der einen oder anderen Stelle den Bedarf, das noch weiter zu präzisieren?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Mit dem IT-Sicherheitsgesetz sind ja die Betreiber kritischer Infrastrukturen entsprechend eingeordnet worden. Das sind sieben Sektoren, um die es dort geht. Das ist zum Beispiel Telekommunikationsindustrie, Wasser und Versorgung und so weiter. Bezogen auf diese kritischen Infrastrukturen – da kommt jetzt die Rechtsverordnung – sieht es wie folgt aus: Da ist das BSI der eindeutig erste Ansprechpartner – bezogen auf Mindeststandards, die definiert werden und bei denen zu einem späteren Zeitpunkt verifiziert wird, ob sie eingehalten werden.

Das zweite Thema ist die Meldepflicht bezogen auf kritische Sicherheitsfälle. Da erfolgt die Meldung von dem Betreiber der kritischen Infrastruktur in Richtung des BSI – auch eindeutig geregelt –, dieses bewertet das, wird dann entsprechend der Situation weitere Aktivitäten durchführen und informiert nach der Bewertung die anderen Betreiber der kritischen Infrastrukturen, sodass sie rechtzeitig Vorsorge treffen können. Die Verantwortlichkeiten sind eindeutig geregelt.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Meine nächste Frage an Sie, aber auch an Frau Staatssekretärin Suder. Wir haben ja vorhin auch von Herrn Prof. Rid gehört, wie schwierig das für die Experten in Tallinn war, sich darauf zu einigen, ob Stuxnet eigentlich ein bewaffneter Angriff war oder nicht. Was sind denn die Kriterien nach denen die Bundesregierung entscheidet, ob es sich um einen bewaffneten Angriff handelt, wenn beispielsweise ein Cyberangriff verübt werden würde? Welche Qualität muss der haben? Welche Kriterien müssen dafür erfüllt sein?

SV Dr. **Katrin Suder** (BMVg): Da schiele ich so ein bisschen in Richtung von Prof. Rid. Nach meinem Wissen gibt es keinen sozusagen anerkannten Kriterienkatalog, auf den sich alle geeinigt hätten – weder innerstaatlich noch gesamtstaatlich. Man kann jetzt auch darüber spekulieren, warum das so ist. Wenn man das tun würde, würde man ja auch die Grauzone rausnehmen und wir haben ja vorhin mehrfach gehört, warum das von vielen nicht die Absicht ist. Es gibt erste Versuche von Sachverständigen, Kriterien aufzustellen. Einzelne haben wir vorhin auch schon gehört. Es geht ja auch darum, dass es eine gewisse Wirkung haben muss. Auch den zeitlichen Aspekt hatten wir vorhin schon. Es gibt einzelne Kriterien, aber es gibt keine anerkannten. Die gibt es ja übrigens ansonsten, nach meinem Wissen, auch nicht. Das heißt, das ist hier ein Thema, was wir grundsätzlich haben. Ich glaube, das Thema ist in dem Sinne dann größerer Natur. Und wenn es zu einem Incident, zu einem Vorfall kommt, wird man immer den Kontext betrachten müssen und sollen, wenn ich das so sagen darf. Und genau dazu dient ja auch das Gewaltverbot, dass es nicht zu einem Automatismus kommt, sondern dass da auch hohe Schwellen gesetzt sind. Aber da müssen Sie jetzt entscheiden, ob wir nochmal weitergehen oder nicht.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Ich würde gerne mit einem Stichwort weitermachen. Der Kollege Arnold hat, glaube ich, vorhin Herrn Dr. Kremer gefragt. Entnetzung, Frau Dr. Suder. Was heißt denn das für die Bundeswehr? Gab es da in den letzten Jahren schon den großen Versuch, Systeme, die am Netz sind, vom Netz zu nehmen, um sie gegen Angriffe von außen sicherer zu machen? Oder ist das etwas, was in den nächsten Jahren, dann auch prioritär, noch gemacht werden soll?

SV **Dr. Katrin Suder** (BMVg): Es gibt bereits heute getrennte Netze. Wir haben ja auch die sogenannten „roten Netze", die geheime Netze sind und die natürlich nicht offen zugänglich sind, die auch gewisse Übergänge haben. Wir haben auch Offlinesysteme – und zwar etliche. Das heißt also, viele Waffensysteme sind selbstverständlich nicht einfach im Internet und online. Das ist ja

bereits Entnetzung. Das dient ja bereits dazu, dass Waffensysteme nicht nur gehärtet, sondern in dem Sinne auch gar nicht zugänglich sind. Insofern ist das bereits heute ein Mechanismus, nach dem wir auch agieren.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Dann würde ich gerne nochmal zu der Frage von vorhin zurückkommen, die wir auch schon diskutiert haben. Isolierte Cyberoperationen. Ich überspitze das jetzt mal. Sie haben vorhin, glaube ich, wenn ich Sie richtig verstanden habe, gesagt, es gebe dafür dann natürlich auch ein Mandat des Deutschen Bundestages. Jetzt ist ja rein aus dieser militärischen Sicht das besonders Attraktive an solchen Cyberoperationen, dass die Attribution eben nicht sofort sichtbar ist, dass diese Operationen natürlich im geheimen, versteckt stattfinden. Und man könnte sich jetzt ja für so eine Aktion wie Stuxnet nicht vorstellen, dass es dazu vorher die Mandatsberatung im Bundestag gebe. Wenn sie vielleicht nochmal erklären könnten, was sie mit „eine reine Cyberoperation würde auch natürlich der Mandatierungspflicht unterliegen" meinten?

SV **Dr. Katrin Suder** (BMVg): Ehrlich gesagt: Genau das, was ich gesagt habe. Es wurde ja auch im Grunde nochmal durch die Auslegung des Juristen bestätigt. Ein Parlamentsbeteiligungsgesetz hat ja auch nicht jedes Land, aber wir haben es, und es sieht genau das vor. Wenn man es so auslegt, wie Prof. Bothe es angeboten hat – und ich würde mich dem anschließen –, ist es so, dass das mandatierungspflichtig ist.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Dann hätte ich noch eine Frage an Prof. Rid. Sie hatten ja auch schon mehrfach darauf abgestellt, dass es extrem große Eskalationsdynamiken gibt, die Sie ja jetzt auch schon sehen und die wir in der Vergangenheit gesehen haben. Sehen Sie denn irgendeine Möglichkeit, politische Maßnahmen oder rechtliche Maßnahmen zu ergreifen, um diese Eskalationsdynamik wenigstens ein Stück weit einzudämmen?

SV **Prof. Dr. Thomas Rid** (King's College London): Rechtliche Maßnahmen halte ich in dem Bereich für extrem schwierig. Reden wir von politischen Maßnahmen, weil viele dieser Operationen, wo wir eine Eskalation sehen, explizit designt sind, um in graue Bereiche reinzufallen. Eine Industriespionage in großem Stil ist hier ein Beispiel. Man kann rechtlich nicht dagegen vorgehen und muss entsprechende Sicherheitsmaßnahmen umsetzen, um dann etwas tun zu können. Die Eskalationsdynamiken – – Übrigens finde ich es schon bemerkenswert, wie wenig führende oder überhaupt Unternehmen, deren Namen einem international einfallen, es in Deutschland gibt, die sich im Bereich IT-Sicherheit, Incident Response oder Threat Intelligence da herumtreiben. Ich hatte es kurz am Ende meines Eingangsstatements erwähnt. Ich meine, ich bin bei diesen ganzen Konferenzen. Ich bin in der Regel einer der ganz wenigen Deutschen. Manchmal gibt es da noch den einen oder anderen Hacker, die da unterwegs sind, aber Unternehmensvertreter ganz selten. Das ist ein großes Problem. Man könnte da viel mehr Venture Capital in den Sektor reinbringen, entsprechende Förderprogramme auflegen, dass man in Deutschland einfach ein bisschen Startup-Szene anfüttert, dass sich da was entwickelt, mit dem man dann arbeiten könnte. Es gibt ja einige sehr gute Hacker; in der Hacking-Kultur sind wir ja gar nicht schlecht unterwegs.

Und nur abschließend nochmal. Dieser Punkt Attribution ist extrem wichtig. Wenn wir die ganze Zeit an Dritte, zum Beispiel russische Operateure in diesem Feld, die Message senden, dass wir, sozusagen, unrealistische, geradezu märchenhafte Standards an Attribution anlegen, dann ist natürlich der Subtext: Ihr könnt uns den ganzen Tag lang hacken, wir werden nie sagen, Ihr wart es.

Abg. **Agnieszka Brugger** (BÜNDIS 90/DIE GRÜNEN): Dann hätte ich noch eine Frage an Herrn Dr. Kremer, weil Sie in ihrem schriftlichen Statement nochmal von der Gefahr der wiederverwendbaren Cyberwaffen, auch aus der Sicht der Wirtschaft, geschrieben hatten. Wie groß sind denn ihre Sorgen, wenn eben immer mehr Staa-

ten militärisch offensive Fähigkeiten erlangen – das ist ja schon Realität –, wenn das sozusagen der Trend der nächsten Jahre ist. Zum Beispiel ist es ja auch bei Stuxnet so, dass der Code ja nicht von Anfang an veröffentlicht worden ist. Aber er hat sich eben verbreitet und konnte dann auch von anderen kriminellen, nichtstaatlichen Akteuren genutzt werden. Welche Sorgen macht Ihnen dieses Thema? Und was wäre Ihre Antwort darauf?

SV **Dr. Thomas Kremer** (Telekom AG): Zunächst einmal vorausgeschickt: Ich bin nicht in der Lage festzustellen, ob ein Angriff auf meine Netze von einem Staat oder von einer kriminellen Organisation kommt. Ich kann nur feststellen, von welchem Server und aus welchen Land er kommt. Insofern bin ich da auf der technischen Ebene etwas mehr limitiert als andere, die zusätzlich über andere Kenntnismöglichkeiten verfügen. Wie ist das mit der Wiederverwendbarkeit? Das ist eigentlich ganz einfach. Wenn Sie sich das mal an einem traditionellen Beispiel vor Augen führen. Wenn Sie irgendwo in eine Bank einbrechen und Hammer und Schweißgerät mitnehmen, um das zu machen, und hinterher auf der Flucht sind, dann lassen Sie das Zeug meistens zurück. Dann ist es weg und kann auch nicht mehr eingesetzt werden. Das ist bei den Cyberwaffen deutlich anders. Die sind einfach noch da. Die gehen nicht weg. Wenn die einmal erfunden sind und im Netz agiert haben, sind die noch da. Damit bilden sie natürlich eine Basis für Kriminelle, um diese zum Beispiel sozusagen als Fonds, als Basis zu nehmen und weiterzuentwickeln. Das ist, je nachdem welche Malware es ist, etwas komplizierter. Manchmal ist es etwas einfacher. Insofern: Ja, natürlich haben wir davor Sorge, dass diese Themen aufkommen; darum habe ich das auch reingeschrieben. Nur muss ich mich mit der Realität abfinden, dass das so ist. Was einmal im Internet ist, kann ich nicht wieder verschwinden lassen. Das ist eine der ganz großen Grunderkenntnisse, die man im Internet hat. Und dazu muss man einfach schauen, dass die entsprechenden Abwehrmaßnahmen dem aktuellen Stand entsprechen. Gerade bei den Advanced Persistent Threats muss man sich klar machen, dass die traditionelle Vorstellung, die wir alle noch haben – nach dem Motto, ich baue eine tolle Firewall dahin und die aktualisiere ich alle fünf Minuten – es nicht bringt. Damit kann ich diese Art von Angriffen gar nicht abwehren. Ich brauche eine Second Line of Defence und diese Second Line of Defence sind verhaltensgesteuerte Systeme, die beobachten, wie sich die Systeme bei mir im Netzwerk verhalten, ob sie sich normal verhalten oder ob sie abweichende Verhaltensweisen zeigen. Sobald sie abweichende Verhaltensweisen zeigen, bin ich sehr gut beraten, wenn ich mir das ganz genau angucke, was sie machen. Dafür halten Unternehmen wie zum Beispiel die Deutsche Telekom Hunter Teams vor, die genau die Aufgabe haben, sich merkwürdig agierende Systeme genau anzusehen.

Abg. **Reinhard Brandl** (CDU/CSU): Ich würde meinen dritten Block unter die Überschrift Schlüsseltechnologien stellen. Und ich würde jetzt mal ganz breit mit einer Frage an Frau Suder beginnen. Wie und in welchen Feldern haben Sie vor, den Wissenstransfer zwischen der Bundeswehr auf der einen Seite und der Wirtschaft und der Wissenschaft auf der anderen Seite in Zukunft zu fördern und zu forcieren, damit die Bundeswehr im Bereich Cybersicherheit auch eigene Kompetenzen aufbauen kann?

SV Stsin **Dr. Katrin Suder** (BMVg): Wenn man mal als Strukturierungselement – jetzt nicht das, was ich vorhin schon beantwortet habe, da bin ich ja über den IT-Stack von Hardware, Betriebssystem bis hoch zur Software gegangen – eine Wertschöpfungskette von Cyber und IT nimmt, dann könnten wir sagen, wir haben Planung, Konzept, Forschung bis zum Prototyping, wir haben die Entwicklung, Muster, Beschaffungen, Produkte und die Nutzung. Wenn man das mal als strukturierendes Element nimmt, dann ist die Idee genau gewesen, speziell in dem Teil Forschung und Entwicklung Startups reinzubringen; wir haben es eigentlich gerade auch schon gehört. Also dort, wo sie dann eben auch kraftvoll wirken können, wo sie auch Schlüsseltechnologien sind, wo wir in Deutschland auch viele Fähigkeiten haben, dort auch gezielt darauf zurückzugreifen und die systematisch in so einer Idee des Cyberclusters mit einzubringen.

Wir müssen dann auch gucken, wo wir Großunternehmen und Mittelstand mit reinnehmen können. Das geht sicher weiter, denn die sind ja auch sehr gut darin, aus einem Muster Skalierungen zu machen und dann auch wieder Lösungen, nach denen wir alle suchen, gesamtstaatlich zur Verfügung zu stellen. Also, insofern würde ich sagen, es kommt so ein bisschen darauf an, wo wir sie genau brauchen.

Wenn wir jetzt zum Thema Planung und Konzept ganz zum Anfang gehen, sind wir da bei der Forschung, bei den Universitäten, und auch bei Instituten und Laboren. Insofern würde ich sagen, wir müssen über die ganze Wertschöpfungskette hinweg denken und dann über den ganzen IT-Stack und dort vor allem wieder im Bereich Krypto; das habe ich auch vorhin schon gesagt, das möchte ich jetzt nicht wiederholen. Denn wie wir es auch vorhin beim WANBw gehört haben, gibt uns das dort die Chance, dass wir dann im Grunde um eine Technologie, die wir nicht selber herstellen, die wir deshalb auch nicht selber vollends kontrollieren können, sozusagen im abstrakten Sinne eine Kapsel legen, um aber wieder sicherzugehen, dass wir geschützt und gesichert sind, soweit das funktioniert. Vielleicht das als kursorische erste Antwort.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Gut. Dann würde ich weiter gehen. Wir haben im letzten Jahr die Schlüsseltechnologiedebatte gehabt und es gibt ein Strategiepapier der Bundesregierung zur Stärkung der Verteidigungsindustrie in Deutschland, vom Kabinett am 8. Juli 2015 beschlossen. Es fällt auf, dass Cyber über alle Fähigkeitsbereiche hinweg als nationale Schlüsseltechnologie in Deutschland mit eingestuft ist. Ich weiß, dass das BMVg bei dem Papier der Bundesregierung gemeinsam, glaube ich, mit dem Wirtschaftsministerium federführend war. Ich würde einleitend fragen, Frau Staatssekretärin, ob Sie ein bisschen was zur Genese des Papiers sagen können und welche Zielrichtung Sie damit verfolgen? Was soll denn passieren, wenn eine Technologie nun als Schlüsseltechnologie mit eingestuft ist?

SV Stsin **Dr. Katrin Suder** (BMVg): Vielen Dank für die Frage. In der Tat war der Kerngedanke dahinter, dass wir uns bei begrenzten finanziellen Ressourcen, aber auch Manpower-Ressourcen überlegen, wie wir priorisieren – und dort haben wir begrenzte Ressourcen. Beim Priorisieren war die Frage, was wir an Technologien national, also in Deutschland, vorhalten müssen, um den Auftrag der Bundeswehr sicher erfüllen zu können. Da steckt natürlich auch eine sicherheitspolitische Komponente drin, aber das war die Kernfrage. Und deshalb ist Cyber in der Tat quer über alle Dimensionen, also Führung, Aufklärung, Wirkung und Unterstützung, gemeint, weil wir in allen Dimensionen sicherstellen wollen, dass wir diejenigen sind, die sicher kontrollieren können, welche Daten wohin fließen. Also die Idee war, dass wir begrenzte Ressourcen haben, es nicht alles Schlüsseltechnologie sein kann und es auch keinen Sinn macht, alles national vorzuhalten – schon allein bei begrenzten Ressourcen nicht, aber auch inhaltlich nicht. Wenn man zum Beispiel, nur um das zu illustrieren, mal in den Bereich der Dreh- und Starrflügler geht, dann haben wir dort bereits eine europäisch ausgerichtete Industrie, die übrigens nicht zum Nachteil des deutschen Standortes war. Das heißt, die Idee war: Wie priorisieren wir? Was brauchen wir unbedingt, um unsere Fähigkeiten, unseren Auftrag sicher erfüllen zu können? Und deshalb war genau die Idee, dass wir dann aber bei vernetzter Operationsführung Verschlüsselung, Krypto und Cyber über alle Dimensionen hinweg haben; und das sieht man in genau diesem Papier. Soviel zur Definition. Es sind wenige Schlüsseltechnologien. Ansonsten wäre es ja auch keine Priorisierung. Denn es ging vor allem ja auch darum zu sagen, was wir denn nicht national vorhalten müssen.

