**** Dies ist ein KI-generiertes Transkript und kann daher Fehler aufweisen****

von der ADB-Podcast. Ich bin Anke Domscheit-Berg, digitalpolitische Sprecherin der Linken im Bundestag und berichte euch mal wieder aus dem Maschinenraum des Bundestages und wie immer über den Digitalausschuss. Heute geht es einmal darum, wir haben Girls' Day. Ich hatte acht Mädels zu Besuch. Das wird also ein Thema sein. Aber wir hatten auch Boris Pistorius im Ausschuss. Der ist Verteidigungsminister und erzählt über Digitales im Militär, über hybride Bedrohungen von Desinformation bis Cyberkrieg. Dann ging es beim zweiten Thema im Digitalausschuss um Hackerangriffe auf Microsoft. Da waren nicht nur VertreterInnen von Microsoft geladen, auch aus den USA, sondern auch vom Innenministerium und vom Bundesamt für Sicherheit in der Informationstechnik. Da ging es also darum, was ist da eigentlich passiert, was waren das für Hackerangriffe und was hat das für Folgen für Deutschland. Angriffe und was hat das für Folgen für Deutschland? Als letztes das mache ich aber nur kurz, Thema, weil das haben wir echt schon wirklich oft gehabt und es langweilt ein wenig, ist die Umsetzung der KI-Verordnung der Europäischen Union. Die Frage, was macht die Bundesregierung da eigentlich wann in den nächsten Monaten und ein, zwei Jahren? Und damit kommen wir zum Girls Day. Ich bin heute nämlich gar nicht allein, nicht mal hier bei der Aufnahme. Neben meiner Mitarbeiterin Melissa sind auch die acht Mädels hier bei der Aufnahme zu Gast. Heute ist der Mädchen-Zukunftstag und die Mädels sind 15 bis 16 Jahre alt, achte bis zehnte Klasse, kommen aus drei Bundesländern, aus Brandenburg, Mecklenburg-Vorpommern und aus Berlin. Ich finde es wichtig, ein Girls' Day auch im Bundestag zu machen, denn da gibt es ja nur gut ein Drittel Frauen. Politik wird also im Bundestag hauptsächlich von Männern gemacht und das ist natürlich ein Problem, denn zum Beispiel gibt es ja ganz viele Themen, die überhaupt nur Frauen betreffen. Aktuell haben wir die Debatte um die Abschaffung des Paragraf 218 und ich persönlich bin fest überzeugt davon, hätten wir 50 Prozent Frauen im Parlament, das nennt man Parität, dann wären Schwangerschaftsabbrüche längst legalisiert und vermutlich würde es auch zum Beispiel mehr Unterstützung für Alleinerziehende geben. Aber Erfahrungen und Kompetenzen von Frauen sind auch für andere Themen interessant, auch im Bereich der Digitalisierung. Zum Beispiel betrifft digitale Gewalt Frauen ganz anders als Männer, Stichwort Revenge-Porn. Die

Mädels waren ein paar Stunden hier und jetzt sagen sie vielleicht ein paar Worte über sich selber.

die Reem und ich komme aus Hülsenberg und gehe in die 10. Klasse und ich bin heute hier, weil mich Politik interessiert. Hallo, ich bin Alinda, ich bin 15 Jahre alt, ich wohne in Köpenick und ich wurde hier heute von einer Freundin eingeladen, mit hier den Girls Day zu besuchen. Und ich fand den Tag sehr spannend. Mir hat am meisten gefallen die Aussicht, die man zu Berlin hat. Und vor allem, dass die Mitarbeiter, die uns durch den Tag geführt haben, sehr freundlich waren, uns alles erklärt haben. Und ja, also ich würde, wenn ich dann noch eine Chance hätte, hierher zu würde kommen, ich auf jeden Fall hierher Und kommen. also ich ja, wenn würde, ich dann noch eine Chance hierher hätte, zu würde kommen, ich auf jeden Fall hierher kommen.

ich bin Selma, ich bin 15 Jahre alt und wohne in Köpenick. Und ich habe heute den Götze hier im Bundestag verbracht und fand es auch super spannend und überwältigend, auch die ganze Aussicht und was alles hier passiert und bin sehr glücklich, hier gewesen zu sein.

bin Rana, ich bin 16 Jahre alt und wohne in Fürstenberg. Ich habe mich sehr gefreut, dass ich hierher eingeladen wurde. Ich fand den Tag sehr toll. Ich wollte schon immer sehen, wie der Bundestag aussieht. Ja, und ich würde sehr gerne nochmal herkommen. Hi, ich bin Nina, ich

bin 16 Jahre alt und komme aus Waren an der Müritz. Ich fand es sehr interessant, dass wir einen kleinen Einblick in die Arbeitswelt des Bundestags bekommen haben. Hallo, ich bin Antonia, ich bin 15 Jahre alt und komme aus Berlin. Und mich hat es schon immer interessiert, wie es so hinter den Kulissen in der Politik aussieht. Und ich bin sehr froh, hier gewesen zu sein. Das waren meine

