unkorrigierte, maschinelle Abschrift

NDR Info Podcast **09.10.2021 / 19.35-20.00 Uhr**

STREITKRÄFTE UND STRATEGIEN **10.10.2021 / 12.35-13.00 Uhr**

Joachim Hagen/Julia Weigelt E-Mail: streitkraefte@ndr.de

www.ndr.de/streitkraefte

Themen:

- Ampel oder Jamaika? Mögliche Folgen für Bundeswehr und Sicherheitspolitik
- SCHWERPUNKT
  Cyberattacke – Gefahr für die internationale Sicherheit?
- SICHERHEITSPOLITISCHE NOTIZEN
  - Nach sechs Jahren – Gorch Fock wieder bei der Marine
  - Nicht mehr zeitgemäß? Bundeswehr-Tornados üben Atomwaffeneinsatz

Abschrift Schwerpunkt

Hagen:
Willkommen, mein Name ist Joachim Hagen. Mit im Studio ist meine Kollegin Julia Weigelt. Hallo Julia.

Weigelt:
Moin, Moin!

Hagen:
In unserem Schwerpunkt geht es heute um die Bedrohung durch sogenannte Cyberangriffe. Früher waren Computerviren und andere Schadprogramme vor allem eine Gefahr für Wirtschaftsunternehmen. Es ging darum, Geld zu erpressen. Aber inzwischen bedrohen solche Cyberangriffe auch staatliche Institutionen und nationale Versorgungsstrukturen.

Weigelt:
Cyberattacken waren auch ein wichtiges Thema während des Genfer Gipfels im Sommer, zwischen US-Präsident Biden und dem russischen Präsidenten Putin. Beide Seiten werfen sich vor, hinter großangelegten Cyberangriffen zu-

stecken. Grund genug zu fragen, ob diese Attacken aus dem Cyberraum letztlich zu Konflikten mit konventionellen Waffen führen können, zu einer kriegerischen Auseinandersetzung zwischen Staaten. Mit dem Thema hat sich in den vergangenen Wochen Jerry Sommer intensiv beschäftigt. Er ist uns nun aus Düsseldorf zugeschaltet. Hallo Jerry.

Sommer:
Hallo Joachim, hallo Julia.

Weigelt:
Jerry, zunächst mal zur Dimension von Cyberattacken. Es häufen sich die Meldungen über Cyberangriffe. Was weiß man über das Ausmaß der Angriffe?

Sommer:
Also es sind unzählige, eine genaue Zahl über die weltweit stattfindenden Attacken, das gibt es gar nicht. Man sollte, finde ich, aber auch zuerst einmal definieren was Cyberangriffe oder Cyberattacken eigentlich sind. Der digitale Raum spielt ja für alle Menschen, Wirtschaft, Staat, Militär eine immer größere Rolle. Als Cyberangriffe, glaube ich, sollte man allerdings nur ansehen, was unbefugt in den Cyberraum von jemand anderem eingreift. Und das kann ganz unterschiedliche Sachen beinhalten. Abhören oder Mitlesen von Nachrichten oder auch der Sprachkommunikation - das kann man ganz allgemein als Spionage bezeichnen. Das kann ausgehen von Einzelpersonen, Unternehmen, aber auch von staatlichen Institutionen wie Geheimdiensten und Militärs. Dann gibt es Angriffe, mit denen Rechner lahmgelegt werden. Das sind vor allen Dingen Erpressungsversuche. Die eingeschleuste Schadsoftware wird erst wieder gelöscht, wenn Geld gezahlt wurde.

Hagen:
So war es ja im Mai dieses Jahres, als das Unternehmen Colonial Pipeline in den USA gehackt wurde. Da blieben zahlreiche Tankstellen ja ohne Sprit.

Sommer:
Ja, das war ein Angriff, für den man russische kriminelle Hacker verantwortlich macht. Da flossen dann Millionen Dollar Erpressungsgelder. Aber die überwiegende Mehrzahl der Cyberangriffe besteht aus solchen kriminellen Aktivitäten. Hinzu kommen sicherlich auch Einflussoperationen im Netz, mit denen also Meinungen und Stimmungen, zum Beispiel im eigenen oder auch in einem fremden Land über das Internet beeinflusst werden sollen. Und schließlich muss man Sabotageoperationen nennen.

Weigelt:
Zu den bekanntesten Sabotageoperationen gehören ja die Sabotageoperationen gegen drei ukrainische Stromverteilerstationen, 2015. Da gab es ja dann einen mehrstündigen Stromausfall. Und wir erinnern uns auch noch an den Angriff auf die iranische Urananreicherung mit dem Stuxnet-Virus, vermutlich von Israel und den USA. Da wurden ja vor zehn Jahren tausend iranische Zentrifugen zerstört.

Sommer:
Ja, das sind zwei Beispiele für Sabotage. Allerdings warnen viele Experten davor, diese ganzen Angriffe unter dem Oberbegriff Cyberkrieg zu fassen. Der Cyberexperte des Instituts für Friedensforschung und Sicherheitspolitik, IFSH in Hamburg, Mischa Hansel, weist auch auf den Stuxnet-Angriff hin, aber möchte solche Attacken folgendermaßen einordnen.