Jetzt sind wir bei den Gebieten. Und dann haben wir uns ressortübergreifend auf diese Gebiete geeinigt. Das wurde ja im Kabinett verabschiedet, wie Sie gesagt haben. Welche Maßnahmen folgen jetzt daraus? Das sind natürlich zuvorderst auch Forschung und Entwicklung. Das heißt, dass wir natürlich überlegen müssen, wie wir die Forschungsbudgets aus unserem Haus, aber auch übergreifend gezielt auf nationale Schlüssel-

technologien, die jetzt aber erstmal aus dem Verteidigungsbereich stammen – das wird ja dann noch ergänzt, auch um den Sicherheitsbereich allgemein – einsetzen, um dann auch dort zu forschen und national vorzuhalten. Das nächste ist Beschaffung. Das heißt, die Beschaffungsentscheidungen, die wir bei uns selber anstellen, sind natürlich davon betroffen. Dann geht es um Export. Und ein ganz wichtiger letzter Hebel ist auch noch, wenn wir in den Bereich des M&A gehen, also Mergers and Acquisitions, das heißt Unternehmensfusion, Unternehmensverkäufe – es gibt ja auch gerade einen, der groß in der Diskussion ist, wo es um Sensorik geht; das ist auch eine Schlüsseltechnologie – – Ich denke, überall dort, wo Schlüsseltechnologien betroffen sind, ist für uns das Strategiepapier in dem Sinne handlungsleitend.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Ich habe jetzt eine Reihe von Fragen, die jeweils an mehrere Sachverständige gerichtet sind, wo mich auch der Vergleich der Einschätzungen zwischen den Sachverständigen interessiert. Und es sind immer die Sachverständigen, die auch einen technischen Hintergrund haben. Ich bitte deswegen um präzise Antworten, damit wir auch vergleichen können, wie die Einschätzungen in den verschiedenen Bereichen sind.

Die erste von diesen Fragen ist, was Sie als nationale Schlüsseltechnologie ansehen? Der Fokus ist der Bereich Cybersicherheit. Und möglichst präzise, ob zum Beispiel Schlüsseltechnologien auf Ebene von Routern, Gesamtsystemkompetenz, Netzwerktechnik zu sehen sind? Oder ist es tiefer angesiedelt? Ist dort ein Bereich? Haben Sie Quellen dazu, die man auch verwenden kann? Wie sehen Sie das? Zur Beantwortung dieser Frage, was Schlüsseltechnologien sind, würde ich Frau Dr. Suder, Herrn Vitt, Frau Prof. Dreo Rodosek und Herrn Dr. Kremer bitten. Was sehen Sie jeweils als nationale Schlüsseltechnologien? Und ich würde vielleicht Frau Dr. Suder bitten zu beginnen, da Sie ja das Papier wesentlich mitverfasst haben. Dann Herr Vitt, Frau Prof. Dreo Rodosek und Herr Dr. Kremer.

SV Stsin **Dr. Katrin Suder** (BMVg): Ich habe im Grunde schon versucht, es auszudrücken. Wir haben vor allem vernetzte Operationsführung, wir haben das Thema Krypto und Verschlüsselung und wir haben das Thema Sensorik. Wenn wir jetzt natürlich eins tiefer reingehen, dann gibt es eine Vielzahl von Einzeltechnologien, die sich im Wesentlichen entlang des Stacks orientieren. Ich glaube, dass wir dort vor allem darüber reden müssen, wie wir bestimmte Betriebssysteme haben, damit wir auf der Softwareseite etwas beherrschen. Da rede ich jetzt nicht von Office-Betriebssystemen, sondern von anderen, also Microkernels. Wir müssen dann darüber reden, wie wir bestimmte Übertragungstechnologien beherrschen können. Wenn wir weiterkommen, ist das letztendlich natürlich unsere eigene Anwendungslandschaft. Das heißt, das sind Führungssysteme, Operationssysteme, Navigationssysteme, die wir selber beherrschen müssen, um Sensorik und um Aufklärung betreiben zu können. Soweit kursorisch. Man kann es natürlich auch immer granularer geben, aber ich würde versuchen, es so zu strukturieren.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ich würde es kurz wiederholen. Netzwerk wäre eine Schlüsseltechnologie, dann Verschlüsselungstechnik selbst und dann bezogen auf Mikroelektronik im Sicherheitskern, sozusagen das, was auf der untersten Ebene verbaut wird, dass man dort auch die Sicherheit entsprechend direkt mit berücksichtigt.

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Ich würde mich anschließen. Das heißt im Prinzip: Krypto, Sensorik als Basis und natürlich zu wissen, was genau in den einzelnen IT-Komponenten enthalten ist, aber natürlich auch in der Entwicklung weiterer anwendungsorientierter, beispielsweise anomaliebasierter, Systeme, IDS usw.

SV **Dr. Thomas Kremer** (Telekom AG):Jetzt werden Sie sich nicht wundern, wenn von mir jetzt nach den drei Vorrednern auch nicht viel Neues kommt. Ich würde sagen, für mich ist das Thema Verschlüsselung besonders wichtig und auch da

das Thema Einfachheit in der Handhabung. Denn wir haben in Deutschland sehr viele Verschlüsselungstechnologien, wir haben allerdings zum Teil auch sehr hochkomplexe. Und wenn sich das durchsetzt, ist das Thema Einfachheit in der Handhabung ein ganz wichtiges Kriterium.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Die zweite Frage in der Richtung wäre, in welchen Bereichen Sie Deutschland besonders gut aufgestellt sehen und in welchen Bereichen wir national einen Nachsteuerungsbedarf haben, wo wir sagen, das wäre für Sie eine Schlüsseltechnologie, die wir aber national nicht vorhalten können? Und vielleicht machen wir die Reihenfolge jetzt genau umgekehrt, dass vielleicht Herr Dr. Kremer beginnt und Frau Dr. Suder am Ende dran ist.

SV **Dr. Thomas Kremer** (Telekom AG): Ich glaube, bei dem Thema Sicherheit unserer Netze sind wir, jedenfalls bei der Telekommunikation, international gut aufgestellt; das ist ok. Wie gesagt, bei dem Thema Krypto sehe ich Deutschland auch in der Spitzengruppe in Europa. Das was mir mehr Sorgen macht, ist die Entwicklung der Cybertechnologie im Allgemeinen. Wir hatten hier in Berlin vor drei Wochen eine Konferenz von Start-ups zum Thema Cybersecurity. Das erste, was auffiel, war, mehr als 50 Prozent der Unternehmen kamen aus Israel und wir hatten aus Deutschland von 20 gerade mal 3, die aus diesem Land kamen. Da sehe ich auch ganz persönlich aus eigener Erfahrung irgendwo Handlungsbedarf, wenn wir nach vorne kommen wollen. Und das ist nicht nur das Thema, wie ich Start-ups anziehen kann, das heißt, wie ich sie fördern kann. Sondern wenn ich das Pflänzchen mal bei mir habe, geht es dann auch um das Thema, wie ich es weiter wachsen sehen kann und wie ich es dann auch bei uns halten kann. Das sind dann alles Fragen, mit denen wird uns auseinandersetzen müssen.

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Dann ergänze ich. Was brauchen wir und was haben wir nicht? Wir haben schon gesagt, Router werden wir nicht neu entwickeln, weil wir die Ressourcen dazu einfach nicht haben. Aber es gibt neue Netztechnologien, Software-defined Networking, die es quasi ermöglichen, dass wir Netze „programmieren". Wenn sich die Technologie in die Weite ausbreitet, dann haben wir quasi eine Büchse der Pandora, da wir ganz neue Sicherheitsanforderungen bekommen. Sowohl SDN selbst zu sichern, aber auf der anderen Seite auch, wie kann SDN dazu genutzt werden, um die Sicherheit zu erhöhen. Ein anderer Bereich. Auf was wir sicherlich fokussieren sollten, ist die Entwicklung innovativer Sicherheitslösungen, die unseren hohen Sicherheitsstandards entsprechen. Das heißt, bauen wir diesen Nukleus, diesen Schild bzw. solche Lösungen, die wir dem Endanwender im Sinne von „Keep it simple" oder „Security as a service" anbieten können.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ich würde wieder die Verschlüsselungstechnik nehmen, würde da aber noch eine Ergänzung machen, was wichtig ist in der Diskussion. Ich nehme jetzt mal das Beispiel Netzwerk. Frau Suder hatte das ja vorher auch dargestellt. Wir werden in dem Routermarkt aus Deutschland keine Firma mehr haben, die maßgebliche Marktanteile gewinnen wird. Aber die Frage ist, was kann ich tun, dass das Netzwerk aus unserer Sicht trotzdem sicher ist. Das bedeutet, die Hersteller von Routern zu motivieren, Schnittstellen offenzulegen, sodass wir unsere Verschlüsselungstools dort integrieren können. Das Gleiche kann ich mir für Betriebssysteme vorstellen. Das Gleiche kann ich mir für Datenbanksysteme vorstellen; denn wir haben auch in den Bereichen in Deutschland, bis auf eine, keine Firmen mehr werden, die große Marktanteile haben, sodass man dort Verschlüsselungstechnologien integrieren kann. Das wäre ein Ansatz. Auch wenn ich in einem Bereich wie Netzwerke sage, das ist eine Schlüsseltechnologie, haben wir in Deutschland aber kein Unternehmen, das einen signifikanten Marktanteil hat, die Sicherheit trotzdem zu gewährleisten. Und dann noch diese Sicherheitskernel, die Mikrokerntechnik. Das wären die beiden Themen.

SV Stsin **Dr. Katrin Suder** (BMVg): Jetzt bleibt nicht mehr viel übrig, außer zu wiederholen. Ich möchte vielleicht nochmal einen kleinen Akzent

setzen; und das ist einfach nur nochmal ein Ergänzen. Ich glaube, gerade die komplexen Datenanalysefähigkeiten, also alles das, was damit zu tun hat – Threat Intelligence, also auf der Metaebene analysieren –, ist ja gerade auch diese Startups-Welt, und ich glaube, da haben wir einen starken Nachholbedarf und das wäre wichtig, dass wir auch dort fördern.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meine nächste Frage richtet sich an Frau Prof. Dreo Rodosek und Herrn Dr. Kremer. Es geht darum, der Staat, also hier im Moment vertreten durch BMVg und BMI, kann auch mit Investitionsmitteln, mit Forschungsmitteln die Entwicklung von Technologien anstoßen. In einem Idealfall wäre es zum Beispiel so, dass sich BMI und BMVg zusammentun würden, würden sagen: das ist jetzt eine Schlüsseltechnologie; die brauchen wir zum Beispiel für unser eigenes Netz; in die investieren wir; in die Entwicklung dieser Technologie investieren wir, und die Wirtschaft würde dann davon profitieren, indem sie die Entwicklungsergebnisse eines sicheren Produktes beispielsweise Made in Germany auch mit nutzen kann. Halten Sie das Konzept, so wie ich es jetzt geschildert habe, grundsätzlich für erfolgversprechend? Kann der Staat diese Entwicklungen in dem Bereich mit den Ressourcen, die er hat, anstoßen? Wenn ja, in welchen Bereichen soll er das machen? Und bei welchen Bereichen, sagen Sie, macht es überhaupt keinen Sinn, wenn der Bund jetzt nochmal 10 Mio. in die Entwicklung eines Routers investiert; denn da werden wir überhaupt keine Chance haben, auf dem Markt ein konkurrenzfähiges Produkt, und sei es mit Bundesförderung, zu entwickeln?

SV **Prof. Dr. Gabi Dreo Rodosek** (UniBw M): Auf jeden Fall. Dass, wie Sie geschildert haben, der Staat, die Anschubfinanzierung für das Cybersicherheit-Cluster liefert, um innovative Wertschöpfung durch die ganze Wertschöpfungskette anzustoßen; das war auch in meinem Eingangsstatement dargelegt. Also die Antwort ist klar: Ja. Wo? Sicherlich in den Teilen, die für unsere Verteidigung wichtig sind, das heißt, für unsere Abwehr, Erkennung von APTs, Sensoren, Big-DataAnalytics, das heißt, Analyse großer Datenmengen, um relevante Informationen zu extrahieren, also Smart Data, und zusätzlich in der Entwicklung von Sicherheitslösungen, nicht nur für den Staat, sondern auch für die Endanwender, für die Endverbraucher, da wir ja immer mehr in der digitalen Gesellschaft leben.

SV **Dr. Thomas Kremer** (Telekom AG): Meine subjektive Antwort würde in erster Linie so aussehen, dass ich sage, die wesentlichen Investitionen, die wir hier tätigen können, ist die Investition in Menschen; denn gut ausgebildete Fachkräfte sind das, was uns hier in Europa langfristig am weitesten nach vorne bringt. Also wenn ein Staat fördert, wäre ich sehr dafür, dass er das Thema Ausbildung, Weiterbildung gerade im Cyberbereich sehr stark unterstützt. Und ein anderer Bereich ist, glaube ich, dass wir noch mehr Intelligenz für das Thema Testing brauchen. Das heißt für die Situation, wo wir selber eben nicht mehr die Basistechnologie haben. Der Router ist jetzt schon, ich weiß nicht wie oft, hier durch die Gänge und die Hallen gelaufen. Der wird dann eben von anderen gebaut. Aber unsere Kernkompetenz muss dann darin liegen, wie können wir rauskriegen, wie sicher das Gerät ist. Also Standardisierungen von Sicherheitslösungen, Testing, das sind alles Dinge, wo wir uns auf Dauer wirklich verstärken und wirklich auch behaupten wollen. Und ich glaube, das Thema Verschlüsselung ist jetzt auch schon mehrfach genannt worden.

Abg. **Dr. Reinhard Brandl** (CDU/CSU): Meine nächste Frage richtet sich an die beiden Staatssekretäre. Wie kann sichergestellt werden, dass Entwicklungen, die von Staatsseite aus gefördert werden, konvergent laufen und dass dieser Effekt, dass tatsächlich auch die private Seite davon profitiert, was angeschoben worden ist, auch eintritt? Ich habe es vorher schon mal erwähnt. Mein Negativbeispiel aus der Vergangenheit, aus Ihrer beiden Voramtszeiten ist das Thema BWI und das Thema BSI-Zertifizierung des WANBw. Wir hatten damals die Situation, dass wir auf der einen Seite ein Amt haben, nämlich das BSI, das wunderbare Standards und hoch fachlich und „alles super" aufstellt, und auf der anderen Seite haben wir das größte Netz innerhalb der Bun-

desregierung; und das größte Netz erfüllt diese Standards nicht. Eigentlich wäre es mein Ziel zu sagen, wir haben auf der einen Seite das BSI im Geschäftsbereich des BMI, das die Standards definiert, und auf der anderen Seite die Bundeswehr als großer Nachfrager, die genau in diesen Bereichen dann auch investiert und damit in Deutschland Produkte schafft, die diese Sicherheitsstandards auch miterfüllen. Jetzt habe ich zum Thema WANBw schon gefragt. Jetzt würde ich eine andere Technologie, an der Sie es vielleicht darstellen können, herausstellen; das ist das Thema Cloud-Technologie. Auch da ist es so, dass die BWI, die Bundeswehr, im Bereich Cloud entwickelt. Da ist es so, dass im Bereich gemeinsame IT des Bundes, Teilprojekt 6, IT-Konsolidierung, ein eigenes Cloud-Vorhaben stattfindet. Und auch da ist es so, dass das BSI Sicherheitsstandards durchführt. Mir wäre jetzt daran gelegen, dass Sie darstellen, wie die Zusammenarbeit zwischen den Beteiligten im Idealfall aussehen kann und soll.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung):Ich fange mal mit dem letzten Thema Cloud an. Da geht es ja darum, bezogen auf Cloud-Technologien, in welchem Bereich es sinnvoll wäre, eine Cloud einzusetzen – da gibt es wieder zwei, eine Public und eine Private Cloud, also eine öffentliche Cloud von einem externen Betreiber – oder intern selbst eine Cloud aufzubauen. Wenn man betrachtet, was es bedeutet, intern eine Cloud aufzubauen; es ist nichts anderes, als eine hochgradige Standardisierung mit einem hohen Grad der Automatisierung in der Bereitstellung von – – Um das mal ganz plastisch zu machen: Angenommen Sie haben einen E-Mail-Account bei Google, dann haben Sie null Chancen, diesen E-Mail-Account für sich individuell auszuprägen. Und das bedeutet einfach hochgradige Standardisierung.

