Folge 53 Aus Regierungskreisen – der Podcast der Bundesregierung

Thema: Die Diplomatin Dr. Regine Grienberger und Barbara Kluge aus dem Bundesinnenministerium über die außen- und innenpolitischen Dimensionen des Themas Cybersicherheit

[Musik]

[Nadine Kreutzer, Moderatorin] Die Digitalisierung verändert unser aller Leben. Aber je mehr automatisiert und digitalisiert wird, desto größer auch die Angriffsfläche. Cybersicherheit ist heute unser Thema und wir haben zwei tolle Frauen eingeladen, mit denen wir das besprechen möchten. Ich bin Nadine Kreutzer und freue mich, dass Sie dabei sind. Zu Gast ist zum einen Barbara Kluge aus dem Bundesinnenministerium. Dort ist sie Ständige Vertreterin des Abteilungsleiters für Cyber- und Informationssicherheit. Und ich sage: „Herzlich Willkommen, Frau Kluge!“

[Barbara Kluge, Gast] Vielen Dank für die Einladung.

[Kreutzer] Und aus dem Auswärtigen Amt begrüßen wir Regine Grienberger. Sie ist Beauftragte für Cyber-Außen- und Sicherheitspolitik und auch Deutschlands erste Cyberbotschafterin. Auch an Sie ein herzliches Willkommen!

[Regine Grienberger, Gast] Vielen Dank, dass ich hier sein darf.

[Kreutzer] Wir haben hier eine Diplomatin und eine Juristin und interessanterweise haben Sie ja vorher natürlich andere Sachen gemacht. Zum Beispiel Sie, Frau Grienberger, kommen eigentlich aus der Landwirtschaft und haben das mal studiert.

[Grienberger] Genau. Ich bin eine Diplom-Ingenieurin für Agrarwissenschaften, bin aber schon seit langer Zeit nicht mehr in diesem Beruf unterwegs.

[Kreutzer] Ja, spannend, dann auf einmal den Bogen hier zu schlagen oder die Brücke zu gehen zum Thema Cybersicherheit, wo Sie jetzt absolute Expertin sind und wir zusammen mit Ihnen gleich hinter die Kulissen blicken. Bei Ihnen, Frau Kluge, ist es so, dass Sie früher auch mal selber Diplomatin waren.

[Kluge] Ja, das stimmt. Ende der 80er Jahre habe ich im Auswärtigen Dienst angefangen und dann Jura studiert und dann nicht zurück ins AA gefunden, sondern ins BMI.

[Kreutzer] Und im BMI, da sind Sie jetzt die Ständige Vertreterin, wie man so sagt, des Abteilungsleiters für Cyber- und Informationssicherheit. Erklären Sie uns das mal. Was beinhaltet dieses Amt alles?

[Kluge] Ja, die Abteilung CI, wie sie in Kurzform heißt, hat eine relativ umfassende Zuständigkeit. Wir sind zuständig für die nationale Cybersicherheitsarchitektur. Wir machen die Gesetzgebung im Cyberbereich, aber auch die EU-Rechtsetzung in diesem Bereich und kümmern uns auch um zivile Aspekte der NATO-Zusammenarbeit bei Cyber. Die Zusammenarbeit mit der Wirtschaft und der Schutz kritischer Infrastrukturen ist wesentlicher Bestandteil unserer Arbeit, wie auch der Eigenschutz der Bundesverwaltung. Weiterhin sind wir zuständig für die Regierungsnetze, für den Digitalfunk und auch für die Cyberfähigkeiten der Sicherheitsbehörden.

[Kreutzer] Ok, wow, das sind ganz schön viele Bereiche, die das abdeckt. Frau Grienberger, sind Sie dann sozusagen die Frau Kluge für den internationalen Raum? Darf man das so sagen?

[Grienberger] Ja, genau das können Sie so sagen. Also, genauso wie Frau Kluge, beziehungsweise das Innenministerium nach innen [schaut], also nach Deutschland, so [schauen] ich und das Auswärtige Amt dann nach außen, also ins Ausland, zu unseren Partnern. Und wir kümmern uns dann, wie es so schön heißt, um die externe Dimension der Cybersicherheit.

[Kreutzer] Ich hatte schon den Begriff Cyberbotschafterin erwähnt. Erste Cyberbotschafterin Deutschlands. Was macht man als Cyberbotschafterin?