O-Ton Hansel:
„Aus wissenschaftlicher Perspektive ist Krieg normalerweise mit physischer Zerstörung verbunden. Das ist durchaus möglich im Cyberraum. Wir haben ja zum Beispiel die Manipulation der Zentrifugen in der iranischen Nuklearanreicherung gesehen, 2010 und 2011. Aber trotzdem müssen wir feststellen, dass ganz überwiegend Cyberattacken für Spionagezwecke eingesetzt werden oder im Bereich von Cyberkriminalität zu verorten sind.“

Weigelt:
Das heißt also, der Angriff auf die iranischen Zentrifugen, das war eher ein untypischer Cyberangriff, so habe ich Mischa Hansel verstanden. Cyberangriffe haben vielmehr das Ziel, in die Datennetze einzudringen, um Informationen zu

beschaffen. Und da geht es den Täterinnen und Tätern vor allem um das Ausspähen oder Erpressen. Welche größeren Angriffe sind denn da bekannt geworden? Ich erinnere mich noch an den auf das Pentagon. Die Opfer solcher Angriffe machen ja diese Attacken lieber oft nicht publik.

Sommer:
Ja, im Juni 2020 hat eine Attacke nicht nur viele Unternehmen und Regierungsbehörden in den USA, sondern auch das Pentagon getroffen. Allerdings sollen da keine wichtigen nationalen Sicherheitsfunktionen betroffen gewesen sein. Und auch die Bundeswehr erklärt, um mal jetzt bei den militärischen Institutionen zu bleiben - auch die Bundeswehr erklärt, dass allein 2019 über fünf Millionen Cyberangriffe auf ihren Systemen erkannt und abgewehrt wurden. Genaues weiß man natürlich nicht. Und ich teile die Vermutung, dass bei wirklich großen gravierenden Angriffen auf das Militär, diese vom Militär nicht an die große Glocke gehängt werden.

Hagen:
Es haben ja auch die Streitkräfte vieler Staaten seit einiger Zeit sogenannte Cyberkommandos. Das heißt, auch die Streitkräfte planen Cyberoperationen und führen diese durch. Geschieht dies nur bei einer bewaffneten Auseinandersetzung, also im Krieg, oder auch in Friedenszeiten?

Sommer:
Also Aufklärung oder Spionage mit Cyberoperationen - wie man das nennt, das liegt sicherlich im Auge des Betrachters - spielt auch in Friedenszeiten schon eine große Rolle. Im Krieg weiß man natürlich nicht so genau, was das Militär gemacht hat, zum Beispiel in Syrien, im Irak und in Afghanistan. Aber einige Sachen sind da schon bekannt geworden, dass - außer Aufklärung durch Abhören und Mitlesen von Nachrichten feindlicher Kräfte - zum Beispiel die USA eine Website des sogenannten Islamischen Staates gehackt und manipuliert haben. Es ist auch bekannt, dass die Israelis 2007 syrische Radaranlagen gehackt haben, bevor sie eine im Bau befindliche Nuklearanlage mit Bomben zerstört haben.

Weigelt:
Du hast eben mal von Aufklärung gesprochen und dann auch von Spionage - und wenn ich dich richtig verstanden habe, werden hierfür auch Cyberoperationen genutzt. Man versucht, in gegnerische Daten oder Telefonnetze reinzukommen. Sind Aufklärung und Spionage nicht zwei rechtlich unterschiedliche Kategorien, gerade in Friedenszeiten? Aufklärung ist da doch eher das legitime Sammeln von Informationen, während man bei der Spionage illegal Daten sammelt, also Gesetze verletzt, oder?

Sommer:
Also ich bin kein Jurist - aber bei Cyberoperationen geht es ja darum, in fremde Netze einzubrechen, um unter anderem eben Informationen zu sammeln. Also wenn man zum Beispiel daran zurückblickt: die US-Geheimdienste haben ja selbst das Handy der Bundeskanzlerin abgehört. Und wahrscheinlich haben sie das als Aufklärung angesehen und betrachtet, weil sie ja aufklären wollten, was die Bundeskanzlerin so denkt und macht. Wenn man Cyberoperationen durchführt, zum Beispiel, um terroristischen Angriffen zuvorzukommen, kann man das sicherlich auch als Aufklärung ansehen. Und natürlich gibt es auch Aufklärungsmittel, die ohne Zweifel legal sind – zum Beispiel Radarsysteme, die Flugzeuge oder Raketen erfassen. Aber wenn man zur Informationsbeschaffung in Netze anderer eindringt, scheint mir der Begriff Spionage doch angemessen zu sein.

Hagen:
Ich möchte mal auf die Fragestellung unseres Podcasts zu sprechen kommen, „Cyberangriffe - eine unterschätzte Gefahr für die internationale Sicherheit?“, so heißt es da ja. Gefährden denn nun Cyberattacken die Stabilität? Können sie zu einer Eskalation führen, bis hin zu bewaffneten Konflikten?