Mädels. Die Mädels gehen jetzt gleich wieder in mein Büro, um sich mit meinen wissenschaftlichen Mitarbeitern zu parlamentarischen Abläufen auszutauschen. Ich erzähle euch inzwischen weiter über Digitales im Bundestag. Und damit kommen wir zu unserem ersten fachlichen Thema aus dem Digitalausschuss, nämlich Verteidigungsminister Pistorius war zu Gast und ein paar Generäle hat er auch mitgebracht, aus Verantwortungsbereichen,

die irgendwie mit digital zu tun haben. Wir hatten das Verteidigungsministerium ja schon am 25. Januar im letzten Jahr mal da, ohne Minister allerdings. In der Podcast-Folge 8 habe ich darüber erzählt. Ich verlinke euch das natürlich in den Shownotes. Allgemein sind wir als Linke ja bekanntlich aufrüstungskritisch. Allgemein sind wir als Linke ja bekanntlich also so 100 Milliarden aufrüstungskritisch, plus immer mehr X und Kriegstüchtigkeit und solche Dinge Zeitenwende, als zentrale und hauptsächliche das sehen wir natürlich kritisch. Antwort, Aber davon ganz unbenommen ist es natürlich auch für uns total spannend zu was treibt erfahren, man denn so Digitales im Verteidigungsministerium und das ist nämlich ziemlich viel. Vielleicht es gibt im Verteidigungsbereich ja auch diverse vorneweg, die mit den digitalen Fragen zu tun Also Strukturen, zum einen gibt es das das Cyber- und haben. Das wurde jetzt CIR, gerade frisch Informationsraumkommando. im April als eigenständige Teilstreitkraft ist also parallel und gleichberechtigt aufgewertet, also Luftwaffe und Marine. nebenher, Landstreitkräfte, Zu den Aufgaben dieses Cyber- und Informationsraumkommandos gehört die elektronische Kampfführung und Cyberoperation, Analyse hybrider Bedrohungen aller möglichen auch Desinformationskampagnen Arten, gehören dazu. Natürlich auch der Schutz der IT-Infrastruktur und der die IT-Systeme, da auch im Einsatz im Feld irgendwo sind. Ganz wichtig ist aber vor allem dieser Bereich Aufklärung. Das ist also Bedrohung Feindbeobachtung, erkennen und so Kram und die sogenannte Wirkung. Jetzt müsst ihr daran Wirkung im allgemeinen denken, Sprachgebrauch ist nicht das gleiche wie Wirkung im militärischen Sinn. Wirkung im militärischen Sinn heißt was Schaden alles, beim Feind anrichtet. Also ein Schuss aus dem Gewehr, das ist dann die Wirkung oder die Granate auf dem Gefechtsstand. Für beides übrigens werden zunehmend Drohnen eingesetzt, also für Aufklärung und für Wirkung, also diese Wirkung. Zum Beispiel eine Kamikaze-Drohne, die mit so einer Minibombe da so ein Panzer anfliegt, um mit ihm zu kollidieren und zu explodieren, das ist dann die Wirkung. Neben diesem Cyber- und Informationsraum haben wir noch das BWI oder die BWI GmbH. Das ist der IT-Dienstleister des Verteidigungsbereichs, gehört zu 100 Prozent dem Bund, gilt also, wenn man da Vergaben macht, als quasi Inhouse. Die entwickeln IT-Kram, die betreiben IT-Kram. Die haben zum Beispiel auch einen KI-Chatbot entwickelt. Der soll in Datenbeständen Dinge suchen und nennt sich Scout passenderweise. Der wurde übrigens vortrainiert auf der Basis von Aleph Alpha. Das ist also dieses eine große KI-Unternehmen made in Germany. Und dann gibt es noch den Cyber Innovation Hub. Das ist eine Plattform zur Erforschung und Weiterentwicklung innovativer Technologien, hat ganz

viel mit Startups zu tun und ist so ein bisschen so ein Experimentierfeld, wo so ganz frühe Entwicklungen gemacht werden können. Und wenn die erfolgreich sind, dann gibt es eventuell einen Pilot im realen militärischen Leben sozusagen. Und als letztes in diesem Bereich gibt es die Cyberagentur in von Halle, der habe ich euch auch schon mal in einem Podcast Das erzählt. ist auch eine separate die einen GmbH, Haufen Kohle gemeinsam kriegt, vom aber BMVG, auch vom BMI getragen Und die wird. vergibt also sehr großvolumige Forschungsaufträge mit einem sehr langfristigen aber Fokus, ausschließlich zum Schwerpunkt Cybersicherheit. Bevor es jetzt losgeht direkt mit dem Digitalausschuss, will ich euch noch auf ein paar Links in den Shownotes hinweisen, falls ihr zu diesem Thema euch richtig tiefgehend informieren wollt. Dann gibt es nämlich ganz nagelneu und druckfrisch den sechsten Digitalbericht des Verteidigungsministeriums und es gibt auch superfrisch den Jahresbericht der Werbeauftragten. Da steht zum Beispiel drin, dass WLAN in Unterkünften noch fehlt, aber dazu komme ich auch Für dieses nochmal. Thema wichtig ist auch zum Beispiel die Cy dass WLAN in Unterkünften noch aber dazu komme fehlt, ich auch nochmal. Für dieses Thema wichtig ist auch zum Beispiel die Cybersicherheitsstrategie der Bundesregierung. Die ist schon von 2021 und hat säuberlich also so wer für was zuständig ist. aufgeteilt, halbsäuberlich, Nämlich einerseits das Verteidigungsministerium für den Bereich Cyberverteidigung, das Auswärtige Amt für die Cyberaußenpolitik und für die Cybersicherheitsinnenpolitik, das Innenministerium. Das klingt also nach einer klaren Aufteilung, aber wir werden noch sehen, so einfach ist es dann gar nicht, weil das überlappt sich alles immer so ein bisschen. Und dann gibt es natürlich die berühmte Digitalstrategie. Und da stehen dann auch so Projekte drin, für die das Verteidigungsministerium zuständig ist. Also so Sachen wie Förderung eines digitalen Mindsets aller Beschäftigten. Na ja, da haben die, glaube ich, noch zu tun. Ja, dann gehen wir mal direkt in den Ausschuss. Wie immer hat der Minister selber eine ganze Weile was erzählt. Der berichtete also, wie hart sich die Bedrohungslage verschärft hat, insbesondere auch durch den Krieg von Russland gegen die Ukraine und dass man da so ganz viele Weichen jetzt nochmal neu und anders stellen musste und dass genau deshalb auch aus dem Cyber- und Informationsraumkommando eine eigene gleichberechtigte Streitkraft geworden ist, weil eben Kriege längst in sämtlichen Dimensionen stattfinden, also als, wie schon erwähnt, hybride Auseinandersetzungen und er sprach dann von elektronischer Kampfführung, von den Drohnen nochmal, von Cyberangriffen auf Staaten oder von Staaten, von Cyberangriffen auf Kritis, also kritische Infrastrukturen und er hat auch beschrieben, wie unscharf diese