[Grienberger] Also, ich bin die erste Cyberbotschafterin, aber dieses Amt gibt es schon länger. Meine Aufgabe ist es, den Kontakt [...] zu unseren ausländischen Partnerinnen und Partnern [herzustellen]. Die informiere ich über unsere deutsche Politik. Die wollen ja wissen, was wir so machen, was wir vorhaben. Ich höre ihnen auch zu und bringe das als Impulse mit zurück in unsere deutsche Diskussion. Und ich arbeite mit internationalen Partnern zusammen, auch an gemeinsamen Fragestellungen, die wir alle irgendwie beantworten müssen. Da bin ich dann zum Beispiel als Vorsitz der deutschen Delegation bei Verhandlungen, bei denen Spielregeln für Staaten im Internet verabredet werden. Solche Verhandlungen gibt es regelmäßig, zum Beispiel in New York, bei den Vereinten Nationen.

[Kreutzer] Cyber-Außenpolitik was verbirgt sich genau hinter diesem Begriff?

[Grienberger] Als das Internet in den 90er Jahren so richtig laufen lernte und sich schnell entwickelte, war dann auch bald klar, dass wir Spielregeln vereinbaren müssen, wie sich Staaten auch im Internet verhalten. Denn der Cyberspace soll ja eben nicht der Wilde Westen sein, wo das Recht des Stärkeren gilt. Sondern wenn wir uns alle im Internet frei und sicher bewegen wollen, wenn wir uns da informieren wollen, lernen wollen, einkaufen wollen, auch Dinge verkaufen wollen, kurz — unsere Geschäfte abwickeln, uns vernetzen wollen, uns an politischen Diskussionen beteiligen wollen, dann brauchen wir solche Spielregeln. Und weil wir festgestellt haben, dass wir darüber auch mit unseren Freunden reden müssen — das war ja klar, als Edward Snowden seine Enthüllungen offenlegte —, gibt es eben seit 2013 auch einen Cyberbotschafter, sozusagen als Gesicht der Bundesregierung für unsere Partner im Ausland.

[Kreutzer] Also, Snowden war dann sozusagen der Auslöser, dass man auch hier eine aktive Cyber-Außenpolitik betreibt.

[Grienberger] Ja.

[Kreutzer] Gibt es bei Ihnen beiden so gängige Missverständnisse, was den Job betrifft? Also, [...] so große Klischees, die immer nachgefragt werden, die man mit Ihrer Arbeit in Verbindung bringt, die aber natürlich überhaupt nicht stimmen? Vielleicht ... Da schmunzeln Sie beide schon drauf los. Was werden Sie da so des Öfteren gefragt?

[Grienberger] Also, ich bin nicht zuständig für die Computer des Auswärtigen Amtes. Ich kann auch nicht programmieren. Ich bin Diplomatin und ich benutze die diplomatischen Instrumente.

[Kreutzer] Wie ist das bei Ihnen?

[Kluge] Ja, bei mir wird auch oft gefragt: „Kennst du dich so gut mit IT aus? Du hast doch Jura studiert.“ Nein, ich kann auch nicht hacken. Ich kann nicht programmieren. Das ist auch nicht meine Aufgabe. Als Juristin geht es mir darum, den Rechtsrahmen mitzugestalten und vorzubereiten. Bisschen Berührungsängste kann man damit auch nehmen, wenn man das erklärt, dass wir nicht hacken und nicht programmieren und nicht Bits und Bytes bewegen.

[Kreutzer] Wie haben Sie beide ja nicht ohne Grund gemeinsam zu diesem Thema Cybersicherheit eingeladen, denn es gibt ja ganz offenbar eine enge Zusammenarbeit beider Häuser, worauf man vielleicht nicht gleich am Anfang kommen würde. Frau Kluge, erklären Sie uns das bitte noch mal: die Arbeitsteilung vom BMI und vom Auswärtigen Amt in Bezug auf Cybersicherheit, Cyberkriminalität.

[Kluge] Also, wir im BMI machen primär natürlich die nationale Cybersicherheit einschließlich der EU-Belange. Wir sind zuständig dafür, dass der Rechtsrahmen definiert ist, dass die entsprechenden Verpflichtungen — wir kommen bestimmt auch noch zum Thema kritische Infrastrukturen — klar sind, dass die Behörden entsprechend ausgerüstet und aufgestellt sind. [Das] sind also alle nationalen Belange und weil der Cyberraum bekanntermaßen ja keine Grenzen kennt, ist [auch] sehr viel EU-Arbeit [...] damit verbunden, sowohl im regulativen Bereich, also EU-Rechtsetzung, als auch mit Blick auf Wissens- und

Erfahrungsaustausch mit den anderen EU-Staaten und auch Krisenmechanismen, Krisenreaktionsmechanismen auf EU-Ebene. Und dann haben wir auch schon eine Überlappung bei der EU. Es gibt die Cyberdiplomatie, das ist Regine Grienbergers tägliches Brot und da kann sie bestimmt mehr zu sagen.