Dann ist die nächste Frage, in welchen Bereichen würden wir Clouds aufbauen? Da sind wir in der engen Abstimmung mit dem BMVg. Da werden wir zum Beispiel in der Office-Umgebung, das heißt, in der Büro-, Arbeitsplatz- und Kommunikationsumgebung eine Cloud aufbauen. Da werden wir uns abstimmen. Das wird eine Private, eine interne Cloud sein. Dann würden wir uns andere Bereiche vornehmen und sagen, wo es sinnvoll ist, gemeinsame Standards für Plattformen wie die Office-Umgebung festzulegen, und dann gucken, dass wir die gleichen Technologien einsetzen. Das muss natürlich von den Anwendungen bei den anderen Bereichen auch passen. Also: Cloud, da haben wir ein Teilprojekt 6, haben eine enge Abstimmung mit dem BMVg, um uns dorthin zu entwickeln, weil wir gerade am Anfang stehen. Es hat noch keiner wirklich implementiert.

Sie hatten noch gefragt, da wollte ich noch ganz kurz drauf antworten, wie kann sichergestellt werden, dass man Entwicklungen gemeinsam macht. Ich glaube wichtig ist die Grundlage, dass wir mal die Schlüsseltechnologien festgelegt haben. Und wenn dürfte es ja nur in den Bereichen sein. Die sind für uns wichtig, die sind priorisiert; und da gibt es ja einen detaillierten Katalog, der ziemlich weit runtergeht. Und bis jetzt, glaube ich, ist es uns gut gelungen, dass wir nicht in den unterschiedlichsten Bereichen investieren und das abgestimmt machen.

SV Stsin **Dr. Katrin Suder** (BMVg): Dem gibt es jetzt nicht so viel hinzuzufügen. Ich kann dem nur zustimmen, was Herr Vitt gesagt hat, und glaube, es ist klar, das BSI ist die Standardisierungsentität. Wir haben dann auf Staatssekretärsebene und runterkaskadiert auf verschiedenen Ebenen gemeinsame Runden, wo es dann gilt, das Ganze dann auch Top-down als Strategiepapier festzulegen und für die Umsetzung zu sorgen. Und ja, natürlich! Es kann alles immer konvergenter sein, es kann immer alles schneller und besser sein; aber ich glaube, wir haben es jetzt so aufgesetzt, dass wir es auch gut und gemeinsam umsetzen können. Da gilt es dann zu balancieren. Das ist ja immer das Thema, was wir haben, wenn sie Standardisierung und Zentralisierung haben; dass sie gleichzeitig die Geschwindigkeit aufrechterhalten müssen, weil es natürlich nicht passieren darf, dass sie ständig darauf warten, dass das eine, sozusagen die Standardisierung, die Zentralisierung, da ist und sie müssen aber heute mit den Problemen leben, die Sie im Alltag haben. Aber ich glaube, das geht

am besten über das Miteinander und den Austausch. Und da, finde ich, sind wir auf dem guten Weg.

Abg. **Gerold Reichenbach** (SPD, Ausschuss Digitale Agenda): Ich habe zunächst zwei Fragen. Die eine ist nochmal eine Nachfrage an Prof. Dr. Rid. Sie haben vorhin ausgeführt, dass Deutschland beim Sicherheitsthema hinterherhängt. Können Sie das noch ein bisschen ausführen und spezifizieren?

SV **Prof. Dr. Thomas Rid** (King's College London): Ich greife in Beantwortung Ihrer Frage auch mal das Thema Schlüsseltechnologien auf. Deutschland ist ja aufgrund des NSA-Untersuchungsausschusses, der besonderen Art und Weise, wie Deutschland mit diesem großen Skandal umgeht, in einer besonderen Situation. International wird Deutschland, denke ich, als das Land gesehen, in dem Datenschutz, Privatheit aufgrund der in doppelter Hinsicht besonderen Vergangenheit in Deutschland am meisten wert ist. Darin steckt natürlich im Bereich Schlüsseltechnologien auch eine Chance für Deutschland. Alle haben bisher Kryptografie als zentrale Schlüsseltechnologie hervorgehoben. Bei Kryptografie geht es um Vertrauen. Krypto ist eine Vertrauenstechnologie. Und wir haben ja jetzt gerade eine große Vertrauenskrise – mit dieser hochgekochten Apple-FBI-Geschichte, auch in Großbritannien mit dem Draft Investigatory Powers Bills, einem neuen Gesetz, das auch höchst kontrovers ist. Ich spitze es mal zu: Wenn Deutschland heute zum Beispiel eine Cryptocurrency, also eine kryptografische Währung wie Bitcoin – aber halt richtig gemacht und vernünftig aufgegleist und staatlich gefördert usw. – auf den Markt bringen würde, dann wäre Deutschland in einer ganz besonders guten Position gerade aufgrund seiner besonderen Situation in dieser ganzen Debatte. Also dieses Problem „Deutschland hängt hinterher", wenn Sie so wollen, könnte man auf den Kopf stellen und als große Gelegenheit neuinterpretieren.

Abg. **Gerold Reichenbach** (SPD): Wobei mein Eindruck ist, die Debatte über Trust ist in den USA inzwischen auch ganz heftig im Gang. Ich habe eine zweite Frage, da geht es eher an die Völkerrechtsexperten und an die beiden betroffenen Ministerien, also Innen- und Verteidigungsministerium. Vorhin wurde drüber geredet, bei Cyberangriffen, Intrusion und ähnlichem ist ja völkerrechtlich nicht so ganz klar, ob dies auch als Angriff zu werten ist. Nur hatten wir ja, ich glaube, von Estland ausgehend, vom estnischen Außenministerium damals bei dem Angriff auf die Netzsteuerung und auf die Kraftwerke dort mal die Debatte gehabt, ob dies denn völkerrechtlich eine neue Qualität ist und als Angriff zu werten ist. Jetzt drehe ich nochmal eins weiter. Also ein Stuxnet-Angriff, der in einem Land zwei Kernkraftwerke zum Durchdrehen bringt; also das wäre garantiert einer Waffenwirkung gleichzusetzen. Jetzt kriegen wir aber völkerrechtlich, wenn ich das richtig verstehe, ein Problem. Vorhin wurde gesprochen, wir haben im Darknet so eine Art Cyberwaffenindustrie – teilweise auf PPP-Basis, also Public-private-Partnership, mit kriminellen Strukturen – die aber diese Waffenbaukästen auch für andere anbietet. Wenn dieses Kraftwerk jetzt von einer privaten Organisation aus welchen Gründen auch immer zum Super-GAU gebracht wird, dann wäre es völkerrechtlich ein krimineller Akt, also eine polizeiliche Zuständigkeit. Wenn dies ein Geheimdienst oder ein militärischer Dienst eines fremden Landes wäre, wäre es völkerrechtlich wohl ein Angriff. Wenn es eine private Organisation wäre, von der das jeweilige Land und die Regierung dieses Landes nichts weiß, wäre es wiederum ein polizeiliches Thema. Wenn es eine private Organisation wäre, von der die Regierung des Landes aber weiß und sie gewähren lässt, wäre es völkerrechtlich wohl wieder ein Kriegsakt. Da würde ich jetzt gerne mal von den Völkerrechtlern wissen, wie denn diese Abgrenzung, die rechtstheoretisch offensichtlich relativ einfach geht, sich dann in der Praxis realisieren soll?

Und die zweite Frage. Wie soll denn sowohl bei der Prävention, als auch dann anschließend bei der Bekämpfung die Aufgabenzuteilung zwischen den beiden potenziell betroffenen Ministerien, also dem für die Strafverfolgung zuständigen Innenministerium im polizeilichen Bereich

und dem für die Landesverteidigung zuständigen Verteidigungsministerium im anderen völkerrechtlichen Bereich, passieren? Da hätte ich gerne von Ihnen mal eine Einschätzung; denn mir ist bislang immer noch nicht klar, ob da diese klassische Trennung überhaupt noch funktioniert.

SV **Prof. em. Dr. Michael Bothe**: Sie muss funktionieren! – Nein, es ist natürlich wesentlich ernster. Wir könnten ja doch an der Struktur der Welt, so wie sie ist, nicht einfach vorbeigehen. Es gibt Staaten, und die Staaten haben Regierungen. Und dann gibt es nichtstaatliche Akteure, die sind keine Regierungen und sind rechtlich unterschiedlich zu behandeln. Das ist eigentlich ziemlich grundlegend. Daran ändert auch das Phänomen der Digitalisierung nichts. Was wesentlich ist, ist die Frage einmal der Zurechnung. Das ist schon eine Tatfrage. Sie haben gesagt: „gewähren lässt". Da gibt es nun unterschiedliche Varianten. Das kann eine positive Anleitung sein, dann hätten wir genug Grund zur Zurechnung. Es kann aber auch einfach sein, dass die staatlichen Organe, die eigentlich kontrollieren müssten, dazu nicht in der Lage sind, was leider vorkommt. Dann gibt es keine Grundlage für eine Zurechnung. Das wäre aber ein Bereich, in dem die Staaten handeln und bei ihren Kontrollmaßnahmen zusammenarbeiten müssten. In diese Richtung gehen auch die Arbeiten der Vereinten Nationen.

Zur Qualifikation als bewaffneter Angriff: Sie setzt, darüber besteht wohl Einigkeiten, voraus, dass ein erheblicher physischer Schaden entstanden ist. Man sollte aber mit der Behauptung, dass ein bewaffneter Angriff in diesem Sinne von einem bestimmten Staat ausgegangen ist, sehr vorsichtig sein. Ich habe vorhin das Beispiel von Stuxnet gebracht. Man ist sich zum ersten nicht darüber einig, ob der dadurch entstandene Schaden so erheblich ist, dass die Schädigung einem bewaffneten Angriff entspricht. Zum zweiten ist die Zurechnung unklar. Ein militärischer Gegenschlag auf Verdacht, etwa gegen Israel als einen vermuteten Urheber, kommt da rechtlich nicht in Betracht.

In solchen unklaren Fällen ist polizeiliche Zusammenarbeit gefragt, zum Beispiel über Interpol, um notwendige Beweise zu erlangen. In eine solche Richtung müssen praktische Lösungen gehen. Die theoretische Konstruktion von bewaffnetem Angriff und militärischer Selbstverteidigung trifft auf einer abstrakten Ebene zu. Praktisch und konkret müssen solche Fälle des Verdachts staatlicher Schädigungsmaßnahmen im Cyberraum mit Augenmaß behandelt werden.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ja, ich wollte den zweiten Part übernehmen. Ich nehme jetzt wieder das Beispiel Kernkraftwerke: Prävention und Bekämpfung. Da war ja die Frage: Ist das eindeutig geregelt? Kernkraftwerke gehören zu dem Sektor Energie bei den Betreibern kritischer Infrastruktur. Damit fallen die unter das neue IT-Sicherheitsgesetz. Das heißt, wenn so ein Vorfall eintreten würde, dann würde das BSI informiert. Das BSI würde bezogen auf die Kritikalität das Cyberabwehrzentrum informieren. Da sind die einzelnen unterschiedlichen Einheiten wie BKA und Bundespolizei beteiligt. Dort wird dann die Lage bewertet; wird überlegt, welche Maßnahmen ergriffen werden – BSI unterstützt den Betreiber? wird es eine polizeiliche Maßnahme? kann es sein, dass das BKA aktiv wird? –; dann würden die anderen Betreiber in dem Sektor über das BSI informiert, wenn die Bewertung vorgenommen worden ist. Das heißt, die Zuständigkeit und die weiteren Aktivitäten liegen eindeutig beim BSI. Im Cybersicherheitsrat ist auch das BMVg vertreten. Wenn ich nochmal auf die Prävention zurückgehe: Für die Betreiber kritischer Infrastrukturen sind Mindeststandards für die IT-Sicherheit definiert worden. Das ist sehr konkret ausgeprägt. Jetzt gibt es eine Übergangsfrist. Nach der Übergangsfrist wird das auch verifiziert und überprüft.

Abg. **Rainer Arnold** (SPD): Ich würde gerne mal den Politikberater um Rat bitten. Wir haben insbesondere von Herrn Dr. Rid gehört, da ist die nachrichtendienstliche Aufgabe; gleichzeitig machen die Streitkräfte ähnliches, zumindest, wenn es um Informationsbeschaffung geht, und kooperieren auch eng, insbesondere im Ausland.

Meine Frage an den Politikberater wäre: Brauchen wir nicht noch ein Instrument, um das, was sich in der Bundeswehr, möglicherweise auch im Bereich von Nachrichtengewinnung und Kampffähigkeiten im Cyberbereich, tut, parlamentarisch so zu kontrollieren, wie es bei uns bei den Nachrichtendiensten eingeführt ist? Haben wir dort eine Lücke? Oder ist das geklärt?

SV **Prof. em. Dr. Michael Bothe**: Wenn eine Lücke besteht, dann ist es an Ihnen, sie zu schließen, nämlich dafür zu sorgen, dass zwischen dem Kontrollgremium für die Geheimdienste und den Ausschüssen, die bei der parlamentarischen Zustimmung beraten, eben nichts hindurchfällt. Das ist eine genuine parlamentarische Aufgabe. Sie haben Recht! Wir haben zwei unterschiedliche Verfahren; natürlich! Aber sie sind beide in den Händen des Parlaments, und es ist die Aufgabe des Parlaments, dafür zu sorgen, dass da nichts hindurchfällt.

SV **Dr. Marcel Dickow** (SWP): Das ist tatsächlich eine spannende Frage; denn so klar, wie man im konventionellen Fall den Einsatz von Streitkräften definieren kann – Truppen rücken irgendwohin, sind bewaffnet, erfüllen ein Mandat und gehen zurück – kann man das im Cyberbereich nicht so sehr. Ich habe ja geschildert, dass es da einen Graubereich gibt. Den könnte man sozusagen mandatieren, mandatieren lassen; das wäre die eine Variante. Die andere Variante wäre eher in Richtung nachrichtendienstliche Kontrolle. Man könnte sich vorstellen, dass man im Vorfeld von solchen Aktivitäten eben nochmal genauer hinschaut. Mein Plädoyer wäre, es eben strikt voneinander zu trennen, also ganz klar zu sagen, wer was macht, und zu gucken, dass die, die entsprechende Dinge tun, auch im Rahmen der Kontrolle erfasst werden, also der Bundeswehr bestimmte Fähigkeiten zum Beispiel nur im Einsatz und unter Mandat zur Verfügung zu stellen und nicht in dem sogenannten Graubereich.

Abg. **Rainer Arnold** (SPD): Dann hätte ich noch eine Frage an Herrn Dr. Rid. Sehen sie das Risiko, dass im Bereich Cyber das staatliche Gewaltmonopol ausgehöhlt wird, insbesondere von Teilen der Wirtschaft, die anfangen, sich selbst mit Methoden, die über den Schutz hinausgehen, zu wehren? Und bräuchten wir, um so etwas einzuschränken, möglicherweise strengere Regulierungen von spezifischer Software in diesem Bereich?

SV **Prof. Dr. Thomas Rid** (King's College London): Ich denke, diese Thematik Active Defence – „hacking back" in der extremeren Wortwahl – wird gemeinhin überschätzt; also da ist die Debatte insbesondere in den USA von nicht besonderer hoher Qualität. Es gibt da sehr wenige Beispiele, auf die wir wirklich hinweisen können, die Sinn machen. Hacking back. Man kann nicht einfach irgendeinen Server in einem anderen Land oder im anderen Unternehmen ausschalten und damit einen Effekt erzielen, weil es in der Regel Command-and-Control-Server sind. Da wäre ich sozusagen weniger besorgt, um das jetzt auf ihre Frage angewendet umzudrehen. Ich denke nicht, dass wir hier das Gewaltmonopol verlieren.

Kann ich noch eine kurze Beobachtung anfügen? Wenn Sie sich die Nachrichtendienste in den technischen Bereichen USA und in Großbritannien anschauen, dann gibt es da einen ganz scharfen Kontrast zu Deutschland; nämlich dass die NSA und die GSHQ zu den jeweiligen Human Intelligences – CIA oder SIS bzw. MI6 – getrennte Organisationen darstellen. In Deutschland sind beide Spezialisierungen – menschliche Intelligenz und technische Aufklärung – unter einem Dach im BND gebündelt. Das macht es natürlich für die technische Seite des Hauses extrem schwierig, sich zu öffnen. Es ist im englischsprachigen Raum völlig normal, dass Ihnen heute die Mitarbeiter eine Karte in die Hand drücken und sagen, lassen sie uns das mal beim Kaffee besprechen. Sowas ist ganz schwierig in Deutschland. Also die Öffnung, die die Angelsachsen hier durchgemacht haben, ist in Deutschland organisatorisch bedingt sehr schwierig. Ich stelle es einfach mal als Frage in den Raum: Vielleicht ist jetzt irgendwann ein guter Moment gekommen, um hier auch mit einer großen Reorganisation ranzugehen, um diese Fähigkeiten letztlich ins 21. Jahrhundert zu holen.

Abg. **Alexander S. Neu** (DIE LINKE.): Angesichts der vorgerückten Stunde würde ich einfach nur um die Antworten der noch ausstehenden Fragen bitten.