Sommer:
Die Cybersicherheitsexpertin der Berliner Stiftung Wissenschaft und Politik, Annegret Bendiek, hat in einem Interview mit mir die Gefahren für die Staaten

der Europäischen Union durch Erpressungsangriffe, zum Teil auch auf Krankenhäuser und andere kritische Infrastrukturen, hervorgehoben.

O-Ton Bendiek:

„Hacker hatten dann Konten von mehreren Zehntausenden von Kunden, um dann Lösegeldforderungen anzufordern, um diese Daten wieder freizugeben. Aber auch bis hin zu Angriffen auf Lieferketten, Cloud-Infrastrukturen. Das ist schon etwas, was für den Binnenmarkt, für die Europäische Union, für die politische Sicherheit oder Stabilität hier in Europa sehr essenziell ist."

Hagen:

Aber kann man denn sagen, dass damit die internationale Sicherheit gefährdet ist? Die NATO geht inzwischen davon aus, dass Cyberangriffe auch den Bündnisfall auslösen können.

Sommer:

Also ich denke, man sollte die Gefahren durch Cyberangriffe weder untertreiben, noch übertreiben. Einen bewaffneten Konflikt zwischen Großmächten, der mit Angriffen beginnt, den kann ich mir nur unter ganz bestimmten Bedingungen vorstellen. Dass nämlich die politische und militärische Eskalation schon vorher sehr weit fortgeschritten sind. Dann sind Cyberangriffe sozusagen Teil einer militärischen Operation. Etwas anderes ist es aber, wenn Cyberangriffe das Verhältnis zwischen Staaten, Großmächten, die sich nicht sonderlich wohlgesonnen sind, zum Beispiel negativ beeinflusst und damit eben auch internationale Spannungen erhöht. Trotzdem halte ich es für ziemlich unwahrscheinlich, dass zum Beispiel aus Cyberangriffen auf Krankenhäuser, die ja zweifellos Menschenleben gefährden, militärische Auseinandersetzungen entstehen. Auch Erpressungen von Unternehmen, was ja auch hohe finanzielle Schäden verursacht, werden höchstwahrscheinlich nicht zu bewaffneten Auseinandersetzungen führen. Aber es gibt zwei Gefahren oder zwei Wege, die zu einer vor allem auch erst einmal politischen Eskalation schon in Friedenszeiten führen können. Mischa Hansel vom Hamburger Institut für Friedensforschung und Sicherheitspolitik zum Beispiel, hält das für möglich, wenn Hacker kritische Infrastrukturen angreifen - nicht nur das Gesundheitswesen, vielleicht auch das System der demokratischen Wahlen, Wasser und die Energieversorgung. Und zwar, wenn man annehmen kann, dass diese Angriffe von Hackern im Auftrag

oder auch nur mit Duldung von anderen Staaten ausgeübt worden sind. Das wirft man ja Russland und China zum Beispiel vor, dass die Länder Hacker dulden oder gar beauftragen. Ob allerdings diese Eskalation wirklich über politische und ökonomische Sanktionen oder vielleicht auch kleinere Gegenhackerangriffe hinausgeht und zu bewaffneten Auseinandersetzungen führen könnte, das halte ich doch für sehr fraglich. Aber prinzipiell sieht Mischa Hansel vom IFSH darin natürlich eine Eskalationsmöglichkeit. Und eine zweite Eskalationsgefahr sieht er in den zunehmenden gegenseitigen Bemühungen, auch gerade von Großmächten, in die Kommando- und Kontrollsysteme der Gegenseite durch Cyberangriffe einzubrechen. Mischa Hansel.

O-Ton Hansel:

„Bei der Frühwarnung vor Nuklearschlägen oder eben bei der Kontrolle von Nuklearwaffen selber, von eigenen Nuklearwaffen. Hier ist das Risiko nicht so sehr der bewusste Kriegsakt, aber eben die Möglichkeit, dass Spionageaktivitäten fehlgedeutet werden und, dass Nuklearmächte dann denken, dass ihre eigene strategische Abschreckung in Frage gestellt ist und wir dann dadurch eben eine internationale Eskalation sehen."

Sommer:

Um das noch ein klein wenig zu erläutern: Er sieht das Problem also vor allem darin, dass die Angegriffenen nicht wissen, ist der Gegner nur in unseren Systemen, um uns auszuspionieren, oder hat er auch Schadsoftware eingepflanzt in unsere Systeme, zum Beispiel, um unsere Frühwarnfähigkeiten auszuschalten oder manipulieren zu können?

Weigelt:

Was weißt du denn darüber, inwieweit die USA, China oder Russland, um jetzt noch mal so die größten Player zu nennen, kritische Infrastruktur oder gar militärische Kontroll- und Kommandozentralen der anderen gehackt haben?