[Grienberger] Ja, wir haben eine nationale Cybersicherheitsstrategie und da sind bestimmte Handlungsfelder definiert und ich fühle mich zuständig für dieses Handlungsfeld Internationales und Europa. Das ist ja sozusagen ein Zwitter; bisschen national und ein bisschen international. Und konkret [...] heißt es, dass wir uns da zum Beispiel für die bessere, wirksamere Strafverfolgung von Cybercrime einsetzen. Dafür muss man dann eben auch mit anderen Staaten sprechen, denn oft sitzt ja der Täter im Ausland oder es wird ausländische Infrastruktur benutzt und wir verhandeln da zum Beispiel — das ist auch noch mal ein konkretes Beispiel für, wie wir uns ergänzen — im Moment einen völkerrechtlichen Vertrag — also nicht nationale Gesetze, sondern sozusagen völkerrechtliche Gesetze — für den Austausch von Beweismitteln bei Cybercrimefällen. Damit wird [...] die Strafverfolgung erleichtert.

[Kreutzer] Vielleicht können Sie uns mal ein Beispiel geben. Was wäre denn ein solches Cybercrime?

[Grienberger] Also, der klassische Fall ist eigentlich, dass ein Unternehmen oder eine öffentliche Institution oder auch eine Privatperson in Deutschland durch einen Cyberangriff einen finanziellen Schaden erleidet. Also, der Fall, den wir jetzt häufiger sehen, ist Ransomware. Das heißt, der Angreifer dringt in ein System ein, verschlüsselt es, und droht dem Besitzer des Systems damit, die Daten entweder zu löschen oder zu verkaufen, wenn kein Lösegeld dafür bezahlt wird. In so einem Fall kommt es eben darauf an, möglichst schnell auch die Beweise zu sichern. Dann stellt man häufig fest: Für den Angriff wurde Infrastruktur im Ausland benutzt. Oder auch: Die kriminelle Organisation, die dahintersteht, ist im Ausland. Und dann muss man über den diplomatischen Weg oder über die Rechtshilfe versuchen, mit den Strafverfolgungsbehörden in diesem anderen Land zusammenzuarbeiten, um den Täter ergreifen und bestrafen zu können.

[Kreutzer] Frau Kluge, was macht denn das Innenministerium, um Deutschland vor Cyberangriffen zu schützen?

[Kluge] Das ist ein weites Feld. Für uns ist eines der primären Handlungsziele, dass wir die Resilienz stärken, die Abwehrfähigkeit, die Widerstandskraft. Ich habe gerade schon gesagt: Kritische Infrastrukturen, das sind diese Strukturen, die für unser tägliches Miteinander unerlässlich sind, wie zum Beispiel Wasserversorgung, Stromversorgung, Verkehr. Die müssen besonders geschützt werden. Da gibt es gesetzliche Vorgaben für diese Unternehmen. Und das BSI, das Bundesamt für Sicherheit in der Informationstechnik, ist da in ganz engem Austausch und unterstützt auch und berät. Aber nicht nur diese Betreiber kritischer Infrastrukturen werden beraten. Wir haben natürlich die Aufgabe, die staatlichen Strukturen zu schützen, damit unsere Verwaltung, unser Gemeinwesen funktioniert. Und wir adressieren auch den normalen Bürger, der heutzutage ja überall im Internet ist. Der Kühlschrank wurde ja schon von Ihnen erwähnt. Also, es gibt so was wie digitalen Verbraucherschutz und wir haben auch ein IT-Sicherheitskennzeichen. Das kann oder soll [...] bei der Kaufentscheidung [unterstützen]. Wenn ein Produkt dieses Kennzeichen hat, dann kann man sicher sein, dass das auch einen ordentlichen Cybersicherheitsstandard hat.

[Kreutzer] Vielleicht können wir das auch noch mal ein bisschen deutlicher machen. Wir alle haben einen Kühlschrank zu Hause stehen, vielleicht einen hoch digitalisierten. Wie kann der zu einer Cyberwaffe werden?

[Kluge] Ja, sobald ein Gerät mit dem Internet verbunden ist, können Sie es theoretisch auch übernehmen, kapern. Hier sind wieder diese Sicherheitsstandards, die ich schon genannt habe, ganz wichtig, um das zu verhindern. Wenn Sie es kapern können, dann können Sie mit Staubsauger, Kühlschränken, Geschirrspülern, und Waschmaschinen ein sogenanntes Botnetz erstellen. Dieses Botnetz sind also alles gekaperte Geräte, die Sie zusammenschließen, um dann solche DDoS- Attacken auszuführen und ganz gezielt staatliche oder nichtstaatliche Strukturen zu attackieren, dass sie in die Knie gehen.