Trennlinien sind und das Thema hat uns eigentlich in der ganzen Debatte begleitet. Also du kannst nicht genau was ist denn ein eindeutig staatlich sagen, gelenkter was sind private

eine besonders enge Kooperation geben bei der inneren und der äußeren Sicherheit im Cyberraum, weil man eben nicht so genau weiß, was ist jetzt eigentlich die innere und die äußere und wo ist die Trennlinie? Eine Herausforderung ist natürlich in diesem Feld, wie stärkt man die Resilienz? Also wenn die Angreifer immer mehr und immer komplexer werden, wie macht man sich selbst sicherer? Wie kann man dieser komplexer werdenden Bedrohung sinnvoll begegnen? Und dann fielen in seiner Intro vom Minister auch so ein Satz wie, den Gegner muss man im Ernstfall bekämpfen bevor können, er gegen uns wirken kann. Das heißt bevor der was gemacht machen wir was gegen den Gegner. also, hat, Das klingt irgendwie fatal nach vorbeugender Hackback. Haben wir später debattiert, wurde nicht ganz aufgeklärt, aber wir kommen noch dazu. Er sprach natürlich auch von diesem 100 Milliarden Sondervermögen. Da geht nämlich einiges auch in den Bereich Digitalisierung. Aber er hat auch gesagt, man würde noch viel, viel mehr als diese 100 Milliarden brauchen. Gerade auch für den Bereich Digitalisierung. Also noch hätte man zum Beispiel alte Funkgeräte zum Teil im Einsatz. Bald sollen das alles Software-Defined Radios sein. Das wird aus dem Sondervermögen aber schon finanziert. Und er hat dann nochmal bemeckert, dass es einen eklatanten Mangel an Funkfrequenzen gibt. Und wenn ihr treue Hörer und Hörerinnen dieses Podcasts seid, dann erinnert ihr euch vielleicht, wir hatten ja ein paar Mal das Thema Weltfunkkonferenz, wo es um die Neuordnung der Kultur- und TV-Frequenzen ging. Und Pistorius, der hat sich da ganz offen dass gefreut, die Weltfunkkonferenz beschlossen dass die hat, KulturFrequenzen Und gingen. der Pistorius, hat sich da ganz offen gefreut, dass die Weltfunkkonferenz beschlossen hat, dass die Kulturfrequenzen für eine sogenannte sekundäre Nutzung durch den Mobilfunk geöffnet werden sollen. Und will jetzt unbedingt in Deutschland die militärische Nutzung dieser Kulturfrequenzen erreichen. Also da bin ich ja gespannt, wie sich die Kultur und Medien dagegen wehren können. Denn es heißt ja sekundäre Nutzung. Sie dürfen also eigentlich Kultur und Medien nicht beeinträchtigen. Und da die Kultur und Medien sagen, sie haben eh schon zu wenig, weiß ich gar nicht, wie sich der Wunsch von Pistorius erfüllen soll. Das war also durchaus interessant, dass er da so große Hoffnungen hat. Das Sondervermögen reicht ihm nicht. Er hat offen erklärt, der Militäretat, der muss jetzt jedes Jahr steigen. Ich finde ja persönlich, die Bundeswehr hat seit Jahren

gezeigt, dass sie auch mit sehr viel Geld sehr wenig gebacken kriegen. Also das Geld landet hauptsächlich bei Rüstungsunternehmen, die sich da goldene Nasen verdienen und viel Impact hat es gar nicht. Aber damit kommen wir jetzt schon mal zur Debatte. Und da ging es unter anderem um das Thema Sicherheitslücken. Da stellte sich die Frage, wenn der Cyber- und Informationsraum, also dieses Kommando auch Wirkung in diesem militärischen Sinn, im Cyberthema entfalten soll und jetzt auch formell eine Streitkraft ist, gibt es dann nicht einen natürlichen Konflikt zur Schließung von Sicherheitslücken? Der Konflikt kommt natürlich daher, dass du Wirken im Cyberbereich eigentlich nur kannst, wenn du eine Sicherheitslücke ausnutzt, um irgendwo anzugreifen. Das ist der Hintergrund. sämtliche gefundenen Schwachstellen immer dem BSI anzeigen. Es hat auch eine eigene Responsible Disclosure Policy zum Umgang mit Schwachstellen. Und man hat zwar kein Bounty-Programm, weil das findet man irgendwie blöd, dafür Geld zu bezahlen, aber man hat so ein Programm, wo man honoriert, wenn Menschen Sicherheitslücken finden und die melden. Also da wirbt man darum und man anerkennt die öffentlich. Die kriegen also so eine Urkunde und werden virtuell angepriesen und das soll wohl auch ganz gut laufen. Es gab dann aber auch noch mal die kluge Frage, finde ich, ob Sicherheitslücken in mandatierten Einsätzen, also die, wo es ein parlamentarisches Mandat für Einsätze im Ausland gibt, ob man da Sicherheitslücken ausnutzt, um zu wirken mit Cyber-Cyber. Da hatte der Minister keine Ahnung, hat aber auch gesagt, er würde, auch wenn er es wüsste, in öffentlicher Sitzung, und es war eine öffentliche Sitzung, dazu auch nichts sagen. Das hat mir natürlich die Gelegenheit gegeben, mal nachzufragen, dass er das also bitte gerne schriftlich nachreichen möge. Und wenn das nicht öffentlich geht, dann muss er es halt einstufen. Was heißt, ich kann darüber natürlich nicht reden, aber wenigstens weiß ich es dann, und das ist ja auch schon mal was. Dann haben wir eine ganze Weile über das Thema Graubereiche besprochen. Ich habe ja erzählt, das ist nicht so einfach. Wer ist dafür was zuständig? Und da ging es auch so allgemein um neue Regulierungsbedarfe, zum Beispiel für die Aufklärungstätigkeiten der Bundeswehr. Der MAD, der Militärische Abschirmdienst, ist ja einer der Geheimdienste in Deutschland, hat ziemlich viele Befugnisse und auch ziemlich viele Sonderrechte. Da war also gefragt worden, müsse man da jetzt ein bisschen härter regulieren oder hingucken? Aber Pistorius hat wenig überraschend gesagt, nein, nein, also diesen Sonderstatus des MAD, das ist schon ganz okay so, für Regulierung sieht er da einfach gar keinen Bedarf. Auf Nachfrage hat Pistorius allerdings bestätigt, es gibt eine permanente Überwachung im Cyberraum, auch durch die