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Die Fragen, die noch offen waren, waren ja Cyberangriff auf der einen Seite und „die Freiheit im Internet – ergeben sich daraus Konsequenzen?" auf der anderen Seite. Ich würde es einmal zwischen Unternehmen und Bürgern differenzieren. Nehmen wir mal an, ein Unternehmen lässt den Mitarbeitern im Unternehmen sämtliche Freiheiten im Internet – also alles zu benutzen, Apps runterzuladen, alles was dazugehört. Dann muss das Unternehmen wissen, welches Risiko es eingeht; denn das Risiko, das das Unternehmen eingeht, ist relativ hoch. Das heißt auf der anderen Seite, Sicherheitsmaßnahmen werden immer eine gewisse Konsequenz der Einschränkung haben, auch in der Internetznutzung, natürlich immer nur begrenzt. Aber wenn ich die volle Freiheit habe, habe ich ein hohes Risiko. Begrenze ich ein Stück die Freiheit, reduziere ich deutlich das Risiko. Das übertrage ich jetzt mal auf den Bürger. Für den Bürger gilt genau das gleiche. Wenn Sie die Beispiele nehmen, die es dort gibt. Wenn der Bürger im Internet alles benutzt, was es gibt, sich alles runterlädt, was es gibt, ohne darüber nachzudenken, welches Risiko er eingeht, ist die Gefahr ziemlich groß, dass sein PC von einem Schadprogramm befallen wird. So ist die Freiheit immer auf die Sicherheitsmaßnahmen und auf das Risiko, das ich eingehen möchte, bezogen.

Abg. **Alexander S. Neu** (DIE LINKE.): Ich möchte da nochmal nachfragen. Wenn Staaten für ihre Bürger verantwortlich sind und Bürger als Hacker andere Staaten cybermäßig angreifen; ist der Staat in irgendeiner Weise gehalten, dem Einhalt zu gebieten, weil er Verantwortung für seine Bürger hat? Was heißt das konkret, zum Beispiel mit Blick auf die Internetfreiheit für Deutschland? Welche Szenarien oder Gedankenexperimente gibt es, um so der Verantwortung des Staates gerecht zu werden?

SV Sts **Klaus Vitt** (BMI/IT-Beauftragter Bundesregierung): Ich kann das jetzt natürlich nur allgemein beantworten. Es wird für den Staat schwierig sein zu identifizieren, dass ein Bürger als Hacker aktiv ist. Dafür müsste man ihm die Tätigkeit nachweisen. Nehmen wir einmal an, der Bürger greift sozusagen ein Unternehmen in einem anderen Land an. Dann wird man in dem Land feststellen, dass es einen Hackerangriff gibt. Die eins-zu-eins Nachverfolgung, woher eigentlich der Ursprung stammt, ist relativ schwierig, weil solche Hacker normalerweise intelligent sind und andere Systeme missbrauchen, um das durchzuführen.

Abg. **Dr. Tobias Lindner** (BÜNDNIS90/DIE GRÜNEN): Tut mir leid, dass es jetzt mit meinen Fragen runter in den Maschinenraum geht. Die Fragen richten sich dann auch an die Staatssekretärin Dr. Suder. Ich will vielleicht mal so anfangen: Frau Staatssekretärin! Halten Sie auch angesichts der, ich will jetzt mal sagen, unscharfen oder schwierigen Grenzziehungen, die es an vielen Stellen in dem Themenbereich gibt, es noch für zeitgemäß, innerhalb der Bundeswehr eine Unterteilung in „weiße" und „grüne" IT vorzunehmen? Da ich vermute, dass Ihre Antwort „Nein" sein dürfte, wäre meine Rückfrage, welche Schlüsse Sie denn dann organisatorisch daraus ziehen? Es war ja früher so, dass die BWI den Auftrag hatte, sich nur um die „weiße" IT bei der Bundeswehr zu kümmern. Was wird sich zum Beispiel für den Auftrag der BWI daraus ergeben bzw. wo haben wir hier dann auch neue organisatorische Gemengelagen vor uns?

SV **Dr. Katrin Suder** (BMVg): Ja, ihre Annahme ist richtig. Insofern gibt es da in der Tat organisatorische Änderungen. Ich hatte vorhin schon mal was zur BWI gesagt. Ich würde jetzt nochmal das Pendant auf ministerieller Ebene – – Wir sind mit der Arbeit des Aufbaustabes noch nicht fertig; die soll ja im April beendet werden. Aber es zeichnet sich jetzt schon ab, dass wir auf der Ministeriumsebene klare Verantwortlichkeiten für IT, egal ob für „weiße" oder für „grüne", bündeln müssen; denn nur so stellen wir gesamthaft eine IT-Architektursicht sicher. Und die ist wichtig. Was heißt Architektur? Das heißt im

Grunde: Welche Standards nehme ich? Also wie soll Software, wie sollen Netze aufgebaut werden? Welche Sicherheitsmechanismen – und, und, und. Das heißt, durch eine starke Bündelung. Und ich bin sonst nicht immer eine Verfechterin der Bündelung, das hatten wir ja vorhin schon mal am Rande erwähnt. Zentralisierung ist nicht immer das Mittel der Wahl. Aber wenn ich hier durchsetzen will, dass ich klare IT-Standards habe, dass ich bestimmte Architekturen auch auf Dauer implementieren möchte, dann geht das nur, indem ich die Verantwortung übergreifend bündle. Das haben wir auch vor. Und insofern muss das aus einer Hand kommen; das ist dann in der Tat, genauso wie sie es, glaube ich, angedeutet haben, eine organisatorische Antwort auf die Bündelung von „grüner" und „weißer" IT.

Abg. **Dr. Tobias Lindner** (BÜNDNIS90/DIE GRÜNEN): Den Punkt Standards nochmal aufnehmend. Sie haben ja vorhin auch schon das Beispiel eingeführt. Mir ist sehr wohl bewusst, dass unsere Kampfpanzer nicht unbedingt in Echtzeit mit dem Internet vernetzt bzw. überhaupt nicht irgendwie damit verbunden sind. Aber ich habe mal in einer Berichtsbitte vom Ministerium, als ich wissen wollte, ob wir denn noch Computer im Geschäftsbereich BMVg/Bundeswehr mit Windows XP haben, zur Antwort erhalten: Na ja, bei HERKULES, BWI ist vieles in Ordnung; kommt so gut wie gar nicht mehr vor; aber die meisten unserer Waffensysteme laufen noch auf Windows XP. – Sehen Sie eine Notwendigkeit, an solchen Stellen dann auch Waffensysteme zu härten bzw. warum sehen Sie die nicht? Denn ich meine, Sie haben ja eben auch erwähnt, wir wollen gemeinsame Standards einhalten. Und in dem Zusammenhang wäre man ja sofort auch wieder im Zertifizierungs- und Umrüstungsproblem, wenn man die einhalten wollte, also eine Modernisierung vornehmen würde. Wo verlaufen für Sie die Grenzen zwischen dem, was man unbedingt tun muss, und dem, was man lassen sollte, weil es unter Umständen zu komplex oder zu teuer ist?

SV **Dr. Katrin Suder** (BMVg): Ja, im Grunde ist es dann eine Einzelfallentscheidung, genauso wie sie es ja vorskizziert haben, dass man sich sehr genau überlegen muss: Schaffe ich zunächst erstmal eine prozessuale und nicht perspektivische Lösung? Das heißt, dass die entsprechenden Computer eben nicht am Netz sind; dass ich dafür sorge, dass bei Wartungsvorgängen solche Dinge wie das berühmte USB-Beispiel eben nicht passieren; dass ich auch Maßstäbe, insbesondere Qualifizierungs- und Zertifizierungsmaßstäbe, an meine ganzen Zulieferer anlege; dass ich auch Sicherheitsüberprüfungen anlege; und, und, und... Und gleichzeitig, was ich vorhin schon mal erwähnt habe, dass über die CERTs auch immer wieder Penetrationstests mache. Das heißt, das ist ja erstmal eine prozessuale Lösung.

Perspektivisch müssen wir mit dem Obsoleszensproblem, wie es so schön heißt, dann ja auch umgehen. Das ist natürlich eine echte Herausforderung gerade in Waffensystemen, weil wir natürlich Waffensysteme haben, die lange Entwicklungszyklen haben; und das wissen Sie aus den diversen anderen Diskussionen, die wir immer wieder haben, sehr gut. Die IT hat dahinter nun mal andere Entwicklungszyklen. Jetzt gleichzeitig sozusagen in einem Big Bang Approach alle Rechner auf einmal auszutauschen, ist auch nicht praktikabel. Und deshalb müssen wir uns das Stück für Stück vornehmen. Und es steckt aber auch genau dahinter zu sagen, wir brauchen deshalb klare Architekturrichtlinien und müssen das sozusagen über die Zeit sinnvoll bereinigen. Das war ja vorhin auch irgendwie die Frage: Wie viel kostet das denn? Man kann es natürlich beliebig ausweiten und dann ist irgendwann bei den Grenzkosten die Frage, ob das noch der richtige Ansatz ist. Insofern muss es nur ein abgewogenes Vorgehen sein.

Abg. **Dr. Tobias Lindner** (BÜNDNIS90/DIE GRÜNEN): Ich würde nochmal das Thema mit den CERTs und den von Ihnen erwähnten Penetrationstests aufgreifen. Wenn ich offensiv in andere Netze wirken wollen würde, um das mal ganz bewusst im Konjunktiv zu formulieren, dann muss ich das ja auch irgendwie üben. Sind solche Tests, wie sie die CERTs durchführen, die quasi auch der Eigensicherung und der Schwachstellenanalyse dienen sollen, für Sie das gleiche wie Üben? Oder sind Sie der Auffassung,

wenn Bedarf besteht zu üben, ginge das darüber hinaus? Und wie müsste ich mir das skizzenhaft vorstellen?

SV **Dr. Katrin Suder** (BMVg): Die CERTs sind in meinen Augen von den CNO-Kräften getrennt zu betrachten. Und dann haben wir nochmal Übungstätigkeit der CNO-Kräfte in dem Sinne, wie wir es vorhin diskutiert haben, also um eine Fähigkeit vorzuhalten, die dann der Politik als Option im Rahmen des Parlamentsbeteiligungsgesetzes, was wir vorhin hatten, zur Verfügung gestellt werden kann. – Da möchte ich übrigens nochmal ganz kurz als Annex dranhängen: das Parlamentsbeteiligungsgesetz sieht ja in bestimmten Spezialfällen, also Gefahr in Verzug oder EvakOp-Maßnahmen, auch nochmal bestimmte Regelungen vor; die sind natürlich inkludiert. Aber es bleibt das Parlamentsbeteiligungsgesetz in seiner Intention, wie schon intensiv diskutiert. Das war das Thema CNO.

Was ich aber mit Üben vor allem auch meinte ist, dass wir auch gesamtstaatlich über das Austauschen von Daten sprechen – auch das ist ja schon mehrfach gekommen –, um möglichst zu vermeiden, dass alle davon betroffen sind, wenn irgendwo eine Lücke identifiziert wird. Nein, eben nicht! Sondern dass man auch Lagebilder teilt. Dieses Thema Need-to-share. Das heißt, dass man sich darüber austauscht, was denn jetzt genau die Schwachstellen sind, und dass man auch solche Fälle übt. Da kann die Bundeswehr genauso betroffen sein. Das heißt, irgendwo tritt ein Incident auf, irgendwo ist dieser berühmte Tag Null, wo erstmal wieder ein Breach entdeckt worden ist; und die Frage ist dann: Wie kann das schnell funktionieren, dass alle das sehen, dass das auch „24/7" funktioniert? Und dann: Was passiert auf unserer Seite, um entsprechend darauf zu reagieren? Also insofern eine geteilte Antwort. Das eine ist CNO, das ist was anderes als die CERTs. Dort wird in einem abgeschlossenen, gekapselten Raum geübt. Das ist in meinen Augen auch notwendig. Und dann gibt es das ganze Thema gesamtstaatliches Üben sozusagen zur Sicherheit.

Abg. **Dr. Tobias Lindner** (BÜNDNIS90/DIE GRÜNEN): Zum Abschluss würde ich Ihnen jetzt gerne die Gretchenfrage stellen; ein bisschen ein Blick in die Glaskugel. Die Ministerin hat ja entschieden, wie Sie so schön formuliert haben, den Bereich Cyber jetzt zusammenzuziehen. Es ist daran gedacht, einen Org.-Bereich innerhalb der Streitkräfte aufzubauen. Wenn ich jetzt ein paar Jahre nach vorne blicke, wie muss ich mir den Org.-Bereich vorstellen? Was ich vor allem wissen will: Muss ich mir vorstellen, dass da zukünftig eher zivile Mitarbeiterinnen und Mitarbeiter der Bundeswehr sitzen? Oder werden es Soldatinnen und Soldaten sein? Wenn wir Cyber als einen Raum wie Luft, Land, Wasser, Weltall, sonst was begreifen würden, wie muss ich mir das dann vom Charakter und der Kultur dieses Org.-Bereiches her vorstellen?

SV **Dr. Katrin Suder** (BMVg): Wir reden jetzt vom nachgeordneten Org.-Bereich, nicht von dem ministeriellen; das sieht da nochmal anders aus. Ich hatte ja vorhin erwähnt, dass wir mit Mannschaftssoldaten rund 21 000 Kräfte haben, die sich mit IT beschäftigen. 15 000, wenn wir die Mannschafter rauslassen; so ungefähr Pi mal Daumen. Auf diese Zahl bezogen sind das im überwiegenden Maße Soldatinnen und Soldaten, die auch IT im Einsatz zur Verfügung stellen. Insofern ist diese Frage dadurch beantwortet, dass die Kräfte, die den anderen Truppen als querschnittliche Aufgabe IT zur Verfügung stellen, Soldatinnen und Soldaten sind. Das macht die Mehrheit dieses Bereiches aus und wird es auch weiter ausmachen. Im Grunde kommt die große Zahl daher zustande.

Vors. **Wolfgang Hellmich** (SPD): Vielen Dank! Dann sind wir am Ende unserer Fragerunde angekommen. Ich sage den Expertinnen und Experten, die sich hier zur Verfügung gestellt haben, herzlichen Dank. Wir haben ein breites Lagebild mit vielen Aufgaben von der Parlamentsbeteiligung bis zu Entscheidungen im Haushalt erhalten, wo über Struktur, Aufgaben und Ausstattung der Bundeswehr entschieden wird. Da wird in der Konsequenz Einiges auf uns zukommen, wo wir uns um die Umsetzung und die Konsequenzen unterhalten werden. Da der Weg nicht in Richtung Schreibmaschine und Brieftauben zu-

rückgeht, ist es eindeutig, wo der Weg innerhalb kürzester Zeit für uns hingehen muss. Wir werden uns mit Hochdruck an die Auswertung dieser Anhörung und an eine Debatte über die notwendigen Konsequenzen machen. Herzlichen Dank für Ihre Teilnahme, auch den Kolleginnen und Kollegen aus den beteiligten Ausschüssen. Ich glaube, auch in deren Namen kann ich Ihnen für ihre fundierten Beiträge herzlichen Dank sagen. Damit schließe ich die heutige Sitzung.

Schluss der Sitzung: 17:05 Uhr

Für das Protokoll

Wolfgang Hellmich, MdB
Vorsitzender

(RD Dr. Christian Schnellecke)

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)633
17.02.2016 - 18/2686
5410

Stellungnahme zu Rechtsfragen des Cyberwar
für den Verteidigungsschuss der Deutschen Bundestages

Prof. em. Dr. Michael Bothe
J.W. Goethe-Universität, Frankfurt/Main

Die folgende Stellungnahme behandelt in einer systematischen Auswahl die Rechtsfragen, die vom Verteidigungsausschuss zur Vorbereitung der Anhörung am 22.2.2016 gestellt wurden.

Zusammenfassung

Die Nutzung von Computernetzwerken zur Schädigung fremder Staaten (Cyber-Angriff) besitzt ein hohes Schadenspotenzial, das eine Klärung seiner rechtlicher Schranken erfordert. Dieses neue Phänomen ist keineswegs ein rechtliches Niemandsland. Vielmehr kann bestehendes Recht sinnvoll darauf angewandt werden.

Völkerrechtlich ist auch auf Cyber-Angriffe die Grundregel anzuwenden, die Staaten verbietet, andere Staaten zu schädigen, und die Staaten gebietet, mit der gebotenen Sorgfalt (due diligence) zu verhindern, dass von ihrem Territorium Schaden auf dem Gebiet anderer Staaten verursacht wird (no harm rule). Cyber-Angriffe sind sie als Verletzungen des völkerrechtlichen Gewaltverbots oder auch als bewaffnete Angriffe im Sinne des Art. 51 UN Charter zu qualifizieren, wenn sie hinsichtlich Umfang und Wirkung („scale and effects") dem Einsatz von Waffengewalt vergleichbar sind. Es kommt für die Vergleichbarkeit wesentlich auf den Umfang der durch einen Cyberangriff verursachten physischen Schäden an. Ein solcherart als „bewaffneter" Angriff zu qualifizierender Cyberangriff berechtigt zu Selbstverteidigung, d.h. zum militärischen Gegenschlag, und führt zur Anwendbarkeit von Art. 5 des NATO-Vertrages.
Bei der Frage, wann ein Cyber-Angriff solcherart bewaffneter Gewalt gleich zu achten ist, bestehen Interpretationsspielräume, die ein hohes Missbrauchspotenzial im Sinne einer falschen Rechtfertigung militärischer Gegengewalt in sich bergen. Selbstverteidigung ist nur gegen den Staat zulässig, der die Erstgewalt ausgeübt hat, d.h. dem ein erster Cyber-Angriff nachweisbar zuzurechnen ist. Selbstverteidigung auf Verdacht ist unzulässig. Diese Regel ist zu beachten, obwohl gerade bei Cyber-Angriffen der Nachweis des Urhebers schwierig ist. Von der Selbstverteidigung, die einen bewaffneten Angriff im Rechtssinne voraussetzt, sind reine Schutz- und Abwehrmaßnahmen (nicht immer einfach) zu unterscheiden, die ein Staat stets treffen darf.