[Kreutzer] Aber dann würde jemand anderes mein Smart Home sozusagen kapern, um einen solchen Angriff zu starten?

[Kluge] Mmh. (zustimmend)

[Kreutzer] Okay. Also, dann sind wir bei dem Internet of Things angekommen, bei diesen Produkten, die wir alle zu Hause haben und die wir durchdigitalisiert haben. Viele schrecken ja auch davor zurück und sagen: „Nein, will ich gar nicht.!“ Andere lieben es und bei denen geht sofort das Licht an, wenn man — weiß ich auch nicht — „Schnipp „Schnapp“ macht oder so ähnlich. Also, da ist dann schon Obacht geboten. Das heißt, man muss auch beim Kauf solcher Produkte [darauf] achten, dass das einen hohen Sicherheitsstandard hat?

[Kluge] Genau. Also, wir haben schon angefangen mit dem IT-Sicherheitskennzeichen. Das ist ein nationales Kennzeichen, so eine Art Gütesiegel. Und die EU hat sich des Themas jetzt auch angenommen. Es wird einen sogenannten Cyber Resilience Act geben, der genau an diesem Punkt ansetzt. Da sollen Mindestsicherheitsstandards geschaffen werden für Produkte, aber auch für Software und Services. Und das gilt im Massen- und Konsumentenbereich genauso wie im Hightech-Sektor, dass man einfach verbindliche Standards hat und sich darauf verlassen kann, dass man sich eben keine leicht zu übernehmenden Geräte ins Haus stellt und dann unwissentlich Teil eines Angriffsszenarios wird.

[Kreutzer] Was wäre kein ordentlicher Cybersicherheitsstandard? Was würde das für Folgen haben?

[Kluge] Na ja, […] vor allem Billigprodukte haben oft gar keine Absicherung. Also, Sie haben Router, die Sie gar nicht schützen können, wo sich jeder einwählen kann, wo es ganz einfach ist, die Geräte zu kapern, zu übernehmen, wo man Sie ausspähen kann. Und es gibt so einen Mindestsicherheitsstandard, einen Stand der Technik, der wird dann abgeprüft und das ist auch eine dynamische Sache. Das muss auch immer weiter entwickelt werden, upgedatet werden. Und wenn zum Beispiel Hersteller keine Updates, keine Sicherheitsupdates liefern, ist es ein großes Problem. Wir machen aber noch mehr außer dieser Stärkung der Resilienz. Wir versuchen auch, die zuständigen Behörden besser aufzustellen und zu stärken. Das gilt natürlich im präventiven Bereich. Ich habe das Bundesamt für Sicherheit in der Informationstechnik schon genannt. Es gilt aber auch im repressiven Bereich, im Sicherheitsbereich, beim BKA zum Beispiel. Die müssen in der Lage sein, Cybercrime zu verfolgen und aufzuklären. Wir haben auch das Phänomen der Cyberspionage. Dagegen muss etwas unternommen werden. Und jetzt haben wir seit dem Ukraine-Krieg auch eine sehr akute Diskussion um das Thema aktive Cyberabwehr. Das bedeutet nicht, dass man Gegenschläge oder Vergeltungsschläge auf Angriffe ausübt, sondern dass man laufende Angriffe abwehrt. Da haben wir derzeit eine sehr lebhafte politische Diskussion.

[Kreutzer] Das klingt nach wirklich vielen Aufgaben. Das müssen viele Leute sein, die in Ihrer Abteilung arbeiten, oder?

[Kluge] Ja, wir sind nicht so viele, wie wir eigentlich bräuchten.

[Kreutzer] Aha. Das ist auch so eine Frage, die ich gern noch mal stellen möchte: Wie sieht es aus mit Expertinnen und Experten, die firm sind in diesen Sachen und da gut geschult sind? Ist man da ständig auf der Suche oder werden Ihnen die Türen eingerannt?

[Grienberger] Nein, ich bin ständig auf der Suche nach guten Kolleginnen und Kollegen, die sich für dieses Thema interessieren und auch eine Leidenschaft dafür entwickeln. Denn es ist ja etwas, [das] wir nicht kurzfristig lösen können, sondern da sind dicke Bretter zu bohren. Und da muss man auch eine gewisse Frustrationstoleranz haben und eben eine große Motivation, intrinsische Motivation, um da mitarbeiten zu können.

[Kreutzer] Was braucht man für Voraussetzungen?