Sommer:

Also, darüber weiß man wirklich nicht viel Genaues. Es gibt aber, zum Beispiel einen New York Times-Artikel von 2019. Darin wird berichtet, dass amerikanische Geheimdienste Schadsoftware in das russische Stromnetz eingeschleust hätten. Auch Präsident Biden hat dieses Jahr im Juni in Genf auf seiner Pres-

sekonferenz nach dem Treffen mit Putin erklärt - Zitat: „Wir haben erhebliche Cyberfähigkeiten, die wir auch einsetzen würden.“ Zitatende. Und er sprach ausdrücklich die russische Ölindustrie an, als mögliches Ziel für Vergeltungsangriffe auf die kritische Infrastruktur der USA. Und auch der Cybersicherheitsexperte Matthias Schulze von der Stiftung Wissenschaft und Politik, hält es für höchstwahrscheinlich, dass die Großmächte schon jetzt - in Friedenszeiten - in den Netzen des Gegners aktiv sind. Das sagte er in einem Podcast seiner Stiftung.

O-Ton Schulze:

„Weil Cyberangriffe vorbereitet werden müssen und eben nicht in zeitkritischen Situationen so schnell verfügbar sind, machen das Staaten im Vorfeld schon - und zwar die ganze Zeit - nämlich in Friedenszeiten. Das heißt, sie dringen gegeneinander in ihre sensiblen Netzwerke ein: Verteidigungsministerien, Auswärtige Ämter, kritische Infrastrukturbetreiber, Energie, Wasserwerke - aber auch Rüstungsunternehmen und Rüstungstechnologie allgemein, um frühzeitig an Informationen zu kommen, um für den Fall eines Konfliktes irgendwann in der Zukunft schon Vorbereitungs- oder Vorlaufzeit zu haben, um dann relativ schnell eine Schadsoftware schreiben zu können.“

Hagen:

Also Matthias Schulze geht davon aus, dass die großen Akteure bereits in den Netzwerken der anderen Seite sind - dass die Großmächte Software oder Trojaner längst installiert haben, die dann bei einer Auseinandersetzung nur noch aktiviert werden müssen. Im Extremfall vielleicht sogar in den Kommandostellen eines Gegners, sodass beispielsweise Raketenstarts oder die Kommunikation zwischen militärischen Einrichtungen lahmgelegt werden könnte. Oder kann man das ausschließen?

Sommer:

Das kann man sicherlich nicht ausschließen. Aber auch hier gilt: man darf die Gefahr nicht überschätzen. Öffentlich bekannt ist da nicht viel. Aber ich denke, man kann davon ausgehen, dass zumindest die Großmächte sehr genau darauf achten, dass ihre Kommandozentralen und ihre Raketenanlagen und Kommunikation mit entsprechenden Anlagen - dass diese gut geschützt sind. Und man sollte auch noch etwas anderes bedenken: Man weiß natürlich auch nicht, ob die Spionage- oder Sabotagesoftware, die beim Gegner eingepflanzt

ist, ob die nicht schon längst erkannt worden ist, und ob sie wirklich dann funktioniert oder eben nicht funktioniert. Aber zweifellos - solche Schadsoftware einzupflanzen, das ist schon eine gefährliche offensive militärische Operation. Und wenn alle das machen, würde das natürlich in den ganzen internationalen Beziehungen die Unsicherheit erheblich steigern.

Hagen:
Also das heißt doch, dass es zu einer solchen Instabilität und Verunsicherung durchaus kommen kann. Und wenn eine Seite dann glaubt, dass beispielsweise eigene strategische Raketen lahmgelegt worden sind, dann könnte sie auch glauben, dass ein gegnerischer Atomangriff unmittelbar bevorsteht oder sogar schon begonnen hat. Mich erinnert dieses Szenario ja an den Film „Dr. Seltsam oder: Wie ich lernte, die Bombe zu lieben“ von Stanley Kubrick. Und die Folge könnte nun sein, die vermeintlich angegriffene Seite startet mit dem restlichen Waffenarsenal einen nuklearen Vergeltungsschlag. Die Folge wäre ein Nuklearkrieg aus Versehen. Ist so ein Horrorszenario wirklich denkbar oder eben doch nur eine Hollywood-Phantasie?

Sommer:
Also ausschließen kann man sicherlich nichts. Aber ich würde das auf keinen Fall als einen Nuklearkrieg aus Versehen betrachten. Wenn eine Seite zum Beispiel Überwachungsfähigkeiten der anderen Seite lahmlegt, dann geschieht das eigentlich nur, wenn man danach angreifen will. Und insofern würde es dann zur Katastrophe kommen. Aber das würde nicht aus Versehen geschehen, sondern, weil man mit Cyberoperation sozusagen ein Krieg begonnen hat.

Weigelt:
Also es besteht schon eine Gefahr, dass Cyberattacken zu Missverständnissen und vielleicht sogar bewaffneten Konflikt führen könnten. Und auch deshalb haben ja Putin und Biden in Genf beschlossen, eine Arbeitsgruppe zum Thema Cybersicherheit zu bilden. In der UNO gibt es ja schon seit vielen Jahren Diskussionen über eine diplomatische Einhegung der Cybergefahren. Ist das denn ein erfolgversprechender Weg?

Sommer:
Also, ich denke, man muss zwei Tendenzen sehen, die als Antwort auf die wachsenden Cybergefahren gelten. Und das eine ist der diplomatische Weg, aber das andere ist das Setzen auf offensive Cyberfähigkeiten, um damit den potenziellen Gegner abzuschrecken oder auch bekämpfen zu können.