Wenn ein bewaffneter Konflikt wie auch immer einmal entstanden ist, gilt auch für Cyber-Angriffe das allgemein für die Zulässigkeit von Schädigungshandlungen anwendbare Recht bewaffneter Konflikte (humanitäres Völkerrecht, ius in bello). Insbesondere ist das Unterscheidungsgebot zu beachten: Angriffe dürfen nur auf militärische Ziele, nicht auf zivile Objekte oder Zivilpersonen gerichtet werden. Der zivile Begleitschaden, der u.U. von

Angriffen auf zivile Objekte verursacht wird, darf nicht außer Verhältnis zu dem erwarteten militärischen Vorteil stehen. Die Anwendung dieser Regeln wirft Schwierigkeiten der Qualifizierung von Objekten und Abwägung zwischen zivilem Schaden und militärischem Vorteil nicht nur bei Cyber-Angriffen Schwierigkeiten auf.

Die Bundesrepublik ist nach Art. 26 GG verfassungsrechtlich verpflichtet, keine Cyber-Angriffe auszuführen oder sich an ihnen zu beteiligen, die den Tatbestand des Gewaltverbots erfüllen.
Werden Cyber-Angriffe von deutschen Streitkräften ausgeführt, so gilt das Erfordernis parlamentarischer Zustimmung. Diesem Erfordernis unterfallen nach dem Grundsatz der Vergleichbarkeit zumindest Maßnahmen, deren (auch indirekte) physische Wirkung („scale and effects") so erheblich ist, dass sie als militärische Gewaltmaßnahmen zu qualifizieren sind. Welche Cyber-Operationen darüber hinaus Einbezug in militärische Operationen zu qualifizieren sind, die das Zustimmungserfordernis auslösen, ist ohne eingehende Analyse möglicher Szenarien kaum zu entscheiden.
Zu erwägen ist auch, ob unter Anwendung der Grundsätze des Bundesverfassungsgerichts für Cyber-Operationen, deren Wirksamkeit von der vorherigen Geheimhaltung abhängt, das Zustimmungsverfahren im Sinne des Geheimschutzes modifiziert werden kann.
Die in der völker- und verfassungsrechtlichen Analyse dargestellten Unsicherheiten und Unklarheiten werden die Frage nach der lex ferenda, nach neuen völkervertraglichen Regelungen auf. Streitig dabei insbesondere die Tragweite möglicher staatlicher Kontrollpflichten. Darüber hinaus stehen allerdings die Chancen für völkerrechtliche Neuregelungen zu Schranken militärischer Gewalt im gegenwärtigen Klima der internationalen Beziehungen eher schlecht.

1. Die Problematik

Maßnahmen des Cyberwar oder Cyberangriffe sind eine neue Form der grenzüberschreitenden Schädigung: Störung oder Vernichtung der Funktionsfähigkeit von Computern oder Computernetzwerken in einem anderen Staat mit Hilfe von Computer-Netzwerken. Die so gestörten Computer oder Computer-Netzwerke steuern ihrerseits eine Vielzahl von Vorgängen in der physischen Welt, insbesondere kritische Infrastruktur. In dem Verlust der Steuerungsfähigkeit oder der Verfälschung der Steuerung besteht das hohe Schadenspotenzial von Cyberangriffen.[1] Dieses Schadenspotenzial macht es erforderlich, die Rechtsregeln, insbesondere die Völkerrechtsregeln zu klären, die für solche Angriffe gelten. Dies ist der Zweck der folgenden Ausführungen.

Die Ausführungen gehen davon aus, dass die Neuheit des Phänomens keineswegs erfordert, dass das bislang geltende Recht davor kapitulieren muss, oder dass es sich um ein „völkerrechtliches Niemandsland" handelt, wo alle auftretenden Fragen und Konflikte neu geregelt werden müssten.[2] Eine Antwort auf die Frage nach den rechtlichen Schranken dieser Schädigungsvorgänge muss vielmehr versuchen, bestehende Regeln auf dieses neue Phänomen anzuwenden, d.h. in diesem neuen Phänomen die Tatbestandsmerkmale der vorhandenen Regeln zu erkennen und herauszuarbeiten. Das ist der konsequent durchgeführte Ansatz des Tallinn Manual on the International Law Applicable to Cyber Warfare,[3] ein von einer internationalen Expertengruppe erarbeitetes Regelwerk mit ausführlichem Kommentar. Diese Gruppe war von der NATO eingeladen, es handelt sich aber nicht um ein offizielles NATO-Dokument. Die Gruppe besitzt natürlich keine Rechtssetzungskompetenz, aber das fachliche Ansehen der Mitglieder der Gruppe verleiht ihrer Meinung zur Rechtslage ein hohes Gewicht in einem sich fortsetzenden rechtlichen Diskurs.

Auch die von der UN-Generalversammlung eingesetzte Arbeitsgruppe über internationale Sicherheit im Bereich der Telematik setzt auf die Anwendbarkeit des geltenden Völkerrechts.[4] Im internationalen Diskurs gibt es allerdings auch Stimmen, die stärker die Notwendigkeit von Neuregelungen betonen. Sie fordern insbesondere mehr staatliche Kontrolle von IT-Aktivitäten, so etwa Russland und China.[5] Dem wird von anderer Seite mit einer Betonung des freien Informationsflusses widersprochen.

---

[1] GA Resolution 66/24. Vgl. die Berichte der von der UN-Generalversammlung eingesetzten Expertengruppe, UN Doc. A/65/201 und A/68/98; vgl. ferner Sandro Gaycken, 'Die vielen Plagen des Cyberwar', in Roman Schmidt-Radefeldt/Christine Meissler (Hrsg.), Automatisierung und Digitaliserung des Krieges, Baden-Baden 2012, S. 89 ff, 91 ff.

[2] Wolff Heintschel von Heinegg, ‚Cyberspace – Ein völkerrechtliches Niemandsland?', in Schmidt-Radefeld/Meissler (Hrsg.). a.a.O. Anm. 1, S. 159 ff.

[3] Michael N. Schmitt (Hrsg.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepare by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence, Cambridge 2013.

[4] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. 68/98, Ziff. 16 ff.

[5] Sven-Hendrik Schulze, Cyber-"War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015, S. 177; Heike Krieger, ‚Krieg gegen anonymus. Völkerrechtliche Regelungsmöglichkeiten bei unsicherer Zurechnung im Cyberwar', AVR 50 (2012), S. 1 ff., 18.

Der Ansatz des Tallinn Manual stößt zumindest an seine Grenzen wegen eines spezifischen Problems von Cyberangriffen, nämlich ihrer mangelnden Rückverfolgbarkeit,[6] d.h. der fehlenden Identifizierbarkeit des Urhebers. Dies ist eine Herausforderung für jede Rechtsordnung, deren Regelungsmöglichkeiten vorrangig auf Zurechnung beruhen.[7] Wo der Urheber eines Schadens nicht zu ermitteln ist, ist eine Ahndung der Schadensstiftung als Unrecht nicht möglich. Das ist an sich kein neues Phänomen. Wo allerdings die mangelnde Bestimmbarkeit des Schädigers für eine bestimmte Form der Schadensstiftung so typisch ist wie bei Cyberangriffen, stellt sich die Frage, ob es mit einem solchen unbefriedigenden Ergebnis sein Bewenden haben kann und ob es Wege gibt, das Problem der Rückverfolgbarkeit von Cyberangriffen angemessen zu regeln.

Im Folgenden soll versucht werden, für einige relevante Regeln des Völkerrechts und des Verfassungsrecht die Anwendung auf die besondere Form der Schadensstiftung durch Cyberangriffe zu untersuchen und dabei auch auf das besagte Problem der Rückverfolgung einzugehen.

2. Völkerrecht

Zur völkerrechtlichen Beurteilung sind folgende Normen zugrunde zu legen:

- Verbot der grenzüberschreitenden Schadensstiftung, sog. no harm rule;
- Interventionsverbot;
- Gewaltverbot;
- Verbot des bewaffneten Angriffs, eine qualifizierte Form des Gewaltverbots.

Diese Kategorisierungen beruhen auf der einschlägigen Rechtsprechung des Internationalen Gerichtshofs. Er hat sie insbesondere in dem Urteil in Sachen Nicaragua gg. USA 1986 entwickelt,[8] das bis heute als im wesentlichen unbestrittene Feststellung der Rechtslage nach Völkergewohnheitsrecht gilt. Verletzungen dieser Verbote können mit verhältnismäßigen Gegenmaßnahmen beantwortet werden, mit einem militärischen Gegenschlag, d.h. Selbstverteidigung i.S. Art. 51 UN Charter, nur der bewaffnete Angriff.

Das Verbot grenzüberschreitender Schadensstiftung ist eine Regel des allgemeinen Völkerrechts, die in den letzten Jahrzehnten vor allem bei Fragen des Ersatzes für grenzüberschreitende Umweltbelastungen eine Rolle gespielt hat. Sie gilt aber für jede Art von Schadensstiftung. Sie verbietet nicht nur direkte Schadensstiftung durch staatliche Organe, sondern verpflichtet auch die Staaten, keine grenzüberschreitende Schadensstiftung durch Private zuzulassen. Nach Völkergewohnheitsrecht müssen die Staaten zur Verhinderung grenzüberschreitender Schadensverursachung die gebotene Sorgfalt (due

[6] Schulze, a.a.O. Anm. 5, S. 36 ff.
[7] Krieger, a.a.O. Anm. 5, S. 3.
[8] *Military and Paramilitary Activities in and around Nicaragua, Nicaragua v. U.S.*, Merits, Urteil v. 27.6.1986, Ziff. 195; siehe auch Andreas v. Arnault, Völkerrecht, 2. Aufl., Karlsruhe 2014, S. 449

diligence) walten lassen.[9] Das gilt auch für Schädigungen mittels Cyber-Angriffen. Welche Sorgfaltspflichten allerdings insofern zur Verhinderung grenzüberschreitender privater Hacker-Tätigkeiten u.ä. folgen, ist noch weitgehend ungeklärt. Das Tallinn Manual formuliert diese Pflicht zur Verhinderung solcher schadenstiftender Cyberaktivitäten ein, die dem Staat bekannt sind:

> „A State shall not knowingly allow cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[10]

Damit bleibt das Manual meines Erachtens hinsichtlich des wissen Müssens hinter dem geltenden Gewohnheitsrecht zurück. In der Expertengruppe herrschte diesbezüglich Uneinigkeit.[11] Über die Tragweite staatlicher Pflichten zur Kontrolle von privaten schadensstiftenden Handlungen mittels und in Computer-Netzwerken ist de lege lata und de lege ferenda weiter nachzudenken.

Das Interventionsverbot ist Bestandteil des völkerrechtlichen Gewohnheitsrechts. Es verbietet (so der IGH) die Ausübung von Zwang gegenüber einem Staat in Bereichen, die kraft der staatlichen Souveränität seiner freien Entscheidung unterliegen.[12]
Wo genau die Schwelle verbotener Einflussnahme liegt, ist schon für das Interventionsverbot im Allgemeinen umstritten. Wird ein solcher Eingriff durch Einflussnahme auf das Funktionieren von Computer-Systemen ausgeübt, ist diese Grenzziehung noch weitgehend ungeklärt. Das entscheidende Kriterium kann nur die Vergleichbarkeit mit Einflussnahmen traditioneller Art sein.[13]

Das Gewaltverbot nach der Satzung der Vereinten Nationen und nach völkerrechtlichem Gewohnheitsrecht verbietet nur militärische Gewalt. Wird die Gewalt nicht durch staatliche Organe selbst ausgeübt, so ist sie einem Staat dennoch zuzurechnen, wenn er in die betreffenden nicht staatlichen Aktivitäten erheblich involviert ist.[14] Darum ist zu prüfen, ob Schadensstiftung durch Computerangriffe ggf. einem militärischen Angriff gleich zu achten sind. In den einschlägigen völkerrechtlichen Diskursen setzt sich insofern das Kriterium von „scale and effects" (Umfang und Wirkung) durch. Dem folgt auch das Tallinn Manual. Schadensstiftung durch Computerangriffe ist also militärischer Gewalt gleich zu achten, wenn sie physische Zerstörungen von erheblichem Umfang verursacht, die denen vergleichbar sind,

[9] Eine Übersicht über die verschiedenen Rechtsbereiche, in denen due diligence eine Rolle spielt, bei Timo Koivurova, ‚Due Diligence', Rdn. 29 ff., in Rüdiger Wolfrum (Hrsg.), Max Planck Encyclopedia of Public International Law (www.mpepil.com); vgl. auch Schulze, a.a.O. Anm. 5, S. 118 ff., 143.
[10] Tallinn Manual, Rule 5.
[11] Tallinn Manual, S. 28; unklar Schulze, a.a.O. Anm. 5, S. 143.
[12] Philip Kunig, 'Intervention, Prohibition of', in MPEPIL (Anm.9).
[13] Vgl. Tobias O. Keber/Przemysław Roguski, ‚Ius ad bellum electronicum. Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis', AVR 49 (2011), S. 399 ff., 409 f.
[14] *Nicaragua*-Urteil, Anm. 8, Ziff. 195.

die durch gewöhnliche militärische Angriffe, insbesondere Angriffe mittels kinetischer Waffen, verursacht werden:[15]

> „A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force."[16]

Was in diesem Sinne „erheblich" ist, d.h. „rising to the level of the use of force", darüber ist Streit möglich und sogar wahrscheinlich. Das gilt auch und gerade für die Unterscheidung zwischen einer Verletzungen des Gewaltverbots von minderem Ausmaß und dem bewaffneten Angriff, der ein Selbstverteidigungsrecht auslöst:

> „A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."[17]

Die Zulässigkeit eines militärischen Gegenschlags hängt also davon ab, ob die zuvor ausgeübte (oder unmittelbar drohende) Erstgewalt die Schwelle eines bewaffneten Angriffs erreicht oder überschreitet. Es bestehen erhebliche Interpretationsspielräume. Diese Interpretationsspielräume sind missbrauchsanfällig, da die als rechtliche Grundlage einer Entscheidung zum Einsatz militärischer Gewalt nicht nur ge-, sondern auch missbraucht werden können. Einzelheiten waren denn auch in der Expertengruppe des Tallinn Manual umstritten. Die Mehrheit der Gruppe war der Auffassung, dass ein bewaffneter Angriff in diesem Sinn jedenfalls nicht den Einsatz von Waffengewalt mit kinetischer Energie voraussetzt (dann könnte ein Cyber-Angriff wohl nie als bewaffneter angriff qualifiziert werden), sondern dass es auf die Wirkung des Angriffs ankommt. Gleicht diese Wirkung der eines Angriffs mit kinetischer Energie, d.h. führt sie zu Tod oder Verwundung von Personen bzw. Beschädigung oder Zerstörung von Sachgütern, liegt ein bewaffneter Angriff vor.[18] Gerade wegen der besagten Missbrauchsmöglichkeit müssen an den Umfang des physischen Schadens, dessen Verursachung das Selbstverteidigungsrecht auslöst, hohe Anforderungen gestellt werden.[19] Ob auch erhebliche Schäden anderer Art einen Cyber-Angriff zu einem „bewaffneten" Angriff machen, war in der Expertengruppe umstritten.[20] M.E. ist dies wegen der besagten Missbrauchsmöglichkeit abzulehnen.

Bislang ist der einzige bekannte Fall eines Cyber-Angriffs, bei dem physische Schäden verursacht wurden, der Stuxnet-Angriff auf iranische Atomzentrifugen 2010. Die Expertengruppe des Tallinn Manual war sich in der Beurteilung nicht einig.[21] Ein Autor

---

[15] In diesem Sinn auch Daniel B. Silver, ‚Computer Network Attacks as a Use of Force under Article 2(4) 0f the United Nations Charter', in: Michael N. Schmitt/Brian T. O'Donnell (Hrsg.), Computer Network Attack and International Law, International Law Studies vol. 76, Newport 2002, S. 73 ff., 85.
[16] Tallinn Manual, Rule 11.
[17] Tallinn Manual, Rule 13.
[18] Talinn Manual, S. 55. In diesem Sinn auch Yoram Dinstein, 'Computer Network Attacks and Self-Defence', in Schmitt/O'Donnell (Hrsg.), a.a.O. Anm. 15, S. 99 ff., 103; Keber/Roguski, a.a.O. Anm. 13, S.408.
[19] Krieger, a.a.O. Anm. 5, S. 11.
[20] Tallinn Manual, S. 56.
[21] Tallinn Manual, S. 58.

äußert sich vorsichtig dahin, dass die Qualifizierung als bewaffneter Angriff „nicht von vornherein ausgeschlossen“ sei.[22]

Aus dem Gesagten folgt: Ein Cyber-Angriff auf einen NATO-Staat löst nur dann die Rechtsfolge des Art. 5 NATO-Vertrag aus, wenn er die dargestellte Schwelle eines bewaffneten Angriffs erreicht.