[Grienberger] Also, ich suche Diplomatinnen und Diplomaten, die Erfahrungen haben im multilateralen Geschäft, das heißt Verhandlungen führen können, insbesondere auf der ganz oberen Ebene, also in den

Vereinten Nationen, wo wir ja 193 Staaten sind. Also, da braucht man auch einen gewissen Überblick. Und dann suche ich auch Leute, die gerne mit diesen ein bisschen technisch daherkommenden Themen zu tun haben, die aber in Wirklichkeit sehr politische Fragen berühren.

[Kreutzer] Ja, dann haben wir doch gleich hier schon mal einen Jobaufruf gemacht. Und wenn Sie sich berufen fühlen und sagen: „Das ist genau mein Ding“, dann melden Sie sich gerne bei Frau Grienberger. Frau Kluge hat uns jetzt schon beschrieben, was das Bundesinnenministerium macht, um Deutschland vor Cyberangriffen zu schützen. Vielleicht auch noch mal ganz kurz aus Ihrer Warte vom Auswärtigen Amt.

[Grienberger] Ich spreche mit den Guten und auch mit den Bösen. Die Guten, das sind unsere Partner, mit denen wir zusammen — also mit denen wir unsere Ideen teilen, mit denen wir gemeinsam bestimmte Maßnahmen vereinbaren können, die uns allen helfen, zum Beispiel Informationen teilen oder eben auch die Strafverfolgung von Cyberkriminellen zu erleichtern. Und mit den Bösen spreche ich auch; insbesondere darüber, warum wir [...] ihr Verhalten [nicht] akzeptieren können, warum wir das nicht einfach hinnehmen können, dass sie uns angreifen und auch, wie wir darauf reagieren werden, also zum Beispiel mit Sanktionen.

[Kreutzer] Was sagen die denn dann? Wie gesprächsbereit sind die denn?

[Grienberger] Auf diese Gespräche müssen sie sich einlassen, das müssen sie sich einfach anhören, und dann versuchen wir, im Weiteren Lösungen [...] für die Probleme, die wir hier aufgezeigt haben, [zu finden].

[Kreutzer] Das Auswärtige Amt macht ja auch gerade im Auftrag der ganzen Bundesregierung eine Nationale Sicherheitsstrategie. Das ist auch die erste in ihrer Art in Deutschland. Vielleicht können Sie uns dazu mal was sagen, denn es gibt zum ersten Mal auch einen erweiterten Sicherheitsbegriff, wie es heißt. Und demnach steht wohl der Mensch im Mittelpunkt.

[Grienberger] Genau. Also, dieser Sicherheitsbegriff, der erweiterte oder umfassende Sicherheitsbegriff, der umfasst eben nicht nur Militär und Diplomatie, wie das bei den klassischen Sicherheitsstrategien ist, sondern beschäftigt sich eben auch mit Themen wie Gesundheit, Klima, Migration und eben auch Cybersicherheit. Und dabei stellen wir die menschliche Sicherheit in den Mittelpunkt, nicht die territoriale, sondern die menschliche Sicherheit. Und das macht bei allen Themen rund um Digitalisierung und Cyber aus meiner Sicht auch absolut Sinn, weil das Internet ja keine Grenzen hat, die man verteidigen kann.

[Kreutzer] Aber was heißt das genau „den Menschen in den Mittelpunkt stellen“? Was bedeutet das für uns Bürgerinnen und Bürger?

[Grienberger] Das bedeutet, dass wir, jeder Einzelne, jeder und jede Einzelne von uns, [uns sicher] im Internet [...] bewegen können; also frei sind von Gewalt, dass wir unsere Meinung äußern dürfen, dass wir uns digital versammeln dürfen. Also, dass Menschenrechte und Bürgerrechte online genauso wie offline gelten.

[Kreutzer] Frau Kluge, inwieweit ist das BMI beteiligt an der Nationalen Sicherheitsstrategie?

[Kluge] Ja, das Auswärtige Amt hat die Aufgabe, den Entwurf zu erstellen. Das machen die natürlich auch nicht alleine. Jedes betroffene Ressort liefert zu, bringt sich ein und gestaltet die Bereiche, für die, [es] jeweils zuständig [ist]. Das ist bei uns genau das Gleiche. Die Nationale Sicherheitsstrategie ist ja auch eine Art Dachstrategie. Wir haben ja auch eine Nationale Cybersicherheitsstrategie und das muss ja zusammenpassen. Da schauen wir also schon, dass da auch eine Kohärenz hergestellt wird. Und die Nationale Cybersicherheitsstrategie aus dem letzten Jahr, aus 2021, werden wir auch weiterentwickeln und das muss alles zusammenpassen. Also, wir bringen uns da ganz aktiv ein. Und eine nationale Strategie zu entwickeln, bedeutet ja auch, dass das eine gemeinsame Strategie der ganzen Bundesregierung ist. Es wird also alles auch [miteinander] abgestimmt [...]. Das ist eine gemeinsame Position.