Hagen:
Okay, dann eins nach dem anderen. Stellen wir also die diplomatischen Lösungsbemühungen erst einmal zurück. Zunächst also zur Frage, ob man Cyberattacken durch Abschreckung verhindern kann. Ob - etwas überspitzt formuliert - das Prinzip der nuklearen Abschreckung in einem gewissen Sinne übertragbar ist. Du hast ja am Anfang bereits Präsident Biden zitiert, nach dem Genfer Gipfel mit Putin. Biden hat Russland für Cyberangriffe verantwortlich gemacht und damit gedroht, die USA hätten ebenfalls erhebliche Cyberfähigkeiten, die man auch einsetzen würde. Diese Drohung ist doch Abschreckung. Würde sie aber auch funktionieren? Was sagen die Experten?

Sommer:
Also, zuerst einmal denke ich, sollte man darüber nachdenken, ob nicht der Schutz der eigenen Systeme die beste Abschreckung vor Cyberangriffen ist - von wem auch immer diese Angriffe ausgehen. Auf die Defensive als Schwerpunkt - dafür plädieren eine Reihe von Experten. Manche warnen zudem davor, die Abschreckungswirkung von offensiven Cyberoperation zu überschätzen. Gerade heute gibt es ja im Unterschied zur nuklearen Abschreckung im Kalten Krieg, viele Akteure. Kleinere Staaten, nichtstaatliche Gruppen, Terroristen, Kriminelle - alle können Cyberoperationen durchführen. Und ob die sich abschrecken lassen, ist fraglich. Und dann gibt es noch ein Problem: nämlich das Problem der Verschleierung und damit dass der sogenannten Attribution, also der Feststellung, wer für die Angriffe verantwortlich ist. Was ist zum Beispiel, wenn jemand - seien es Staaten oder Kriminelle - zum Beispiel Angriffe auf Krankenhäuser in einem anderen Land durchführen, aber von einem Server eines Krankenhauses aus, möglicherweise eines Krankenhauses in einem dritten Land? Ein Hackback, ein Cybergegenangriff, könnte dann weitere Men-

schenleben dort gefährden, aber die Kriminellen nicht wirklich treffen. Und wenn Staaten so etwas dann machen, wäre ihnen internationale Kritik sicher.

Weigelt:
Wenn also so eine Abschreckung von Cyberattacken schwierig ist und man sich nicht nur auf die Abwehr von Cyberangriffen festlegen will, dann ist es doch eine weitere Möglichkeit zu versuchen, den Angreifer selbst auszuschalten. Indem man ihn lokalisiert und dann selbst angreift und seinen Server oder sein Netz lahmlegt. Vor allem, wenn dieser Angreifer Teile der eigenen kritischen Infrastruktur attackiert, also Krankenhäuser, Energieversorgungssysteme, Flughäfen zum Beispiel. Ein Angriff würde dann mit einem Gegenangriff beantwortet. Wie schätzt du so ein offensives Vorgehen ein?

Sommer:
Das könnte in einzelnen Fällen vielleicht helfen. Oo hat ja der US-Geheimdienst die Sankt Petersburger Trollfabrik eine zeitlang ausgeschaltet, als diese Einflussoperationen in den USA durchgeführt hat. Aber die Meinungen über den Nutzen einer solchen offensiven Vorwärtsverteidigung gehen ziemlich auseinander. Die US-Administration unter Trump hat erheblich auf eine solche offensive Vorwärtsverteidigung gesetzt. Ob Präsident Biden da zurückrudert, ist noch nicht wirklich klar. Aber das Problem darf man auf keinen Fall unterschätzen. Es ist außerordentlich schwer oder sogar unmöglich, die Herkunft eines Angriffs eindeutig und öffentlich nachvollziehbar zu bestimmen.

Hagen:
Und das ist ja offenbar genau das Problem. Man kann nicht mit Sicherheit feststellen, wer der Angreifer ist. Man könnte daher den Falschen treffen, wenn man einen Gegenangriff startet – man könnte mit einem Cybergegenangriff sogar einem militärischen Schlag durch konventionelle Waffen auslösen.

Sommer:
Das sehe ich genauso. Denn es ist relativ einfach möglich, Operationen im Cyberraum so zu manipulieren, dass man sie einer anderen Seite in die Schuhe schieben kann. Wikileaks hat zum Beispiel 2017 Dokumente veröffentlicht, aus

denen hervorgeht, dass die CIA, der amerikanische Geheimdienst, Programme entwickelt hat, und zwar in Chinesisch, Russisch, Koreanisch, Persisch, Arabisch, damit auch diese Staaten für solche Angriffe verantwortlich gemacht werden können. Und andere Großmächte können und haben das vielleicht genauso gemacht. Und selbst wenn man nicht durch die Forensik, sondern durch andere Indizien und politische Einschätzung meint, eine klare Zuordnung eines Cyberangriffs benennen zu können, kann man total daneben liegen. Ein Beispiel nennt Matthias Schulze von der SWP.