Selbstverteidigung ist diejenige militärische Gewalt, die erforderlich und verhältnismäßig ist, um einen bewaffneten Angriff abzuwehren. Die Selbstverteidigung richtet sich gegen den Angreifer, und nur gegen diesen. Nach der Rechtsprechung des IGH trifft insofern die Beweislast denjenigen, der sich auf Selbstverteidigung beruft. Er muss nachweisen, dass ein bewaffneter Angriff von dem Adressaten der Verteidigungsmaßnahme verübt worden ist,[23] d.h. einem bestimmten Staat zuzurechnen ist. So hat es der IGH in einem Fall unklarer Zuordnung des Erstangriffs entschieden und an diesen Nachweis hohe Anforderungen gestellt.[24] Selbstverteidigung auf Verdacht ist unzulässig.[25] Dies ist angesichts der Unsicherheit der zuverlässigen Beurteilung der Herkunft von Cyberangriffen ein schwieriges Problem. Nach dem Tallinn Manual ist jedenfalls die Tatsache, dass eine Schädigungshandlung von einem Server herrührt, der sich auf dem Gebiet eines bestimmten Staates befindet, nicht ausreichend, um die Schädigungshandlung diesem Staat zuzurechnen[26] und ihn somit zum Adressaten eines zulässigen militärischen Gegenschlages zu machen.

In diesem Zusammenhang stellt sich auch für Cyber-Angriffe die allgemeiner bezüglich terroristischer Angriffe umstrittene Frage, ob und inwieweit Angriffe, die von nicht-staatlichen Akteuren begangen werden, bewaffnete Angriffe im Sinne des Art. 51 UN Charter darstellen.[27] Das kann hier nicht im Einzelnen diskutiert werden. Jedenfalls kann die Verletzung von staatlichen Kontrollpflichten gegenüber privaten Cyber-Angriffen diese nicht zu einem bewaffneten Angriff seitens des Herkunftsstaates machen.

Selbstverteidigung rechtfertigt militärische Gewalt, die ohne diese Rechtfertigung unzulässig wäre. Darum sind von Selbstverteidigung in diesem Sinne zu unterscheiden passive Abwehr- und Schutzmaßnahmen, die ein Staat stets treffen kann. Beispiele in der materialen Welt ist etwa, wenn ein in den staatlichen Luftraum eingedrungenes Flugzeug zur Landung gezwungen wird, selbst wenn das Eindringen noch nicht einen bewaffneten Angriff darstellt. Gegen Computer-Operationen ist eine vergleichbare Maßnahme etwa ein Firewall. Solche Maßnahmen sind ohne Vorliegen eines bewaffneten Angriffs im dargestellten Sinne zulässig. Die Abgrenzung im Einzelnen mag nicht immer einfach sein.

---

[22] Schulze, a.a.O. Anm. 5, S. 127.
[23] *Oil Platforms, Iran v. U.S.*, Merits, Urteil v. 6.11.2003, Ziff. 57 ff., 71 f.; vgl. Marco Roscini, ‚Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, in Jens David Ohlin (Hrsg.), Cyberwar, Oxford 2015, S. 215 ff.
[24] Zu Einzelheiten der Beweismaßstäbe Roscini, a.a.O. Anm. 23, S. 217.
[25] Vgl. auch Michael Bothe, ‚Terrorism and the Legality of Pre-emptive Force‘, EJIL 14 (2003), S. 227 ff., 232: zweifelnd Keber/Roguski, a.a.O. Anm. 13, S. 416.
[26] Tallinn Manual, Rule 8.
[27] Vgl. zum Streit Tallinn Manual , 58 f.; Dinstein, a.a.O. Anm. 18, 111 f.

Von den besagten Verbotsnormen sind zu unterscheiden die Regeln des humanitären Völkerrechts über zulässige oder unzulässige Mittel der Schädigung des Gegners im Rahmen eines bewaffneten Konflikts. Es gilt insbesondere das Unterscheidungsgebot: Angriffe dürfen nur gegen militärische Ziele gerichtet werden, nicht gegen zivile Objekte. Militärische Ziele sind solche Objekte, die zu den militärischen Anstrengungen des Gegners beitragen und deren Zerstörung bzw. sonstige Ausschaltung einen militärischen Vorteil erwarten lässt. Zivile Begleitschäden sind verboten, wenn der zu erwartende zivile Schaden eines Angriffs außer Verhältnis zu dem erwarteten unmittelbaren militärischen Nutzen steht. Wenn einmal ein bewaffneter Konflikt besteht, wie immer er begonnen wurde, stellt sich die Frage, ob und inwieweit Cyberangriffe an diesen Maßstäben zu messen sind. Diese Frage wird heute allgemein bejaht, wenn durch eine Cybermaßnahme die von einem militärischen Angriff gemeinhin ausgehenden Folgen eintreten oder zu erwarten sind: Tod oder Verletzung von Personen bzw. Zerstörung oder Beschädigung von Sachgütern.[28]

Angesichts der Unsicherheiten einer Rückverfolgung von Angriffen und der damit verbundenen faktischen und rechtlichen Schwierigkeit von Gegenmaßnahmen ist die Pflicht zu Vorsichtsmaßnahmen, wie sie z.B. in Art. 58 ZP I formuliert ist, für den Cyberwar besonders wichtig.[29]

Im internationalen bewaffneten Konflikt sind nur Kombattanten, d.h. Angehörige der Streitkräfte berechtigt, an Kampfhandlungen teilzunehmen, d.h. Angriffe auf den Gegner auszuführen. Das macht für den Cyberwar das Problem nicht-staatlicher Akteure (z.B. Hacker) rechtlich besonders heikel.[30]

3. Verfassungsrecht

Eine erste verfassungsrechtliche Folgerung, die aus der völkerrechtlichen Analyse gezogen werden muss, folgt aus Art. 26 GG, dem Verbot des Angriffskrieges. Sie geht dahin, dass die Bundesrepublik keine Cyber-Angriffe unternehmen oder sich an ihnen beteiligen darf, die nach dem Gesagten den Tatbestand des Gewaltverbots erfüllen und nicht als Selbstverteidigung nach Art. 51 UN Charter gerechtfertigt sind. Die bei der völkerrechtlichen Analyse dargestellten Unsicherheiten gelten entsprechend für die verfassungsrechtliche Bewertung. Es ist auch in diesem Zusammenhang zu betonen, dass eine Selbstverteidigung auf Verdacht nicht zulässig ist und damit unter das Verbot des Art. 26 GG fällt.

Eine wesentliche und noch nicht hinreichend diskutierte verfassungsrechtliche Frage ist die Anwendung des Erfordernisses der Parlamentsbeteiligung auf Cyber-Angriffe. Dieser Parlamentsvorbehalt gilt für Beteiligung der deutschen Streitkräfte an militärischen Unternehmen. Eine erste Antwort auf diese Frage liegt in einer angemessenen Anwendung des scale and effects-Kriteriums. Denn wenn für die völkerrechtliche Definition eines Angriffs, der eine Verletzung des Gewaltverbots oder gar einen bewaffneten Angriff im Sinne

[28] Ausführlich: Tallinn Manual, Rules 30-59. Vgl. auch Heintschel von Heinegg, a.a.O. Anm. 2, 162 ff.
[29] Krieger, a.a.O. Anm. 5, S. 17.
[30] Nicolò Bussolati, ‚The Rise of Non-State Actors in Cyberwarfare', in Ohlin (Hrsg.), a.a.O. Anm. 23, S. 102 ff.

des Art. 51 UN Charter darstellt, von der Notwendigkeit eines Waffeneinsatzes abgesehen und auf die Wirkung abgestellt wird, dann sollte das auch für den Einbezug von Soldaten „in bewaffnete Unternehmungen", der nach der Rechtsprechung des Bundesverfassungsgerichts[31] das Zustimmungserfordernis auslöst, relevant sein.

Bei Computer-Angriffen durch deutsche Staatsorgane ist zu beachten, dass das Erfordernis der Parlamentsbeteiligung nur für Handlungen der Streitkräfte gilt. Für andere Staatsorgane, etwa für (nichtmilitärische) Geheimdienste gilt es nicht. Für den internationalen bewaffneten Konflikt gilt allerdings, dass Kampfhandlungen, d.h. Maßnahmen zur Schädigung des Gegners, nur durch Kombattanten, Mitglieder der Streitkräfte ausgeführt werden dürfen. Das gilt auch für Cyber-Angriffe.

Handelt es sich bei Computer-Angriffen um Maßnahmen der Streitkräfte, so gilt der Parlamentsvorbehalt jedenfalls, wenn diese Maßnahmen nach dem scale and effects-Kriterium einer militärischen Maßnahme gleich zu achten sind. Relevant ist diese Frage natürlich nur, soweit Cyberangriffe isolierte Maßnahmen darstellen. Geschehen sie im Rahmen einer ohnehin stattfinden militärischen Aktion, gilt der Parlamentsvorbehalt für die gesamte Aktion.

Bei separaten Cyber-Operationen ist es eine Frage des konkreten Szenarios, ob die Schwelle zu einer militärischen Aktion nach dem scale and effects-Kriterium erreicht oder überschritten ist. Dazu eine Übersicht von Szenarien zu liefern, kann nicht Aufgabe dieser Stellungnahme sein.

Zu bedenken ist in diesem Zusammenhang allerdings darüber hinaus, dass nach der Rechtsprechung des Bundesverfassungsgerichts die Schwelle für den Parlamentsvorbehalt ja viel niedriger liegt als bei dem Einsatz von Waffengewalt, die entweder eine Verletzung des Gewaltverbots darstellt oder der besonderen Rechtfertigung als Selbstverteidigung bzw. durch ein Mandat des Sicherheitsrats bedarf. Welche Cyber-Operationen in diesem Sinne einen Einbezug in militärische Maßnahmen darstellen, ist ohne eine gründliche Diskussion einschlägiger Szenarien kaum zu entscheiden.

In diesem Zusammenhang stellt sich die weitere Frage, ob für Cyber-Angriffe möglicherweise eine vom Bundesverfassungsgericht zugelassene Ausnahme vom Parlamentsvorbehalt vorliegt. Das Bundesverfassungsgericht führt in seiner grundlegenden Entscheidung zur Tragweite des Parlamentsvorbehalts aus, dass durch die Mitwirkung des Bundestages „die militärische Wehrfähigkeit und die Bündnisfähigkeit der Bundesrepublik Deutschland" nicht beeinträchtigt werden dürfe. Als einziges Beispiel für dieses Prinzip führt das Gericht aus, die Bundesregierung sei bei Gefahr im Verzug berechtigt, vorläufig den Einsatz von Streitkräften zu beschließen. Diese Formulierung ist in § 5 des Parlamentsbeteiligungsgesetzes übernommen worden. Dabei wird eine Situation gleich behandelt, bei der eine vorgängige

[31] Urteil vom 12.7.1994, 2 BvE 3/92, BVerfGE 90, 286; ferner die Urteile vom 7.5.2008, 2 BvE 1/03, BVerfGE 121, 135 (AWACS Türkei) und vom 23.9.2015, 2 BvE 6/11 (Libyen).

öffentliche Debatte das Leben von zu rettenden Menschen gefährden würde.[32] Ob in diesem Sinne bei Cyberangriffen, die durch die Bundeswehr durchgeführt werden, Gefahr im Verzug ist, ist eine Frage des Einzelfalls.

In der Praxis hat sich daneben, offenbar auf dem Boden der Forderung des BVerfG, dass die militärische Wehrfähigkeit nicht beeinträchtigt werden dürfe, eine besondere Behandlung von Operationen herausgebildet, von denen angenommen wird, dass sie ihrer Natur nach geheimhaltungsbedürftig sind.[33] Dieses Verfahren beruhte zunächst auf einer Absprache zwischen Bundesregierung und den Fraktionsvorsitzenden und sieht nur eine Unterrichtung bestimmter Abgeordneter unter Wahrung des Geheimschutzes vor. Es soll in die Neufassung des Parlamentsbeteiligungsgesetzes (§ 6a) übernommen werden. Diese Vorschrift betrifft nur den geheimhaltungsbedürftigen Einsatz von Spezialkräften. Cyberangriffe werden in der neuen Bestimmung nicht geregelt. Es wäre freilich zu erwägen, ob der Grundsatz der Nichtbeeinträchtigung der Wehrfähigkeit, wie ihn das BVerfG formuliert hat, nicht auch für bestimmte Cyberangriffe gelten könnte. Es könnte argumentiert werden, dass solche Angriffe nur wirksam sind, wenn sie den Gegner unvorbereitet treffen. Sie könnten deshalb als ihrer Natur nach geheimhaltungsbedürftig angesehen werden. Das Verfahren zum geheimhaltungsbedürftigen Einsatz von Spezialkräften könnte dafür als Vorbild dienen. Die Bundesregierung könnte also nicht einseitig von der Parlamentsbeteiligung absehen, sondern müsste zusammen mit den Funktionsträgern der Fraktionen angemessene Lösungen finden. Allein eine solche kooperative Lösung entspräche dem Sinn des Parlamentsvorbehalts.

4. Sinnhaftigkeit und Möglichkeit neuer völkerrechtlicher Verträge

Die praktische Anwendung des scale and effects-Kriteriums lässt sich wohl kaum in allgemeiner Form durch völkerrechtlichen Vertrag regeln. Immerhin wäre eine allgemeine Formulierung des Prinzips in einem Vertragstext ein Schritt zu mehr Rechtssicherheit.

Auch für die Fragen der Zurechnung oder von Sorgfaltspflichten bei der Kontrolle privater Tätigkeiten auf eigenem Staatsgebiet wäre eine angemessene Regelung wohl sinnvoll. Allerdings scheiden sich die Geister bei der Frage der Intensität staatlicher Kontrollpflichten,[34] wie insbesondere die Beratungen in den Vereinten Nationen ergeben haben.

Ob die Zeit für eine solche Regelung schon reif ist, ist nicht nur deshalb fraglich. Es liegt nicht nur an den dargestellten Schwierigkeiten der Materie, dass die Chancen für den Versuch einer vertraglichen Regelung, was immer ihr Inhalt, schlecht stehen.[35] Gegenwärtig besteht in der internationalen Gemeinschaft ein verbreiteter Unwille, Fragen der Ausübung militärischer

[32] § 5 Abs. 1 Satz 2 ParlamentsbeteiligungsG.
[33] Bericht der sog. Rühe-Kommission, BT Drs. 18/5000, S. 43 f.
[34] Schulze, a.a.O. Anm. 5, S. 177, 182 ff.; Krieger, a.a.O. Anm. 5, S. 18; Keber/Roguski, a.a.O. Anm. 13, S. 420 ff.
[35] Vgl. auch Philip A. Johnson, , Is It Time for a Treaty on Information Warfare?', in Schmitt/O'Donnell (Hrsg.), a.a.O. Anm. 15, S. 439 ff., 453.

Gewalt und insbesondere offene Fragen des humanitären Völkerrechts sowie Fragen der Haftung vertraglich zu regeln.

Deshalb scheint gegenwärtig die wichtigere Option für die Eindämmung der durch Cyber-Angriffe zu befürchtenden Schäden die Entwicklung technischer Schutzmechanismen zu sein.

ERLEBEN, WAS VERBINDET.

DEUTSCHE TELEKOM AG
DR. THOMAS KREMER
Mitglied des Vorstands

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)636

19.02.2016 - 18/2695

5410

Stellungnahme

für die Öffentliche Anhörung des Verteidigungsausschusses des Deutschen Bundestages am 22. Februar 2016

"Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, Völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr"

Zunehmende Digitalisierung und die Folgen

Es gibt heutzutage keinen internationalen Konflikt mehr, der nicht auch virtuell, das heißt im Cyberraum ausgetragen wird: Von Propaganda und gezielter Desinformation bis hin zu Cyberangriffen auf Infrastrukturen, die die Lebensadern jeder Gesellschaft sind. Beispiele sind die Angriffe auf das Elektrizitätsnetz der Ukraine im Dezember oder die jüngsten Veröffentlichungen zum Angriff auf die iranischen Infrastrukturen. Wir stecken mitten in der Digitalisierung unserer Gesellschaft: Menschen, Maschinen und Geräte werden miteinander vernetzt und es entsteht eine Vielfalt an neuen Diensten und Nutzungsmöglichkeiten. Die Digitalisierung berührt alle Bereiche unseres Lebens: Arbeit, Freizeit, Bildung, Gesundheit, Sport, Glauben, Ethik. Nur ein Beispiel: Welches Wertegerüst gilt für selbstlernende Roboter, wer definiert es, wie sicher ist es? Solche Fragen sind heute keine Science Fiction mehr. Es ist letztendlich nur eine Frage der Zeit, bis ein ernsthafter Schaden durch Cyberangriffe auftritt, der auch eine konkrete Gefährdung für Leib und Leben bedeutet.

DEUTSCHE TELEKOM AG
Hausanschrift: Group Headquarters, Friedrich-Ebert-Allee 140, 53113 Bonn
Postanschrift: 53262 Bonn
Telefon: 0228 181-20101 | E-Mail: kremer@telekom.de | Internet: www.telekom.com
Konto: Postbank Saarbrücken, BLZ 590 100 66, Kto.-Nr. 166 095 662 | IBAN: DE0959010066 0166095662 | SWIFT-BIC: PBNKDEFF590
Aufsichtsrat: Prof. Dr. Ulrich Lehner (Vorsitzender) | Vorstand: Timotheus Höttges (Vorsitzender), Reinhard Clemens, Niek Jan van Damme, Thomas Dannenfeldt, Dr. Christian P. Illek, Dr. Thomas Kremer, Claudia Nemat
Handelsregister: Amtsgericht Bonn HRB 6794, Sitz der Gesellschaft Bonn | USt-IdNr. DE 123475223 | WEEE-Reg.-Nr. DE 50478376

Auswirkungen auf die Bundeswehr

Die Bundeswehr ist integraler Bestandteil unserer Gesellschaft. Auch sie ist von der fortschreitenden Digitalisierung unmittelbar betroffen. Im globalen Cyberraum verschwimmen nationalstaatliche Grenzen, Zeitzonen verlieren an Bedeutung und die Differenzierung von Freund und Feind wird zunehmend schwieriger, teilweise gar unmöglich.