Bundeswehr. Und als wir wissen wie dann zu diesen Graubereichen der Austausch ganz konkret erfolgt, wollten, also wenn man die Schnittstelle zwischen innerer und äußerer Sicherheit nicht so ganz klar ist, da meinte dafür er, gibt es ja auch schon eine Institution, nämlich das Nationale Cyberabwehrzentrum und das würde man nutzen, um sich da Informationen über den Zaun zu werfen. Dann gibt es ja noch das sogenannte Zentrum für operative Kommunikation. Da ging es eine ganze Weile um das Thema, welche Aufgaben hat denn das? Die haben sich nämlich verändert. Also mit den neuen Bedrohungslagen sind dann neue Aufgaben gekommen. Früher war dieses Zentrum für operative Kommunikation eigentlich ausschließlich bei mandatierten Auslandseinsätzen aktiv. Die haben also Kommunikation mit den Locals in irgendeinem Ausland gemacht. Also ich stelle mir vor, Bundeswehr in Mali oder irgendein anderer dieser gruseligen Auslandseinsätze. Und dann wollen die da so nett angesehen werden oder sich selbst erklären gegenüber den Locals und drucken da so kleine Erklärbeerflyer und schmeißen die da raus. So war das früher. Heute funktioniert das anders. Heute hat das Zentrum auch Aufgaben wie breite Beobachtung des Internets, entdecken, analysieren und reagieren auf Desinformationskampagnen. Und das war für mich eine ganz neue Nachricht. Man bereitet auch vor, wie dieses Zentrum operativ kommuniziert im Fall des Landes- und Bündnisverteidigungsfall. Also da stellen sich mir ein paar Fragen. das wurde aber nicht näher erklärt. Apropos Verteidigungsfall, also es war auch immer wieder die Rede davon, was ist denn eigentlich, wenn der Verteidigungsfall gar nicht klar ist? Wann ist denn ein Cyberangriff ein Verteidigungsfall? Pistorius meinte, wenn man einen mandatierten Einsatz hat, dann kann das auch voll handlungsfähig sein, wie bei einem Verteidigungsfall. Aber so eine Mandatierung kommt ja nicht von der Bundeswehr und auch nicht von der Regierung, sondern vom Parlament. Wir sind ja eine Parlamentsarmee. Also die Bundeswehr ist eine Parlamentsarmee, ohne dass das Parlament sagt, Verteidigungsfall macht mal dieses oder jenes, machen die nichts. Und ein Einsatz im Inneren ist auch nicht ermöglicht. Also schlicht verboten. Da ist also nur passiver Schutz der IT gegen Angriffe von außen möglich. Aber wie werden denn dann Zuständigkeiten geklärt? Also ein Abgeordneter hat das sehr plastisch beschrieben und hat gesagt, wenn eine Bombe von irgendwoher auf ein AKW fällt, ist völlig klar, Bundeswehr ist zuständig. Wenn aber ein AKW durch einen Cyberangriff ausgeschaltet wird, dann ist es unklar. Was passiert denn dann? Da war die Antwort, die Bundeswehr, die liefert dann mindestens ein 360-Grad-digitales Lagebild, was also so passiert ist und was da wo beschrieben und gesagt wird. Aber es sei ja ganz typisch für