[Kreutzer] Kommen wir noch mal zum Begriff der Datenbotschaft im Ausland. Die Bundesregierung möchte ja eine solche einrichten. Was ist denn das genau, eine Datenbotschaft?

[Grienberger] Eine Datenbotschaft ist ein digitaler Ausweichsitz der Bundesregierung für den Katastrophenfall. Mit der Digitalisierung der Bundesverwaltung fallen ganz viele geschäftskritische Daten an, die wir irgendwo sicher speichern müssen. Wir machen das natürlich in Deutschland an mehreren Orten, aber am besten eben auch irgendwo im Ausland, sodass wir immer unter allen Umständen auf ein Backup zurückgreifen können. Das ist auch eine Lehre aus dem Ukraine-Krieg; damit wir als Bundesregierung unter allen Umständen handlungsfähig sind. Die ukrainische Regierung hat nämlich in den ersten Kriegstagen erlebt, dass ihre Server massiv von Viper-Angriffen betroffen waren, das heißt, dass Daten gelöscht worden sind und unwiederbringlich verloren waren. Und da haben wir uns gefragt: Wie sicher sind wir eigentlich mit unseren Daten? Und das Ding heißt Botschaft, weil es nach den Bestimmungen des Wiener Übereinkommens über diplomatische Beziehungen errichtet wird. Es wird also in einem anderen Land stehen, aber dieses andere Land wird keinen Zugriff auf unsere Daten haben.

[Kreutzer] Und das ist natürlich top secret. Auch wo es im Inland eine sogenannte Redundanz gibt, eine Sicherheitskopie. Frau Kluge?

[Kluge] Werde ich keinen Ton zu sagen.

[Gelächter]

[Kreutzer] Verständlicherweise. Eine Herausforderung von Cybersicherheit ist bestimmt auch die Frage der Einmischung von Hackern. Also, [man hört auch gern die Begriffe] IT-Army [...] oder Cybersöldner. Vielleicht können Sie uns das noch mal genau erklären und wo auch hier die Gefahr liegt.

[Grienberger] Ja, das ist ein Phänomen, das wir jetzt im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine ganz massiv sehen. Und zwar in zweierlei Hinsicht. Einmal ist es so, dass Cyber einfach ein Bestandteil dieses Krieges ist. Also, es war ein Bestandteil des Angriffs auf die Ukraine, von Anfang an, seit der ersten Stunde. Und die Ukraine, die darauf vorbereitet ist, weil sie ja schon seit 2014 sozusagen ständig im Feuer steht, [...] hat dann sehr schnell eine IT-Army aufgestellt, also ihre vielen Computer- und Cyberexperten zusammengetrommelt, um eben die ukrainischen Regierungsstellen, aber eben auch die Zivilgesellschaft zu schützen. Und bei den IT-Söldnern [...] gibt es zwei Beobachtungen. Da gibt es zum einen erst mal diese Einmischung von außen, also Hackerkollektive, die sich auf der einen oder anderen Seite in diesen Konflikt einmischen. Auf der einen Seite ukrainische beziehungsweise russische Ziele direkt attackieren, also zum Beispiel Webseiten lahmlegen oder Daten stehlen. Auf der anderen Seite aber auch die Partner, also zum Beispiel uns in Deutschland, mit solchen DDoS-Angriffen zum Beispiel überziehen.

[Kreutzer] DDoS?

[Grienberger] DDoS heißt, dass Server mit so vielen Anfragen konfrontiert werden von außen, dass sie in die Knie gehen, weil sie diese Menge an Anfragen nicht mehr bearbeiten können. Eins ist wichtig zu verstehen: Dieses Einbrechen in fremde Netze ist verboten. Es ist auch völkerrechtlich nicht erlaubt, aber es ist ein neues Phänomen. Und wie wir in der Praxis damit dann umgehen, darauf haben wir im Moment einfach noch keine Antwort. Ich möchte nur davor warnen, diesen Hacktivismus zu verharmlosen.

[Kreutzer] Hacktivismus, alles klar. Das nehmen wir auch noch mal als Begrifflichkeit mit aus dieser Folge. Wen von Ihnen beiden fragen wir denn jetzt am besten nach der Einschätzung der aktuellen Lage in Sachen Cybersicherheit? Hat da jede für Ihren Bereich eine andere Antwort? Frau Kluge, was würden Sie sagen? Wie sieht es da aus?