Die Bundeswehr, die bisher hauptsächlich auf die Verteidigung der Landesgrenzen und damit die Sicherung der territorialen Integrität unseres Landes fokussiert war, muss sich auf die neue Bedrohungslage einstellen. Eine allein an nationalstaatlichen Grenzen orientierte „border control" – ohne digitale Landesverteidigung - reicht heute nicht mehr aus. Zugleich kann die Bundeswehr selbst Ziel von Cyberangriffen sein.

Gefahrenlage im Cyberraum

Die digitalen Bedrohungen umfassen gezielte Attacken auf staatliche Institutionen oder kritische nationale Infrastrukturen bis hin zu flächendeckenden Angriffen auf die infrastrukturellen Lebensadern ganzer Kontinente. Beispiele sind neben dem Cyberangriff auf den Deutschen Bundestag auch Angriffe auf Medien wie den französischen Fernsehsender TV5 und auf Infrastrukturen wie das ukrainische Stromnetz.

Die Deutsche Telekom identifiziert frühzeitig neue Angriffe auf ihre Infrastruktur und die dabei verwendeten Methoden. Unsere Sensoren im Netz – so genannte Honeypots - registrieren derzeit rund 4 Mio. automatisierte Angriffe auf die Deutsche Telekom pro Tag. Und wir stellen auch fest, dass individuelle Cyberattacken immer professioneller werden: Wir haben Fälle gesehen, in denen Angreifer in nur 6 Minuten die volle Kontrolle über ein System erhalten haben. Auch die Bürger erleben diese Gefahren immer konkreter: Laut einer aktuellen Umfrage von TNS Emnid im Auftrag der Deutschen Telekom ist fast jeder zweite Deutsche bereits Opfer von Cyberkriminalität geworden.

Weitere Fakten sind:

- Der geschätzte weltweite Schaden durch Cyberkriminalität betrug in 2014 laut den Experten von McAfee (Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies June 2014) bis zu 575 Mrd. USD.
- 51 Mrd. Euro beträgt nach aktuellen Schätzungen der jährliche Schaden für die deutsche Wirtschaft (Repräsentative Umfrage unter Unternehmen ab 10 Mitarbeitern im Auftrag des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. Bitkom, April 2015).
- Die durchschnittlichen Kosten pro Schadensfall betrugen für Großunternehmen 360.000 Euro, für kleine und mittelständische Unternehmen 41.000 Euro (Bitkom).
- 51% aller Unternehmen sind Opfer von digitaler Wirtschaftsspionage (Bitkom).
- 92% aller deutschen Unternehmen waren schon Opfer von Cyberangriffen, davon 61% aus dem Mittelstand (Bitkom).
- Die Zahl der Angriffe auf Industriesteuerungssysteme oder Smart Home Devices steigt stark an. Sogar Fernseher oder Haushaltsgeräte im privaten Umfeld werden zu neuen Zielen. Das wird durch aktuelle Medienberichte über Vorfälle in den USA deutlich, wo vernetzte TV-Geräte und sogar ein Kühlschrank für globale Cyberangriffe und den Versand von infizierten SPAM-Mails genutzt wurden.

Zum Vorgehen der Angreifer

Cybercrime ist ein florierendes illegales Geschäft mit hohen Margen und einem niedrigen Strafverfolgungsrisiko. Die Täter haben die Fähigkeit, hohe Summen in Cyber-Werkzeuge und Vorgehensweisen zu investieren. Oftmals ist das aber gar nicht nötig. Viele Unternehmen des Mittelstands machen es den Tätern zudem leicht: IT-Sicherheit wird bei den Investitionen oft vernachlässigt. Die besondere Schwierigkeit im Cyberraum ist darüber hinaus, dass weder Angriffsziel noch Angriffsart valide Schlussfolgerungen auf den tatsächlichen Angreifer zulassen. Als Angreifer können wir nur bestimmte IP-Adressen

identifizieren, ohne zu wissen, ob der Angriff tatsächlich von diesem System erfolgt oder ob es sich nur um ein Werkzeug handelt, das selbst von einem Command-and-Control-Server gesteuert wird. Diese Techniken sind dabei selbstverständlich nicht nur Kriminellen vorbehalten, sondern werden auch zum Beispiel von Geheimdiensten verwendet.

Für Cyberangriffe werden entweder spezifische Programme verwendet oder bestehende Sicherheitslücken in IT Systemen, insbesondere Software, ausgenutzt, mit der ein Angreifer zunächst einmal unbemerkt in die Systeme seines Zielobjektes eindringt. Dort kann er an sensible Informationen gelangen oder komplette Systeme so kompromittieren, dass sie nicht mehr funktionieren. Hinzu kommt: Das Tarnen, Täuschen und oft auch spurlose Verschwinden ist in der globalisierten digitalen Welt um ein Vielfaches einfacher als in der analogen.

Wiederverwendbare Cyberwaffen

Häufig wird die für Angriffe verwendete Software leicht verändert und von unterschiedlichen Tätergruppen gegen neue Ziele eingesetzt. Es gibt inzwischen sogar digitale Marktplätze im Netz, auf denen je nach Bedarf die gewünschten Schadsoftwaremodule gekauft und dann gegen ein gewünschtes Ziel in Stellung gebracht werden können. Primär wird das nach unserer Kenntnis von der organisierten Kriminalität bei Angriffen auf Unternehmen genutzt. Aber auch militärische Cyberwaffen werden von klassischen Tätergruppen wiederverwendet. Ein Beispiel dafür ist die Schadsoftware STUXNET. Mutmaßlich für Angriffe auf das iranische Atomprogramm entwickelt, wurde sie nach der Entdeckung durch Cyberkriminelle abgeändert und für deren Zwecke eingesetzt. Das macht deutlich, dass selbst hochentwickelte Cyberwaffen, die ursprünglich für militärische Zwecke entwickelt worden sind, einmal angewandt, kaum mehr zu kontrollieren sind.

Herausforderungen für die Bundeswehr

Anders als bei der konventionellen Kriegsführung stehen im Cyberraum bisher vor allem zivile Ziele im Fokus. Daher müssen sich Betreiber von kritischer Infrastruktur besonders

gegen virtuelle Angriffe schützen. Hierzu bedarf es einschlägiger Expertise und eines detaillierten Verständnisses, wie und mit welchen Methoden Cyberangriffe ausgeführt werden. Nur wer die Strategien und Methoden des digitalen Angreifers kennt, kann sich wirksam verteidigen. Die Bundeswehr steht dabei vor ähnlichen Herausforderungen wie die Wirtschaft.

Im Ergebnis kommt es für die Bundeswehr wie für zivile Unternehmen darauf an, die Angriffsflächen im Cyberraum zu minimieren, die eigenen Systeme zu härten und auf die Abwehr zukünftiger Angriffe zu fokussieren. Es werden neue Security-Kompetenzen bei Soldaten und Mitarbeitern ziviler Unternehmen benötigt, um aktuellen Gefahrenlagen besser begegnen zu können.

Zunächst einmal sind dafür die allgemein bekannten Sicherheitsmaßnahmen wie Schutz gegen Computerviren, Firewall Systeme aber auch regelmäßige Softwareupdates und Sicherheitstests einzusetzen. Um laufende Angriffe unterbinden zu können, ist aber mehr

erforderlich. Hier bedarf es insbesondere analytischer Fähigkeiten, um die Ursache und Wirkung eines individuellen Angriffs zu erkennen, um dann maßgeschneiderte Gegenmaßnahmen einleiten zu können. Da kaum ein Cyberangriff dem Anderen gleicht, ist in diesem Feld neben der Technologie der menschliche Faktor entscheidend. Für die erfolgreiche Abwehr von Cyberangriffen sind vertiefte Detailkenntnisse von Angriffstechniken und Werkzeugen zwingend erforderlich. Ob diese Fähigkeiten dann ausschließlich für die Abwehr oder auch für aktive Angriffe genutzt werden, ist keine technische Frage und keine Frage der Ausbildung. Unabhängig von diesen Kompetenzen sind außerdem sichere IT-Komponenten erforderlich, deren Hersteller fast ausschließlich nur noch im außereuropäischen Ausland zu finden sind. Deshalb ist es so wichtig, dass beim Thema Cybersicherheit die gesamte Wertschöpfungskette betrachtet wird: Von den Herstellern der Hard- und Software über die Betreiber der Infrastruktur bis zu den Diensteanbietern. Für alle müssen hohe Standards bei IT-Sicherheit und Datenschutz gelten – und das international.

Zur konkreten Beurteilung des Sicherheitsniveaus einer Komponente bedarf es ebenfalls tiefer Detailkenntnisse über Angriffstechniken und Werkzeuge. Sogenannte Penetrations- oder Sicherheitstests sind letztendlich nichts anderes als im Labor simulierte Cyberangriffe.

IT-Experten ausbilden

Für mehr IT-Sicherheit braucht es allerdings Fachkräfte, die heute am Markt kaum verfügbar sind. Die Rekrutierung von Experten aus anderen Ländern ist vielfach mit Risiken verbunden. In vielen Fällen haben sie in ihrem Herkunftsland für staatliche Institutionen oder Behörden gearbeitet. Der Fachkräftemangel an Cybersecurity-Experten wird für Unternehmen zunehmend zum Problem. Allein die Deutsche Telekom sucht bis 2018 über 300 qualifizierte Experten für unsere Business Unit Telekom Security. Um den eigenen Bedarf auch in Zukunft decken zu können, wurde begonnen, Cybersecurity-Spezialisten im Rahmen einer Kooperation mit der Industrie- und Handelskammer Köln selbst auszubilden. An der unternehmenseigenen Hochschule für Telekommunikation in Leipzig (HfTL) wurde darüber hinaus ein Lehrstuhl für Datensicherheit eingerichtet und besetzt. Auch die Bundeswehr könnte ihre renommierten Hochschulen, z.B. mit der Schaffung eines Cybersecurity Clusters, dafür einsetzen – vielleicht auch in Kooperation mit Unternehmen.. Insgesamt kann über die kommenden Jahre von einem vier- bis fünfstelligen Zusatzbedarf an derartigen Fachkräften ausgegangen werden. Parallel dazu sollte die

Forschungsförderung im Bereich der Cybersicherheit intensiviert und entsprechende Budgets bereitgestellt werden. Dabei ist es wichtig, mehr auf anwendungsorientierte Forschung zu setzen, deren Ergebnisse unmittelbar in den Schutz der kritischen Infrastrukturen einfließen können.

Digitale Verantwortung wahrnehmen

Es gibt keine Sicherheit, wenn wir die zunehmenden virtuellen Bedrohungen ignorieren. Dazu gehört, dass Sicherheit immer auch digital gedacht werden muss. Wir müssen uns alle der digitalen Verantwortung stellen. Dafür benötigen wir:

- Erstens: EU-weite und nationale Regeln, die für einen hohen Standard bei Datenschutz- und IT-Sicherheit sorgen. Hier hat die Bundesregierung mit dem IT-Sicherheitsgesetz einen Schritt in die richtige Richtung getan. Aber: Es muss die gesamte digitale Wertschöpfungskette berücksichtigt werden; nicht nur Netzbetreiber, sondern auch die Hersteller von Hard- und Software sowie sogenannte Over-the-top-Player müssen hier einbezogen werden. Es ist nicht konsequent, dass die beiden Letzteren bisher nicht verpflichtet sind, mehr Verantwortung für IT-Sicherheit in Europa zu übernehmen. Und das zeigt auch, dass wir global betrachtet leider immer noch weit davon entfernt sind, dass Sicherheit ein selbstverständliches Designkriterium für Telekommunikations- und IT- Produkte ist.
- Zweitens: Hohe Sicherheit der IT-Systeme von Staat und Wirtschaft. Keine Abhängigkeit von einzelnen Zulieferern und unabhängige Testcenter für Komponenten, die in kritischen Infrastrukturen eingesetzt werden.
- Drittens: Gut vernetzte schnelle Eingreiftruppen in Unternehmen und bei staatlichen Institutionen, die sich als Partner gegenseitig über neue Gefahren informieren. Wir brauchen mehr Transparenz über Cyberangriffe. Eine enge Zusammenarbeit von Unternehmen und Behörden untereinander und übergreifend, wie sie zum Beispiel zwischen dem Bundesamt für Sicherheit in der Informationstechnik und der Deutsche Telekom AG praktiziert wird, ist erforderlich. Durch einen intensiven Austausch kann sichergestellt werden, dass Sicherheitsvorkehrungen schneller getroffen werden – und so wird etwa verhindert, dass ein bestimmtes Angriffsmuster mehrfach erfolgreich ist. In diesem Zusammenhang sind auch klare Zuständigkeiten auf staatlicher Seite erforderlich, denn Cyber-Angriffe lassen sich nicht nach bestimmten Kriterien (kriminell/kriegerisch, Staat/Wirtschaft) trennen.

- Viertens: Einfache Lösungen für einen wirksamen Schutz von Informationen. Dazu gehören insbesondere die wirksame Ende-zu-Ende-Verschlüsselung sowie datenschutzfreundliche und sichere Lösungen für neue digitale Geschäftsmodelle.

Sicher ist: Cybersicherheit gibt es nicht zum Nulltarif. Verbraucher, Unternehmen und Staaten werden sich darauf einstellen müssen, für die virtuelle Sicherheit in Zukunft deutlich mehr Geld ausgeben zu müssen. Auch das bedeutet digitale Verantwortung.

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
18(12)640
22.02.2016 - 18/2702
5410

Stellungnahme zur Öffentlichen Anhörung des Verteidigungsausschusses des Deutschen Bundestages am 22. Februar 2016

„Die Rolle der Bundeswehr im Cyberraum - Verfassungs-, völker- und sonstige nationale und internationale rechtliche Fragen sowie ethische Aspekte im Zusammenhang mit Cyberwarfare und die hieraus erwachsenden Herausforderungen und Aufgaben für die Bundeswehr"

Schriftliche Stellungnahme von Dr. Marcel Dickow,
Leiter Forschungsgruppe Sicherheitspolitik, Stiftung Wissenschaft und Politik

Systematiken im Cyberraum

Im Datenraum (Cyberraum) sind klassische Paradigmen wie Angriff und Verteidigung, Unterscheidungen in rein defensive und offensive Fähigkeiten und das Prinzip der Territorialität wenigstens degeneriert, wenn nicht gänzlich aufgehoben. Das ist das Resultat besonderer technologischer Eigenschaften des Datenraums. Dazu zählen die logische Trennung von Daten und Infrastruktur, die Abstraktion von Software gegenüber der Hardware und die Möglichkeiten, die kryptologische, also mathematische Verfahren schaffen um Identifikation, Zurechenbarkeit und Aufklärung zu verhindern. Während Verteidigung in der realen, physischen Welt in einem kausalen, messbaren Verhältnis zum gerade ablaufenden Angriff oder gerade ablaufenden Angriffsvorbereitungen steht - sie ist die mittelbare oder unmittelbare Schutzreaktion auf (stattfindende oder unmittelbar bevorstehende) Gewaltausübung - fehlen solche Eindeutigkeiten im Cyberraum. Der Ursprung eines Angriffs kann hier selten direkt und unmittelbar beobachtet werden, eine Attribution ist wenn überhaupt nur mit erheblichem forensischen Aufwand im Nachhinein möglich. Oft scheitert sie gänzlich.

Konzepte von Verteidigung im Cyberraum können je nach Fähigkeiten, Strategie und politischer sowie rechtlicher Maßgabe unterschiedliche

Intensität, Reaktivität und Aggressivität aufweisen. Dieses Kontinuum beginnt beim rein passiven Eigenschutz von Infrastruktur, Diensten und Systemen. Schon das führt bereits zur Ausbildung offensiver Fähigkeiten. Nur wer in der Lage ist, den Schutz der eigenen, zu verteidigenden Systeme zu testen, kann sich einigermaßen wirksam und nachhaltig schützen. Das Testen ist allerdings ein Entwickeln und Üben von Angriffsfähigkeiten, wenngleich nur nach „innen" und nicht nach „außen" gerichtet. Damit verschwindet die technische Unterscheidung von defensiven und offensiven Maßnahmen, allein Intention und Ziel, also die Anwendung, bestimmen den Charakter des Mittels. Die komplexe Aufgabe des Infrastrukturschutzes beinhaltet folgerichtig ein kontinuierliches Angreifen eigener Systeme und die Implementierung daraus resultierender Erkenntnisse zur Verbesserung des Eigenschutzes. Zusätzlich müssen Fähigkeiten zur Detektion eines Eindringens (*intrusion detection*) eingesetzt und interne Dienste, Verkehre und Verhalten andauernd überwacht werden (*traffic and behavior monitoring*). Dieses Studium eigener Infrastruktur und Systemarchitektur generiert zusätzliches Wissen, das für offensive Mittel und Wirken genutzt werden kann. Um eine politische Schranke zwischen der Generierung von offensiven Wissen und der Entwicklung offensiver Fähigkeiten zu schaffen, hat die NSA bislang Eigenschutz und Operationen in fremden Netzen/Systemen institutionell getrennt gehalten[1].