hybride Angriffe, dass unklar ist, von wem ein Angriff kommt. Das ist halt die Natur von Cyberangriffen. Das kennen wir auch alle schon seit ewigen Zeiten und deswegen ist es in solchen Zweifelsfällen im Inland immer Aufgabe vom Zivil- und Katastrophenschutz. Die müssen also Versorgung sichern, Schäden begrenzen, können die Bundeswehr zur Amtshilfe holen, aber ansonsten hat die Bundeswehr da halt nichts verloren. Das hat nicht alle Abgeordneten beruhigt. Also einer hat aufgerechnet, dass Bitkom in einem aktuellen Gutachten von 200 Milliarden Euro Schäden für die Wirtschaft in Deutschland sprach, allein durch Cyberattacken. Das soll sich ungefähr halber halber auf China und Russland verteilen. Und da war natürlich die Frage, ab welcher Schadenshöhe ist es denn ein Verteidigungsfall? Ist eine bisschen krude ab welcher Schadenshöhe Frage, ist es denn ein Verteidigungsfall? Ist eine bisschen krude Frage, finde ich. Pistorius hat natürlich geantwortet, dass das nicht definiert ist, weil es ja klar gibt, kein Preistag, ab dann ist Verteidigungsfall. Und er hat auch nochmal betont, nur wenn 100% sicher ist, dass ein staatlich gelenkter Angriff stattgefunden hat, dann kann eventuell ein Rückschlag erfolgen. Und das ist halt trotzdem eine politische Einschätzung, die halt nicht die Bundeswehr macht. Und ganz oft sind es halt kriminelle Attacken. Also die sind so oder so in der Regel verdeckt, also die Verursacher. Aber entscheidend ist ja die Intention. Und zum Beispiel viel ist ja einfach so Ransomware-Attacken, ja, da geht es um Kohle. Viele sind auch Spionagefälle, Wirtschaftsspionage, politische Spionage. Aber Spionagefälle, die lösen keinen Gegenschlag oder Verteidigungsfall aus. Das ist ja genauso, wenn irgend so ein Spion, hatten wir ja gerade die letzten Tage, chinesische Spione hier, russische Spione da. Wenn man die entdeckt, ist es ja nicht automatisch ein Verteidigungsfall gegen Russland oder China. Also das wäre ja ganz schlimm, dann hätten wir ständig Krieg. Also sowas ist da nicht. Wir haben also eine Mischung aus kriminellen Aktionen, aus Spionageaktionen und aus echten staatlichen Angriffen zum Beispiel gegen kritische Infrastrukturen. Aber man weiß es halt nicht wirklich so genau. Was ist gerade welcher Fall? Und solange man keine eindeutige Angreifer-ID hat, ist eben kein Gegenschlag möglich. Wir sind ja, das hat einen anderen Abgeordneten beschäftigt, laut Grundgesetz auch eine ausschließliche Verteidigungsarmee. Und ob das denn vereinbar sei mit proaktiven Aktionen, wie man sie zum Beispiel mit Hackbacks meint. Pistorius hat klargestellt, die Bundeswehr macht keine Hackbacks, hat aber auch gesagt, man braucht eine ehrlichere Diskussion. Man müsse sich also mal ausführlich mit Fragen beschäftigen. Was machen wir denn, wenn wir rein zufällig von einem geplanten Cyberangriff wissen, um den

dann zu verhindern? Das sei also eine riesige Grauzone und da müsse man auch mit ExpertInnen viel mehr darüber diskutieren. Ein bisschen schräger wurde es bei einer nächsten Frage, da wollte ein Abgeordneter nämlich wissen, hat also sozusagen kritisiert, dass offensive Cyberwaffen bisher gar nicht in Deutschland entwickelt werden von deutschen Unternehmen. Da ist man also abhängig von Drittstaaten wie zum Beispiel Israel. Wenn ihr jetzt zufällig am Palantir und ähnliches denkt, denkt ihr richtig. Das findet man eigentlich ganz furchtbar in dieses Zeugs. Aber dieser eine Abgeordnete, der fände es übrigens besser, wenn man das hier bei uns produziert und fragte, soll sich das nicht ändern? Mehr Produktion in Deutschland von offensiven Cyberwaffen. Mir stellen sich da die Haare hoch, ich kriege da Ekelpickel. Aber Pistorius meinte, oh ja, das muss mittelfristig das Ziel sein, aber weil es eine öffentliche Sitzung ist, muss er sich da jetzt zurückhalten. Da kann ich nur sagen, WTF. Ja, WTF ist auch das nächste Thema, wenn auch deutlich harmloser, da geht es nämlich um digitale Infrastruktur und Konnektivität. Da habe ich mal eine Frage gestellt, die kommt vom Jahresbericht der Wehrbeauftragten, paar Wochen erst alt, von 2024. Da steht nämlich drin, dass ein ordentliches WLAN in Unterkünften und Bildungsstätten ganz oft fehlen würde. Also da gibt es dann für die SoldatInnen einfach gar keins. Und das soll sich erst bis 2030 ändern. 2030. Loll, das ist echt lange hin. Also habe ich gefragt, ist das wirklich so? Und da meinte Pistorius, 80 Prozent der Unterkünfte sind doch versorgt, immerhin. Und ein paar Standorte sind halt sehr, sehr abgelegen. Die sind also generell nicht an digitale Infrastruktur angebunden. Und daher gibt es da halt noch die ein oder andere Verzögerung. Aber ich habe Ihnen dann noch mal ganz kurz darauf hingewiesen, es geht nicht nur um abgelegene Orte. Also zum Beispiel auch das Zentrum für Innere Führung in Koblenz hat laut diesem Bericht der Wehrbeauftragten kein WLAN. Und naja. Eine interessante Frage, deren Antwort sich länger hinzieht, war die Frage danach, welche Lehren, auch mit Digitalbezug, zieht denn das Verteidigungsministerium aus dem Krieg Russlands gegen die Ukraine? Pistorius sagte, ganz kurz gefasst, digitale Innovation braucht es in allen Bereichen. Ganz kurz digitale gefasst, Innovation braucht es in allen Bereichen. Es braucht künstliche Intelligenz, es braucht Drohnen für alles Mögliche und es braucht die schon erwähnte elektronische Kampfführung. Sein General Vetter hat das mit zwei Lehren ergänzt. Nämlich einerseits braucht man Durchsetzungsfähigkeit im elektronischen Kampf, inklusive Gegenmaßnahmen gegen das, was die anderen machen auf dem Bereich. Und zweitens, wahnsinnig wichtig, Erhaltung der Konnektivität. Er hat das mal am Beispiel der Drohnen ein bisschen ausgeführt. Der Ukraine-