O-Ton Schulze:

„2015 gab es einen Vorfall, wo der französische TV-Sender TV5 Monde gehackt wurde. Und da haben die Hacker so getan, als wären sie ein Cyber Caliphate, also ein Cyberkalifat. Das war die Zeit, wo die Terrorangriffe des Islamischen Staates in Europa sehr stark waren. Und dann dachten alle: okay, der IS hat den TV-Sender gehackt. Es stellte sich aber dann später, Jahre später heraus, dass das eine Operation unter falscher Flagge war. Das heißt, das war gar nicht der Islamische Staat, sondern es waren vermutlich russische Hacker, die unter falscher Flagge den Hack durchgeführt haben."

Weigelt:

Also noch mal zusammengefasst: Es ist einfach schwer zu erkennen, von wem man im Internet angegriffen wird, trotz IP-Adresse oder anderer Spuren. Das heißt, es besteht wirklich die Gefahr, wenn man tatsächlich zurückschlagen will, dass man Unbeteiligte angreift. Und das könnte dann erst recht zu einer Eskalation führen.

Sommer:

Ja. Das kann auch andere Kollateralschäden zur Folge haben. Die Schadsoftware könnte sich ausbreiten und auch andere Computer und Netzwerke beschädigen - nicht nur die, die man eigentlich angreifen wollte. So hat der Stuxnet-Virus nicht nur die iranische Urananreicherungsanlage getroffen. Er hat weltweit auch eine Reihe von Industrieanlagen befallen, die natürlich von den US-Geheimdiensten - oder wer auch immer das gemacht hat - nicht getroffen werden sollten. Deshalb warnen Cyberexperten, wie Mischa Hansel davor, offensive Maßnahmen und Hackbacks im Cyberraum für die beste Verteidigung zu halten.

O-Ton Hansel:

„Da, glaube ich, spricht vieles dagegen. Und man sieht natürlich auch das Risiko, dass die eigenen, die wirklichen Defensivmaßnahmen, vernachlässigt werden, weil man glaubt, dass man mit der Vorwärtsverteidigung das dann nicht mehr braucht."

Hagen:

Die Bundeswehr hat ja seit einigen Jahren ebenfalls ein eigenes Cyberkommando. Insgesamt umfasst es bis zu 14.000 Soldaten und Soldatinnen. Nach dem eigenen Selbstverständnis liegt die Kernaufgabe darin, Cyberangriffe abzuwehren. Oder wird inzwischen auch darüber nachgedacht, gegebenenfalls auch zum Gegenangriff überzugehen, also diese sogenannten Hackbacks auszuführen?

Sommer:

Dass die Bundeswehr auch an Hackbacks arbeitet - das kann man vermuten, aber genau wissen das auch Experten nicht - jedenfalls Experten außerhalb der Bundeswehr. Man kann aber sicher sein, wie du gesagt hast, dass die Hauptaufgabe des Kommandos „Cyber- und Informationsraum" der Bundeswehr, in der Bereitstellung und im Schutz der eigenen Netzwerke liegt. Ob nun in Deutschland oder in Einsatzorten der Bundeswehr im Ausland. Und man sollte auch darauf hinweisen: die Bundeswehr ist ja in Bezug auf die Cybersicherheit Deutschlands nur ein Teil der Sicherheitsarchitektur und nur für die militärische Sicherheit zuständig. Doch Innenminister Seehofer hat ganz generell von Hackbacks gesprochen, die in kürzester Zeit entschieden werden müssten. Für die Bundeswehr sieht Annegret Bendiek vom SWP da einen gewissen Spielraum bei Gefahr im Verzug.

O-Ton Bendiek:

„Das kennen wir auch schon aus anderen Auslandseinsätzen der Bundeswehr, wo dann im Nachhinein die Bundestagszustimmung eingeholt wurde und auch die Rechtfertigung dazu stattgefunden hat. Sicherlich, auch da gehört es nochmal auch auf den Tisch, inwieweit da die parlamentarische Einbindung möglich ist. Aber die bleibt nach wie vor sehr wichtig, auch wenn wir da im europäischen Rahmen uns abstimmen."

Weigelt:
Du hast eben erwähnt, die Bundeswehr sei mit ihrem Cyber-Kommando vor allem für die Sicherheit der militärischen Einrichtungen zuständig. Wenn es um den Schutz des Bundestags oder auch anderer deutscher Einrichtungen geht, dann hat das Innenministerium das Sagen. Inwieweit arbeiten denn Bundeswehr und Innenministerium zusammen, wenn es um die Abwehr von Cyberangriffen geht? Gibt es dafür spezielle Einrichtungen?

Sommer:
Ja. Im Nationalen Cyber-Abwehrzentrum ist die Bundeswehr sowohl mit dem militärischen Abschirmdienst als auch mit dem Kommando „Cyber- und Informationsraum“ vertreten. Daneben sind dort noch andere Behörden vertreten wie Polizei, Bundeskriminalamt und Bundesnachrichtendienst. Und das Bundesverteidigungsministerium gehört, wie viele andere Ministerien und Bundesländer, dem sogenannten Nationalen Cyber-Sicherheitsrat der Bundesregierung an.