Angriffe im Cyberraum

Angriffe auf IT-Systeme sind möglich, weil Hard- und Software systematische und/oder zufällige Schwachstellen (Verwundbarkeiten) aufweisen. Die Ursachen dafür sind vielfältig: *Security by design* ist noch immer keine Selbstverständlichkeit beim Entwickeln von Software, das Testen von Hard- und Software kann nicht beliebig intensiv durchgeführt werden, Systeme aus heterogenen Komponenten erzeugen unerwartete Fehlerquellen,

[1] Mit der aktuellen institutionellen Reform der NSA wurde diese Trennung aufgehoben. Siehe dazu z.B. „NSA merging anti-hacker team that fixes security holes with one that uses them | US news | The Guardian", zugegriffen 21. Februar 2016, http://www.theguardian.com/technology/2016/feb/03/nsa-hacker-cybersecurity-intelligence. Schon im Jahre 2013 hatte eine von Präsident Obama berufene Regierungskommission in den USA das Gegenteil empfohlen (siehe „Liberty and security in a changing world - Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies", 12. Dezember 2013, https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.).

benutzte Programmiersprachen und Compiler können selbst fehlerhaft und/oder veraltet sein, Überkomplexität, fehlerhafte Implementierungen, zu spätes Patchen (Fehlerbeseitigung) und menschliches Versagen stellen nur einige Ursachen dar. Nicht zuletzt ist Hardware und Software immer vom Menschen entwickelt und damit fehleranfällig, wenngleich inzwischen Teile von Softwareentwicklung und Programmierung automatisiert ablaufen können. Zum Schutz der eigenen Systeme müssen solche Schwachstellen möglichst schnell entdeckt und geschlossen werden. Angreifer jedoch sammeln und nutzen das Wissen um solche Verwundbarkeiten, um in gegnerische Systeme eindringen zu können[2]. Ungepachte Schwachstellen, sogenannte *0-day vulnerabilities*, stellen zusammen mit systematischen Verwundbarkeiten, z.B. unsicherer Hardware, das Haupteinfallstor dar. Staaten, staatliche Stellen und Streitkräfte geraten in einen nicht auflösbaren Interessenskonflikt, wenn sie gleichzeitig für den Schutz von IT-Infrastruktur und für offensive Cyber-Fähigkeiten zuständig sind. Das trifft um so mehr zu, wenn sie zum Schließen von Sicherheitslücken auf die Hilfe kommerzieller Unternehmen angewiesen sind. Dies ist die Regel in zivilen und staatlichen Netzen, die größtenteils proprietäre Software, wie z.B. Microsoft Windows, einsetzen. Dass solche Unternehmen zivile und militärische Netze ausrüsten, global Kunden akquirieren und diese mit Soft- und Hardware ausstatten, macht die beschriebenen Verwundbarkeiten zu einem Problem der internationalen (Cyber-)Sicherheit.

Schutz und Verteidigung im Cyberraum

Der Eigenschutz von Infrastruktur bietet nur relative Sicherheit. Wie in der zu schützenden Systemarchitektur können auch in der Sicherheitsarchitektur Schwachstellen und Lücken klaffen[3]. Dies ist statistisch gesehen bei komplexen Systemen sogar unvermeidbar. Entnetzung, Abschottung oder systematische, logische Begrenzungen innerhalb der Netze können das

[2] Dies geben inzwischen sogar staatliche Stellen, wie das FBI öffentlich zu: siehe „Meet the woman in charge of the FBI's most controversial high-tech tools - The Washington Post", zugegriffen 21. Februar 2016, https://www.washingtonpost.com/world/national-security/meet-the-woman-in-charge-of-the-fbis-most-contentious-high-tech-tools/2015/12/08/15adb35e-9860-11e5-8917-653b65c809eb_story.html.

[3] siehe z.B. das geringe Sicherheitsniveau von kommerzieller Anti-Virus-Produkten beschrieben bei „Mängel beim Selbstschutz von Antiviren-Software | heise Security", zugegriffen 21. Februar 2016, http://www.heise.de/security/meldung/Maengel-beim-Selbstschutz-von-Antiviren-Software-2465869.html.

Schutzniveau verbessern. Diese Maßnahmen können dauerhaft oder nur temporär, z.B. während eines Angriffs oder Eindringens, eingesetzt werden. Solange sie auf die eigene Infrastruktur begrenzt bleiben, entstehen keine völkerrechtlichen Grauzonen. Es gibt allerdings konzeptionelle Überlegungen, die Verteidigung gegen Angriffe bereits in die vorgelagerten Netzen Anderer zu tragen, wenn die eigenen Schutzsysteme nicht wirksam erscheinen oder technische Parameter dort höhere Erfolgsaussichten nahelegen. Konsequent zu Ende gedacht bedeutet eine solche Strategie, den Angreifer in seinem eigenen System anzugreifen während dieser von dort aus gerade operiert oder die Vorbereitungen dazu trifft. Die Identifikation des Angreifers ist aber nur dann eindeutig möglich, wenn der Angriff über alle benutzten eigenen und fremden Netze/Strukturen bis zu seinem Ursprung zurückverfolgt werden kann. Da bei komplexen Angriffsszenarien über das Internet nicht davon auszugehen ist, dass alle Betreiber der genutzten Kontenpunkte (augenblicklich, also während des Angriffs) kooperieren, ist der Angegriffene bei dieser Strategie gezwungen, selbst fremde Netze/Strukturen zu infiltrieren oder gar abzuschalten, um die Verteidigung wirksam werden zu lassen. Dieses Verfahren wird Counter-Hacking genannt und involviert zwangsläufig jene Dritte (bzw. ihre Netze/Strukturen), die der Angreifer zur Verschleierung seines Ursprungs genutzt hat. Nur bei Insider-Attacken in nach außen hin abgeschotteten Netzen ist eine solche, unmittelbare Verteidigungsstrategie erst einmal zwecklos.

Das Attributionsparadigma

Attribution von Cyber-Angriffen stellt also ein wesentliches, möglicherweise nie vollständig systematisch zu lösendes Problem des Cyberraums dar. Obwohl es forensische Instrumente gibt, die ein nachträgliches Bestimmen des Angreifers und seiner Herkunft gelegentlich ermöglichen, z.B. die Analyse des Angriffsquellcodes oder die Auswertung von Log- und Verkehrsdaten aller involvierten Netze, ist eine eindeutige Zuweisung von Angriffen zu (politischen oder institutionellen) Akteuren vermutlich nur dann realistisch, wenn der Angegriffene sich bereits im System des Angreifers befindet und somit den Beginn und Ablauf des Angriffs an seinem Ursprung mitverfolgen und nachweisen kann. Dieser Ansatz macht den Angegriffenen zum Angreifer und gefährdet die juristische Verwertbarkeit der so erlangten Beweismittel. In letzter Konsequenz führt dieser Ansatz die

danach handelnden Akteure dazu, zu jeder Zeit möglichst viele andere, gegnerische Systeme vorbeugend zu infiltrieren und somit ein Interesse an größtmöglicher Unsicherheit von IT-Systemen zu haben.

Charakteristika Digitaler Waffen

Digitale Waffen, also Schadcode (*malicious code*) zum Ausnutzen von Sicherheitslücken, beinhalten in der Regel weitere Funktionalitäten: (1) die Verhinderung bzw. Erschwerung der eigenen Entdeckung, (2) die Weiterverbreitung innerhalb bereits infiltrierter Systeme, (3) die Manipulation des Wirtsystems, (4) die Datenausleitung und (5) die Kommunikation zum *command and control server* zwecks Steuerung durch den Angreifer. Einmal entworfen müssen digitale Waffen ständig weiterentwickelt und an den Gegner und dessen IT-Systeme angepasst werden, und das in deutlich kürzeren zeitlichen Intervallen wie das bei herkömmlichen Waffensystemen notwendig ist. Neue Zugangsmöglichkeiten zum System des Angegriffenen (*0-day exploits*) müssen entdeckt, gesammelt und eingepflegt werden, das anzugreifende System muss unter ständiger Beobachtung - am besten von innen - stehen, um Abwehrmaßnahmen aufzuklären und um vor Entdeckung geschützt zu sein. Hard- und Software-Veränderungen beim Angriffsziel, die ein erfahrener Administrator neben systematischer Überwachung regelmäßig und quasi-willkürlich durchführt, müssen antizipiert und berücksichtigt werden. Deswegen werden digitale Waffen frühzeitig in gegnerischen Systemen platziert um im Angriffsfall bestmöglich auf das Angriffsziel vorbereitet zu sein[4]. Ist die digitale Waffe einmal eingesetzt, ist es nur noch eine Frage der Zeit, bis sie entdeckt und ihr Code analysiert bzw. *reverse-engineered* wurde. Deswegen sind digitale Waffen wartungsaufwändige Einmal-Wirkmittel, die zudem ein hohes Proliferationsrisiko aufweisen. Der Stuxnet-Angriff belegt dies eindrucksvoll. Trotz dieser Einschränkungen bleibt der Angreifer aber prinzipiell im Vorteil gegenüber dem Angegriffenen. Es ist leichter EINE neue Sicherheitslücke beim Gegner

[4] Wie weit solche Strategien gehen können, zeigen Gerüchte um das Programm „Nitro Zeus", über die der Dokumentarfilm „Zero Days" im Februar 2016 berichtet. Siehe dazu „U.S. Hacked Into Iran's Critical Civilian Infrastructure For Massive Cyberattack, New Film Claims - BuzzFeed News", zugegriffen 21. Februar 2016, http://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma#.qe7q1PkxX.

zu finden als ALLE vorhanden Sicherheitslücken (im eigenen System) zu schließen.

Digitale Waffen, also Angriffe im Cyberraum, können auf zivile wie militärische, auf geschlossene wie vernetzte Systeme geführt werden. Proprietäre, militärische Systeme können davon ebenso betroffen sein wie zivile, quelloffene Infrastruktur. Proliferation kann dazu führen, dass nach kurzer Zeit Trittbrettfahrer (wie die organisierte Kriminalität) militärischen Schadcode für Angriffe auf zivile Infrastruktur oder Computer nutzen, selbst wenn der ursprüngliche Angriff hochspezialisiert war (siehe Stuxnet). Der Trend in Streitkräften weltweit, zivile *commercial-off-the-shelf*-Technologie und IT einzusetzen, fördert das „Recyceln" militärischen Schadcodes zusätzlich.

Schlussfolgerungen für die Bundeswehr

Die Bundeswehr ist im Friedensfall, umso mehr im (Auslands-)Einsatz oder im Verteidigungsfall darauf angewiesen, ihre Netze und die dafür notwendige Infrastruktur gegen Angriffe von außen zu schützen. Im erklärten Verteidigungsfall kann sich diese Aufgabe zusätzlich auf die kritische, zivile Infrastruktur erstrecken, wie dies auch bei einem konventionellen Angriff gegeben wäre.

Neben der erforderlichen völkerrechtlichen Bewertung von Angriff und Verteidigung im Cyberraum bleiben politische Fragen bezüglich der Rolle und der Mittel der Bundeswehr. Erstens, soll und darf die Bundeswehr im Friedensfall Schutzfunktionen für kritische IT-Infrastruktur jenseits ihrer eigenen übernehmen? Zweitens, welche Mittel soll und darf sie zur Verteidigung (eigener und ziviler) Systeme einsetzen? Drittens, soll und darf die Bundeswehr offensive Fähigkeiten entwickeln und einsetzen?

1. *Soll und darf die Bundeswehr im Friedensfall Schutzfunktionen für kritische IT-Infrastruktur jenseits ihrer eigenen übernehmen?*

Mit Blick auf die Analyse von Systematiken und Charakteristika des Cyberraums plädiert der Autor für eine enge Beschränkung der Aufgaben der Bundeswehr im Friedensfall auf den Schutz eigener IT-Systeme. Das bedeutet nicht, dass Erkenntnisse über Verwundbarkeiten von IT-Systemen nicht mit anderen staatlichen Stellen zum Zwecke von deren Behebung geteilt werden sollen. Für den Schutz ziviler IT-Infrastruktur bedarf es ziviler,

unabhängiger Stellen, die in keinen Interessenskonflikt mit möglichen offensiven Fähigkeiten geraten können[5].

2. *Welche Mittel soll und darf die Bundeswehr zur Verteidigung (eigener und ziviler) Systeme einsetzen?*

Die Verteidigungsfähigkeit der Bundeswehr sollte im Friedensfall ausschließlich auf die eignen Netze und im Verteidigungsfall ausschließlich auf die eignen und die Netze der in den Konflikt involvierten Akteure (Gegner) beschränkt bleiben. Denkbare Angriffe im Zuge einer „aktiven" Verteidigung auf rein militärische Systeme[6] im Rahmen einer größeren, konventionellen Auseinandersetzung können wirksam und angemessen sein, bergen jedoch immer Eskalations- und Proliferationsrisiken. Eine solche Verteidigung wäre ohne intensive Vorbereitung nicht möglich und stellt de facto die Entwicklung von offensiven Cyber-Angriffsfähigkeiten dar. Der Autor rät in diesem Falle ebenfalls zu einem Verzicht bezüglich der Entwicklung dieser Einsatzmittel.

3. *Soll und darf die Bundeswehr offensive Fähigkeiten entwickeln und einsetzen?*

Vor dem Hintergrund der beschriebenen Eskalations-, Proliferations- und Sicherheitsrisiken rät der Autor generell davon ab, offensive Fähigkeiten im Cyberraum für die Bundeswehr zu entwickeln oder entwickeln zu lassen. Drei Gründe sind dafür besonders bedeutend: (1) Offensive Fähigkeiten im Cyberraum bedürfen offener Sicherheitslücken in Software, die im Allgemeinen auch eigene zivile und militärische System betreffen. Diese gezielt nicht zu schließen vergrößert die Risiken und unterminiert die internationale (Cyber-)Sicherheit. Zudem würde die Bundeswehr den globalen, kommerziellen Handel mit „0-days" weiter befeuern. (2) Vorbereitende Maßnahmen zum Entwickeln und für das Platzieren von Schadcode in gegnerischen Systemen führen auf einen Pfad, der beinhaltet, fremde Systeme generell als legitime Ziele aufzufassen und routinemäßig anzugreifen, um für den Ernstfall vorbereitet zu sein. Diese „Kolonialisierung des Netzes"[7] widerspricht der deutschen Kultur der militärischen Zurück-

[5] Der Autor plädiert an dieser Stelle für eine Unabhängigkeit des BSI vom Bundesministerium des Inneren und u.a. eine Beschränkung des BSI auf Daten- und Kommunikationssicherheit, den Schutz von kritischer IT-Infrastruktur sowie die (Entwicklung und) Zertifizierung von IT-Produkten.

[6] Z.B. die Sabotage von angreifenden Flugzeugen oder ihrer Command and Control (C2) Infrastruktur durch Schadcode.

[7] Vergl. Dokumente der NSA aus dem Fundus von Edward Snowden: „NSA/GCHQ: Das HACIENDA-Programm zur Kolonisierung des Internet | c't Magazin", zugegriffen 21. Februar

haltung und trägt große Eskalationsrisiken in sich, wenn sich dies als Staatenpraxis durchsetzt. (3) Die Entwicklung von offensiven Cyber-Angriffsfähigkeiten in und durch die Bundeswehr würde die Glaubwürdigkeit deutscher (Cyber-)Außenpolitik, vor allem in den Politikbereichen Internet Governance, Völkerrecht des Netzes und Menschenrechte online, massiv einschränken und damit gegen fundamentale ökonomische und menschenrechtspolitische Interessen der Bundesrepublik Deutschland verstoßen. Westliche Staaten wie die USA, Großbritannien und Frankreich haben diese Erfahrung in den vergangenen Jahren bereits gemacht. Diesem Beispiel sollte Deutschland nicht folgen.

2016, http://www.heise.de/ct/artikel/NSA-GCHQ-Das-HACIENDA-Programm-zur-Kolonisierung-des-Internet-2292574.html.

8

Ausgewählte, weiterführende SWP-Literatur:

Christian Schaller: *Internationale Sicherheit und Völkerrecht im Cyberspace*, SWP-Studie, Oktober 2014, http://www.swp-berlin.org/publikationen/swp-studien-de/swp-studien-detail/article/internationale_sicherheit_und_voelkerrecht_im_cyberspace.html.

Marcel Dickow: *Außenpolitik der Dienste - Die strategische Kommunikationsüberwachung und ihre Folgen*, SWP-Aktuell, Februar 2015, http://www.swp-berlin.org/fileadmin/contents/products/aktuell/2015A18_dkw.pdf.

Marcel Dickow und Oliver Meier: *Raus aus der Deckung! Rüstungskontrolle als Fundament einer modernen Ordnungspolitik*, Januar 2016, in Volker Perthes:
Ausblick 2016: Begriffe und Realitäten internationaler Politik, http://www.swp-berlin.org/fileadmin/contents/products/sonstiges/Ausblick2016.pdf#page=28.

Annegret Bendiek, Christoph Berlich und Tobias Metzger: *Drei Prioritäten für die Cyberdiplomatie unter dem deutschen OSZE-Vorsitz 2016*, SWP-Kurz-gesagt, November 2015, http://www.swp-berlin.org/publikationen/kurz-gesagt/drei-prioritaeten-fuer-die-cyberdiplomatie-unter-dem-deutschen-osze-vorsitz-2016.html.