Krieg, da werden ja massenhaft Drohnen eingesetzt, also von klein und billig bis teuer und groß. So wie am Anfang beschrieben, für Aufklärung und für Wirkung. Ihr wisst, was ich meine. Die sich selbst abstürzende Drohne. Und da sei es zum Beispiel wahnsinnig wichtig, die eigenen Drohnen zu schützen, davor, dass der Feind die abschießt oder anderweitig behindert. Aber auch sich gegen fremde Drohnen zu wehren, weil die machen natürlich das Gleiche. Und das bezieht sich auch auf die Konnektivität. Weil wenn die keine sinnvolle Funkverbindung mehr haben, dann können die halt nicht vernünftig gesteuert werden. Und das ist in der Ukraine offenbar ein ziemlich großes Problem. Manchmal prallen ukrainische Drohnen an so eine Art unsichtbare Wand, wenn nämlich die Funkverbindung von den Russen gekappt wurde, und dann stürzen die einfach ab. Und in dem Feld sei Russland ganz klar im Vorteil gegen die Ukraine. Und über sowas muss man natürlich nachdenken, wie das einfach nicht passiert. Der General Vetter hat vor allem einen Schwerpunkt draufgelegt, dass Deutschland sowohl für Informationen als auch für Aufklärung und diese Art von Wirkung mehr Kompetenzen aufbauen muss, aber insgesamt auch robust und resilient verfügbar machen muss. Und das bezog sich auch wieder auf das Thema Konnektivität. Und die findet ja vor allem, also gerade wenn wir auch so von kriegerischen Situationen, und das passiert ja immer öfter reden, die Konnektivität im Feld, wie man die sicherstellt. Und da sind wir ganz schnell bei Satelliten gewesen und dabei, wie in der Ukraine, auch das ganz schwierig war, dass es da diese große Abhängigkeit von Starlink gibt. Wer will von Elon abhängig sein? Ich nicht. Und die EU plant ja eigentlich dieses Iris also Iris hoch zwei Square, Satellitennetz. Das soll ein bisschen wie Starlink funktionieren. Und da kam natürlich die ob das Verteidigungsministerium Frage, sich daran beteiligt. Offensichtlich hat die Bundesregierung dann nämlich noch keine Entscheidung getroffen. Da gab es dann so Satelliten-Connectivity Laber, Laber, ja, total wichtig. Aber ob und wann dieses Iris-Programm die bestehenden Konnektivitätsprobleme lösen ist noch kann, völlig offen. Überhaupt wären noch ganz viele Fragen offen rund um dieses Satelliten-Programm. Aber man baut bereits massiv die Bodeninfrastruktur für Satellitenkommunikation aus. Also ich stelle mir da so riesengroße Schüsseln vor, auf Deutschland verteilt. Man guckt da auch nach privaten Betreibern, die man vielleicht unter Vertrag nimmt. Ich hoffe nicht, dass sie Elon nehmen, aber dieses europäische Iris-Programm, das dauert ja noch eine Weile und so oder so würde eine Satellitenkonnektivität eine viel höhere Resilienz ermöglichen. Und dieses Thema Konnektivität findet sich offenbar auch im Sondervermögen. Zum Thema Drohnen vielleicht

auch noch ein Satz. Die AfD kam da mit einer etwas kruden Frage und hat nämlich gesagt, die Ukraine hat ja irgendwie erklärt, sie will in diesem Jahr eine Million Drohnen bauen und wollte von Pistorius wissen, kann Deutschland das in diesem Jahr auch? Und Pistorius ein bisschen komisch geguckt, wie ihr vielleicht auch gerade. Warum sollte Deutschland in 2024 eine Million Drohnen bauen? Weshalb Historius dann auch sagte, die Frage ist ja total irrelevant, also wir sind ja gar nicht im Krieg. Richtig sei aber, auch Deutschland bräuchte eine Drohnenstrategie und es gäbe eine Taskforce Drohnen seit November 23. Ich hätte gedacht, die gibt es schon deutlich länger, aber die gibt es jetzt und man arbeitet dran. Natürlich gibt es immer auch das Thema künstliche Intelligenz. Da war also die Rede davon, was tut sich denn da so bei der Bundeswehr? Da gibt es ja ganz viele Sachen, die die machen, die wurden nicht alle angesprochen. Aber unter anderem ging es um die Digitalisierung im Gefechtsfeld. Dieses Projekt nennt sich offenbar gläsernes Gefechtsfeld. Schwieriges Wort. Und da ging es unter anderem um die Objekterkennung, die automatisierte. Also das passiert zum Teil über Sensoren. Man kann das aber deutlich verbessern, wenn man die Sensoren über KI vernetzt. Und ab 2026 soll es dann auch eine KI-gestützte Objekterkennung geben. Und dann, jetzt kommt wieder ein bisschen spezialmilitärisches Wording, sollen Effektoren eingebaut werden. spezialmilitärisches sollen Wording, Effektoren eingebaut werden. Ich übersetze das mal für euch auf Deutsch. Ein Wikipedia Effektor, sagt das so, ist ein Teil eines der Wirkung entfaltet. Waffensystems, Und was Wirkung habe ich ist, euch schon beigebracht. Also direkter ein Effektor ist das, gesagt, was zum

daher auch von einem Sensor-to-Shooter-Link, den man realisieren möchte. Also an der einen Stelle ein Sensor mit KI und am anderen Ende sozusagen der Abdrücker zum Schießen.