[Kluge] Ich glaube, Sie kriegen eine ziemlich deckungsgleiche Antwort von uns beiden. Wir sagen schon lange, dass die Sicherheitslage im Cyberraum angespannt ist. Das ist so und das wird [sich] sicherlich [...] in Kürze auch nicht ändern. Wir beobachten mehr und mehr Cybercrime, aber auch staatlich gelenkte Cyberangriffe, Cyberspionage. Das ist insgesamt schon eine angespannte Situation.

[Grienberger] [...] Ich teile das. Die Situation ist angespannt. Wir sehen, dass sich die großen geopolitischen Konflikte rund um Russland und China eben auch im Cyberspace niederschlagen und dass [...] unsere Sicherheitsinteressen [also unmittelbar] gefährdet sind, also wie wir sozusagen den Cyberspace auch für unser tägliches Leben und unsere Wirtschaft nutzen können. Aber darüber hinaus ist auch die Entwicklung des Internet an sich gefährdet, denn im Moment haben wir noch ein globales Internet. Worauf es aber hinauslaufen könnte, wenn Staaten anfangen, sich aufgrund solcher Sicherheitsprobleme dann abzuschotten, ist, dass wir bei einem fragmentierten Internet landen. Und das ist genau das Gegenteil derjenigen, die das Internet einst erfunden haben.

[Kreutzer] Es ist ja oft schon der Begriff der Cybersicherheitsarchitektur gefallen. Wo kommen wir als Bürgerinnen und Bürger in dieser Architektur genau vor?

[Kluge] Die Bürger nehmen schon einen sehr wesentlichen Teil ein. Ich habe vorhin schon gesagt: Jeder ist auch Adressat. Wir betreiben digitalen Verbraucherschutz. Sie haben das Stichwort Kühlschrank als Waffe genannt. Wenn jeder Einzelne mit Augenmaß sich im Cyberraum bewegt und auch Vorsicht walten lässt, kann man bestimmte Angriffsmuster erschweren oder auch verhindern. Also: Regine sagte gerade DDoS-Angriffe, das ist weitverbreitet und hier kommt der Kühlschrank ins Spiel.

[Kreutzer] Da können wir gleich noch mal zu den Unternehmen an dieser Stelle kommen. Die sind ja immer wieder Opfer von Cyberattacken. Da geht es ja teilweise dann um Erpressung, hatten Sie erwähnt, Ransomware-Attacken, teilweise um Diebstahl geistigen Eigentums. Wie ist da die Privatwirtschaft beim Thema IT-Sicherheit aufgestellt und kann der Staat da auch gut helfen?

[Kluge] Der Staat kann nicht nur helfen, der muss helfen und er tut es auch bereits. Also, bei den Betreibern kritischer Infrastrukturen und besonders wichtiger Unternehmen gibt es gesetzliche Vorgaben. Da ist das BSI im engen Austausch und im engen Kontakt mit diesen Betreibern. Aber das BSI adressiert natürlich auch kleine und mittlere Unternehmen, stellt Beratungsangebote zur Verfügung und auch der ganz normale Bürger kriegt vom BSI Hilfestellung. Da gibt es eine Homepage. Mache ich jetzt ein bisschen Werbung: www.bsi-fuer-buerger.de. Da kann jeder auch nachlesen, was wichtig ist, um sich selber zu schützen und was es zu beachten gilt.

[Kreutzer] Frau Grienberger, das Auswärtige Amt möchte mit seiner Cyber-Außenpolitik unter anderem dabei helfen, Menschenrechte auch im digitalen Raum durchzusetzen. Wie genau soll das vonstattengehen? Ich stelle es mir schwierig vor, anderen Ländern vorzuschreiben, zum Beispiel, welche Websites ab sofort jetzt nicht mehr frei zugänglich sein sollten. Können Sie uns da mal mitnehmen?