Hagen:
Du hast ja über offensive Cyberoperationen gesprochen, über das sogenannte Hackback. Diese Maßnahme ist in Deutschland sehr umstritten. Nur noch einmal zum Verständnis: Wenn die Bundeswehr oder das Cyberkommando zu dem Ergebnis kommt, man müsste den Server angreifen, von dem ein Cyberangriff ausgeführt wird, müsste dieser Aktion dann letztlich auch der Bundestag zustimmen - gegebenenfalls nachträglich? Wäre das nicht gleichzusetzen mit einem bewaffneten Einsatz der Bundeswehr? Bei Auslandseinsätzen muss der Bundestag ja auch zustimmen. Oder sind das alles Fragen, die noch gar nicht geklärt sind?

Sommer:
Also sicher ist da noch nicht alles geklärt. Aber ich denke, es dürfen nicht die Bundeswehr oder das Bundeswehr-Cyberkommando sein, die einen Angriffsbeschluss fassen. Da muss zuerst die Bundesregierung sich eine Meinung bilden. Und nach der jetzigen Rechtslage muss auch der Bundestag zustimmen, weil es ja einem Angriff auf einen anderen Staat gleichkommt, wenn die Bun-

deswehr Cyberangriffe im Ausland durchführt. Doch wie du gesagt hast: da ist noch vieles in der Diskussion. Es wäre zumindest eine rechtliche Grauzone und sehr umstritten, wenn die Bundeswehr oder die Bundesregierung so etwas macht und erst nachträglich das Parlament dem zustimmt.

Weigelt:
Noch einmal nachgefragt: Was wäre denn, wenn zivile Stellen des Innenministeriums so einen Hackback durchführen? Ist das rechtlich grundsätzlich möglich, oder muss hier der Bundestag auch einbezogen werden?

Sommer:
Also, du sprichst ja das im Inland an. Auch das Innenministerium muss sich da sicherlich an Recht und Gesetz halten. Aber wie die rechtliche Lage da genau ist - da bin ich kein Experte.

Hagen:
Deutschland hat inzwischen eine Cybersicherheitsstrategie. Die Federführung in Sachen Cyberabwehr hat das Bundesinnenministerium. Das haben wir eben schon festgestellt. In diesem Kontext ist noch im vergangenen Monat von der Bundesregierung die Cybersicherheitsstrategie 2021 verabschiedet worden. Ein Kritikpunkt ist allerdings, dass sich der Staat vorbehält, entdeckte Sicherheitslücken in IT-Systemen nicht sofort an die Betreiber weiterzugeben. Lücken würden bewusst offengelassen. Stimmt das? Und wenn ja: was steckt dahinter?

Sommer:
Ja, also das stimmt: Dem Bundesamt für Sicherheit in der Informationstechnik, dem ist gestattet, durch diese Cybersicherheitsstrategie Sicherheitslücken der Polizei und den Geheimdiensten weiterzugeben, damit sie diese zur Überwachung und Infiltration von beobachteten, zum Beispiel kriminellen Netzwerken nutzen. Auch international ist es üblich, dass Geheimdienste und Polizei nicht unbedingt dafür sorgen, Sicherheitslücken sofort zu schließen, sondern diese für ihre eigenen Zwecke, für Trojaner et cetera ausnutzen. Und auch die neue

Cybersicherheitsstrategie der Bundesregierung lässt diese Möglichkeit offen, kritisiert Mischa Hansel vom IFSH:

O-Ton Hansel:

„Wir müssen uns klarmachen: Wissen über Schwachstellen, das zurückgehalten wurde, bedeutet, diese Schwachstellen können jetzt nicht nur von der deutschen Polizei ausgenutzt werden, sondern auch von fremden Nachrichtendiensten, auch von Cyberkriminellen."

Sommer:

Hansel fordert, dass zumindest in Deutschland eine Stelle geschaffen wird, die evaluiert, ob diese Ausnutzung von Schwachstellen wirklich sinnvoll war oder eben nicht. So könnte auch international, meint er, ein wenig Vertrauen geschaffen werden.

Weigelt:

Stichwort international. Welche Bemühungen und Initiativen gibt es denn auf internationaler Ebene, gegen Cyberattacken vorzugehen?

Sommer:

Ich glaube, man muss der Tatsache ins Auge sehen, Spionage oder auch die Nutzung von Internetoptionen zur Beeinflussung von Meinung - das wird sich nicht durch irgendwelche Abkommen beenden lassen. Das machen alle Staaten, die das können - ob China, Russland, die USA oder andere. Schon jetzt gilt aber, dass der Angriff auf kritische Infrastrukturen völkerrechtswidrig wäre. Das ist eine Norm. Das Problem sei die Umsetzung, sagt Annegret Bendiek von der Berliner SWP. Denn…

O-Ton Bendiek:

„Staaten können nur indirekt zur Verantwortung gezogen werden, wenn nachweisbar ist, dass sie ihrer Sorgfaltspflicht sozusagen nicht nachgekommen sind - also private Akteure und deren schädliches Verhalten von ihrem Territorium aus, nicht unterbunden haben."