gäbe. Wer sich mit dem Thema Human in the Loop schon mal beschäftigt hat, der weiß, das hilft leider wenig. Da gibt es sowas wie Automation Bias und wenn die KI dir empfiehlt, das ist ein Feind, hau mal drauf, dann drücken die meisten Menschen Bestätigung. Da gibt es noch nicht genug Forschung, aber genug Forschung, die darauf hinweist, dass der Human in the Loop leider keine Lösung ist. Wo es auch noch KI geben soll, die nannten das als Einsatz als Management by Exception sein, dass man also Routine, Aufgaben, Analysen und so weiter durch KI erledigen lässt und den Mensch dann agieren lässt, wenn es irgendwelche Anomalien gibt. Und er hat gesagt, ein großes Problem heute ist nicht der Datenmangel im Feld, sondern

das gute Filtern von Daten für das Erreichen von Informationsüberlegenheit. Und Buzzwords haben wir noch nicht alle gehabt. Nee, Blockchain kommt nicht. Das ist ja inzwischen ausgestorben, mehr oder weniger. Aber über Cloud haben wir natürlich geredet. Und da wollte ich wissen, in der deutschen Verwaltungs-Cloud-Strategie, da steht ja ganz hart die Empfehlung drin, unbedingt auf Open Source zu setzen und auf europäische Dienstleister. Und meine Frage an das BMVG war natürlich, macht ihr das? Kurze Antwort war ja. Zwei Sätze mehr war, es gibt eine Private Cloud der Bundeswehr, die sehr stark auf Containerisierung baut und natürlich würden sie auch Open Source Produkte nutzen. Auch Open Source Produkte nutzen sagt natürlich nichts über das Ausmaß. Immerhin, ich gucke mir das aber nochmal genau an. Und ich habe auch nochmal das Thema F-35-Flieger angesprochen. Da wurden ja so Kampfflieger auch von diesen 100 Milliarden geshoppt aus den USA. Und da ist dann nach dem Shopping aufgefallen, dass die nur mit der AWS-Cloud von Amazon zu betreiben sind. Und da gab es ja diverse rechtliche Datenprobleme. Und ich wollte wissen, wie hat man denn das jetzt gelöst, weil immer wenn ich frage, kriege ich darauf keine Antwort und da hieß es, die Rahmenbedingungen sind vorgegeben, man kann die auch nicht verändern. Das heißt, es wird so genutzt, wie die Amis das halt im Paket anbieten und das ist mit AWS Cloud. Aber national souveräne Dinge, also Daten, die von so einer F-35 hier in Deutschland gesammelt werden, die müssen in einen souveränen Infrastrukturen auch verarbeitet werden. Und die bauen sie offenbar gerade und zwar am Standort Büchel. So kurz vor Schluss habe ich dann auch nochmal das Thema WebEx-Skandal angesprochen. Ihr erinnert euch, darüber haben wir ja mit der Bundeswehr schon geredet vor ein paar Wochen. Da gab es also diese WebEx-Videokonferenz, die die Russen abgehört haben, weil sich einer der Bundeswehrführungskräfte in Singapur per Telefon eingewählt hat, was eine Verletzung der Regeln war, weil es unsicher ist und offensichtlich auch unsicher war. Das wurde nämlich ausgenutzt und der ganze Inhalt komplett geleakt im Internet. Ich wollte also wissen, was hatte denn das jetzt für Konsequenzen, weil ja sämtliche Beteiligten die Regelverletzungen nicht bemerkt und kritisiert haben. Und es waren ja alles Führungskräfte. Pestorius erklärte, dass die Ermittlungen wegen der Disziplinarverstöße jetzt quasi dem Ende zugehen. Das war vor ein paar Wochen auch schon so.

Das war vor ein paar Wochen auch schon dass so, aber die Betroffenen selber in ihren eigenen Bereichen sehr stark als Sensibilisierer unterwegs waren, damit die Regeln, die alle kannten,

das war also nicht dass so, sie die Regeln irgendwie vergessen hatten oder nicht wussten, alle haben die gekannt, dass man die künftig auch einhält. Wäre ja mal so was, cyber-cyber-mäßig. Und seitdem hätte sich das Verhalten vieler auch deutlich verbessert. In dieser Videokonferenz war auch von der Nutzung von WhatsApp die Rede. Ich habe also auch nochmal nach diesem Bundeswehr-Messenger gefragt, das mache ich ja auch regelmäßig, und mir wurde erklärt, dass seine Nutzung jetzt auch stark zugenommen hätte. Der wäre jetzt auf 85.000 Smartphones deployed und das würde weiter steigen. Und als ich dann gesagt habe, naja, installieren, nicht gleich nutzen, nutzen die das auch, hat er gesagt, natürlich würden sie die Nutzung jetzt nicht explizit monitoren, aber sie hätten so ein spezielles Luftwaffengeschwader, das damit im Ausland sogar unter VSNFD-Auflage kommuniziert. Ganz zum Schluss noch eins meiner Lieblingsthemen. Ich frage ja einmal im Jahr die Bundesregierung auch, wie nachhaltig ihre IT ist. Und da hat natürlich auch das Verteidigungsministerium mir Ende 2023 geantwortet. Die haben nämlich vier Rechenzentren. Von denen nutzt kein einziges die Abwärme, kein einziges klimafreundliche Kältemittel und der Anteil erneuerbarer Energien hat sich in den zwei Jahren bis 2022 fast halbiert, von 65 auf 35 Prozent. Also falsche Richtung Entwicklung, würde ich mal sagen. Und es hieß aber, dass die jetzt da alles umstellen und irgendwie groß auszussen an diese BWI. Was sich da wie ändern wird? Alles soll sich ändern. Die bisherigen vier Rechenzentren sind quasi Elektroschrott, völlig veraltet, kann man nichts mehr mit anfangen. Aber sie werden jetzt ab 2025 bei der BWI Rechenzentrum as a Service einkaufen, dabei auch zivile Rechenzentren nutzbar machen, die neben den militärischen Anforderungen auch Nachhaltigkeitsaspekte berücksichtigen. Da muss ich mal genauer nachfragen, was genau das heißt, weil die Bandbreite ist da schon echt groß. Als Funfact, die AfD, die hat da noch angefangen, irgendwann so ein Bullshit von Tucker Carlson zu zitieren. Vielleicht habt ihr es mitgekriegt, der war da in Russland im Staatsfernsehen zu Gast und hat gebullshittet und da war Prestorius aber ausgesprochen souverän und hat gesagt, Berichterstattung von Tucker Carlson kommentiert er nicht. War die einzig sinnvolle Antwort auf diesen Müll von der AfD. Mein Fazit, hybride Konflikte sind heute eine Realität. In der Tat brauchen wir eine bessere Verteidigung, aber im sehr engen Sinne. Also Schutz vor Cyberangriffen, mehr Resilienz, schließen alle Sicherheitslücken. Und ja, Graubereiche sind kompliziert. Es gibt sie. Wir müssen auch darüber reden. Beunruhigend finde ich aber, wenn man dann darüber redet, mittelfristig müssen auch in Deutschland offensive Cyberwaffen hergestellt werden. Aber