[Grienberger] Ich glaube, dass wir da anfangen müssen, dass mit der digitalen Transformation, die ja die meisten Staaten im Moment durchlaufen, sie auch [...] Interesse an gemeinsamen Spielregeln entwickeln. Und wir haben in den Vereinten Nationen gesehen, dass im Unterschied zu [...] vor zehn Jahren, wo es im Grunde genommen nur wenige Staaten gab, die mitdiskutieren wollten, jetzt alle an Bord sind. Das gilt auch für die Menschenrechte. In unseren Gesprächen hat sich herausgestellt, dass die Menschenrechtscharta der Vereinten Nationen bei den meisten Staaten die Grundlage ist. Also ist das ein breiter Konsens dafür, dass Menschenrechte online genauso wie offline gelten. Dann haben wir aber eine Reihe von autoritären Staaten, Russland und China zum Beispiel, für die das ein Streitthema ist. Also, die stellen das in Frage. Und sie stellen auch in Frage, wer eigentlich das Internet kontrolliert. Wir gehen davon aus, dass auch die Unternehmen Verantwortung haben. Schließlich besitzen sie den größten Teil der IT-Infrastruktur, aber eben auch die Zivilgesellschaft. Und wir fordern diese Aufgabenteilung, den sogenannten Multi-Stakeholder-Ansatz, überall ein; auch da, wo China und Russland die anderen Stakeholder rausdrängen wollen.

[Kreutzer] Wir haben jetzt sehr abstrakt gesprochen und aber auch viel erfahren aus dem Maschinenraum. Vielleicht können wir noch mal ein bisschen konkreter werden und auch ein paar Beispiele erfahren. Vielleicht auch, wie sich jeder Einzelne, jede Einzelne schützen kann. Oder vielleicht sagen Sie [zu manchem] aus Ihrer Erfahrung, natürlich auch aus Ihrem Dunstkreis heraus: „Das wäre zum Beispiel total naiv. Das darf man auf keinen Fall machen! Das hören wir immer wieder.“ Also, vielleicht mal so ein

bisschen aus dem Cyber-Nähkästchen plaudern. Was sind Dinge, [wovor Sie] warnen, wo man vielleicht hellhörig sein sollte, wo man aufpassen sollte, ob es jetzt [ein] Passwort [ist oder] Gerätschaften [...], die man sich für zu Hause anschafft.

[Grienberger] Ich benutze zum Beispiel sichere Passwörter. Kennen Sie das? Das ist, wenn man sich einen Satz ausdenkt, den man sich leicht merken kann. Und dann nimmt man aus diesem Satz die Anfangsbuchstaben und Zahlen und macht daraus ein Passwort. Also, zum Beispiel sagt man: Meine Tante Erna hat zwei rosarote Fahrräder. Und daraus wird dann: großes M, großes T, großes E, kleines H, 2, zwei R, großes F und ein Ausrufezeichen und schon hat man ein Passwort, [das] kaum jemand erraten kann, [das Sie sich] aber ganz sicher [...] merken können. Also, jetzt benutzen Sie es bitte nicht mehr. Aber im Prinzip funktioniert es so. Und dann: Für alle meine Accounts, also zum Beispiel für meinen Twitter-Account oder auch meine private Mailbox, habe ich eine sogenannte Zwei-Faktor-Authentisierung. Das heißt, dass ich nicht nur mein Passwort eingebe, sondern [...] auch noch über SMS oder biometrischen Fingerabdruck oder so [...] noch mal bestätige, dass wirklich ich mit diesem Gerät diesen Account öffnen möchte. Und mein dritter Tipp wäre: Auch einfach mal offline sein und Dinge offline machen.

[Kluge] Sehr gute Tipps. Ich würde zwei Sachen vielleicht noch ergänzen. Genau hingucken, das ist ganz wichtig. Wenn man E-Mails bekommt — das ist, glaube ich, fast schon kalter Kaffee —, aber nicht irgendwelche Links anklicken, die man nicht kennt, nicht auf irgendwelche Datenanhänge klicken. Phishing ist nach wie vor ein Riesenthema. Und tatsächlich auch Beratungsangebote nutzen. Also, fragen bei Leuten, die sich auskennen oder auf die genannte BSI-Homepage gehen. Mal gucken: Was schreiben die eigentlich? Können die mir Tipps geben, wenn ich einen neuen Router kaufen will? Was soll ich eigentlich tun, um meine private IT anständig abzusichern?

[Kreutzer] Vielen Dank noch mal für diese Tipps hier zum Schluss. Das war's nämlich schon mit „Aus Regierungskreisen“, dem Podcast der Bundesregierung. Frau Kluge und Frau Grienberger, ganz herzlichen Dank für Ihre Zeit.

[Grienberger] Danke Ihnen!

[Kluge] Vielen Dank!

[Kreutzer] Das war unsere Folge zum Thema Cybersicherheit und wir freuen uns, wenn Sie auch beim nächsten Mal wieder dabei sind, beim Blick hinter die Kulissen des Politikapparates. Ich bin Nadine Kreutzer. Bis ganz bald!

Das war „Aus Regierungskreisen“, der Podcast der Bundesregierung. Mehr Informationen zur Politik der Bundesregierung finden Sie auf bundesregierung.de und auf unseren Social-Media-Kanälen.