Hagen:
Du sagst es gibt eine Norm, wonach der Angriff auf kritische Infrastruktur völkerrechtswidrig sei. Du meinst damit die Cybernormen der Vereinten Nationen, oder? Was sind denn die zentralen Bestimmungen?

Sommer:
Also, Regierungssachverständige haben eine Kommission gebildet - auf der Grundlage eines UN-Beschlusses - und die haben einen Bericht vorbereitet, der 2015 von der UN-Generalversammlung angenommen wurde. Da steht zum Beispiel, dass das Völkerrecht auch in Bezug auf den Cyberraum Gültigkeit hat. Und es bezieht sich natürlich vor allen Dingen auf Friedenszeiten - diese Norm. Dazu gehört zum Beispiel, dass Angriffe auf kritische Infrastrukturen wie das Gesundheitswesen oder die Energieversorgung - dass die nicht zulässig oder nicht erlaubt sind, weil sich Staaten verantwortlich verhalten müssen. Staaten dürfen auch keine privaten Hackergruppen unterstützen, wenn solche Angriffe durchgeführt werden. Allerdings: die Umsetzungsmaßnahmen für diese Norm sind ziemlich dünn. Ein internationales Klima der Zusammenarbeit, vor allen Dingen zwischen den Großmächten, wäre dafür sicher hilfreicher als ein Klima der Konfrontation.

Weigelt:
Müssten die Vereinten Nationen nicht viel mehr tun, um Cyberattacken zu verhindern oder sogar auch zu ächten? Was sagen denn da die Konfliktforscher?

Sommer:
Man plädiert für eine Art präventive Rüstungskontrolle. Die kann aber im Cyberraum nicht wie bei anderen Rüstungskontrollmaßnahmen durch Verbote oder Einschränkungen erfolgen, weil im Cyberraum einfach keine Überprüfungen möglich sind. Deshalb geht es um Vereinbarungen über mehr oder weniger unverbindlichen Normen, die aber eben vertrauensbildend sein können. Zum Beispiel die Vereinbarung, Angriffe auf kritische Infrastrukturen, sowie insbesondere auf militärische Kommando- und Kontrollsysteme, vor allem, wenn die mit Nuklearwaffen verbunden sind, mit einem Tabu zu belegen, diese zu ächten. Doch auch weitere, konkrete Maßnahmen schlägt der Computersi-

cherheitsexperte vom Hamburger Institut für Friedensforschung und Sicherheitspolitik, Mischa Hansel vor.

O-Ton Hansel:

„Staaten könnten übereinkommen, dass beispielsweise Cyberattacken gegen bestimmte, besonders sensible Systeme nur von höchster Stelle autorisiert werden dürfen. Also, unter Trump beispielsweise, hat man das ja gewissermaßen runter delegiert, dass das Cyberkommando auch gewisse Dinge in Eigenverantwortung tun konnte. Bei Obama war es noch so, dass der Präsident das immer autorisieren musste."

Hagen:

Aber das sieht ja nicht nach dem großen Wurf aus, nach einem großen Schritt in Richtung Cyberdiplomatie, oder?

Sommer:

Nein, das würde ich genauso sehen. Aber immerhin wäre es ein wenig stabilisierend, wenn die jeweils andere Seite davon ausgehen kann, dass keine niederen Stellen irgendwelche Cyberangriffe auf kritische Infrastrukturen oder militärische Einrichtungen gestartet haben, sondern dass da eben auch die politische Führung vorher gründlich darüber nachgedacht hat. Eine weitere Idee, die Mischa Hansel und andere Experten in die Debatte geworfen haben, ist eine unabhängige Stelle zu schaffen, zum Beispiel von internationalen Forschungsinstituten, die Cyberangriffe analysiert und versucht, die Verantwortlichen herauszufinden. Diese könnte eine größere Autorität haben, als Regierungen, die natürlich innenpolitische und auch parteipolitische Interessen haben, wie wir zum Beispiel in den US-Wahlen gesehen haben. Dieses unabhängige Stellte könnte erklären ob jemand, eventuell sogar eine andere Regierung, für solche Attacken verantwortlich ist. Aber du hast natürlich Recht: auch das wäre nicht der große Wurf. Mir scheint, es gibt in der Cyberdiplomatie nicht so etwas wie den großen Wurf. Wir können froh sein, wenn kleine Brötchen gebacken werden.

Hagen:

Soweit also unser Schwerpunkt zur Gefahr durch Cyberangriffe. Mehr in der Langfassung des Podcasts Streitkräfte und Strategien. Darin befassen wir uns

auch mit den Sondierungsgesprächen in Berlin und welche Rolle sicherheitspolitische Fragen darin spielten und, ob deutsche Tornados weiter mit Atomwaffen trainieren werden. Und wir fragen, ob das jahrelange Drama um die Gorch Fock jetzt endlich vorbei ist. Den Podcast gibt es auf unserer Internetseite unter ndr.de Schrägstrich Streitkräfte oder in der ARD-Audiothek. Tschüss, sagen Joachim Hagen und Julia Weigelt.