natürlich auch, dass die Kulturfrequenzen für militärischen Funk genutzt werden sollen. Da ist mir schon echt lieber, man beteiligt sich an diesem europäischen Satellitenprojekt Iris hoch 2. zweites Ja, spannendes Thema war

Also wir haben ja längst im großen Stil Diebstahl, Industrie-Spionage, die digital Sabotagen, stattfinden. Haben wir ja in dem vorigen Thema auch hybride Bedrohungen und sowas alles. gehört, Und solche Angriffe brauchen Angriffsstellen, also Sicherheitslücken und Zugriff auf Systeme, die möglichst viele Menschen nutzen, möglichst große Honeypots. Und so ein großer Honeypot ist halt Microsoft, weil diese Produkte benutzen ja sehr, sehr viele Menschen weltweit. Und in den letzten drei Monaten hatten wir drei erfolgreiche Fälle in den Schlagzeilen. Das war so einmal im Juli 2023 ein Angriff von China, der nannte sich Storm 558. Da hat man einen Microsoft-Konto-Signaturschlüssel geklaut und damit Zugriff auf E-Mail-Konten von Personen einerseits in Unternehmen, aber auch in der US-Regierung zu erhalten. US-Außenministerium war kompromittiert, Mails vom US-Handelsministerium und noch etliche andere Stellen. Die Ursache dafür war eine ganze Kette, also nicht eine Sicherheitslücke, sondern eine ganze Kette von Fehlern auf Seiten von Microsoft, die bei Outlook waren, bei Office 365, bei OneDrive, bei Teams, also wirklich viele. Und wochenlang haben diese Angreifer ihr Unwesen treiben können. Microsoft hat es also wirklich wahnsinnig spät gemerkt und es ist jetzt immer noch nicht ganz klar, was die Hacker eigentlich gemacht haben. Also ob sie eventuell Daten manipuliert haben, ob sie eventuell Hintertür platziert haben, das wird also noch diskutiert. Es fragt sich dann auch, warum zum Beispiel Schlüssel aus dem Endkundenbereich, der da ursächlich war, warum der Unternehmensanwendung öffnen konnte. Also das darf eigentlich gar nicht sein. Deswegen überrascht es auch nicht, dass das von beiden eingesetzte Cyber Security Review Board geschrieben hat, Microsoft sei eine National Security Liability. Das ist schon mal eine echt harte Ansage. Und die Begründung dafür war, Microsoft würde weder die Enterprise Security Investitionen priorisieren, noch ein rigoroses Risikomanagement. wurde von einer Hackergruppe ausgeübt, die verschiedene Namen hat. Sie ist auch bekannt als Cosibear oder APT29. Dieser Angriff wurde im Januar 2024 bekannt und hat eine ganz klare Verbindung zur russischen Regierung und den Auslandsgeheimdiensten aus Russland. Vielleicht habt ihr von der Gruppe schon mal was gehört. Vielleicht habt ihr von der Gruppe schon mal was gehört. Das sind die 2016 das also die Mails der Demokraten, die, US-DNC, bei den US-Wahlen gehackt haben, was von Trump

natürlich hoffnungslos ausgenutzt worden ist. Und so wurde er ja dann tatsächlich auch Präsident und vielleicht hat dieser Angriff dazu beigetragen, eventuell. Ja, jetzt gab es also von denen einen neuen Hack gegen Microsoft. Sie haben Zugriff auf Quellcode und interne Systeme erlangt. Sie haben dafür Infos aus früheren E-Mail-Hacks ausgenutzt. Microsoft hat dann anschließend potenziell betroffene Kunden sofort kontaktiert. Und es hieß, dass der Angriff wohl schon seit ungefähr November 23 gelaufen ist. Und ob der wirklich zu Ende ist, scheint noch unklar zu sein. Das ist natürlich problematisch und Microsoft hat auch so in Salami-Taktik die Erkenntnisse öffentlich gemacht, was natürlich auch heißen kann, dass sie sie gar nicht sofort immer alle mitgekriegt haben. Ja, und der dritte Angriff, da ging es um einen öffentlich zugänglichen Azure, also Cloud Storage Server mit sehr sensiblen Zugangsdaten. Da sollen also über eine Million interne Microsoft-Dateien rumgelegen haben und da drinnen waren auch Adressen, da drinnen waren Zugangsdaten, Token für interne Microsoft-Dienste und so weiter. Das haben Sicherheitsforscher von Socradar entdeckt, diesen Storage Server, und dass der frei zugänglich für Dritte war. Da gab es einen Bericht auf Born City, den verlinke ich euch, der ist also sehr interessant, schreibt auch ein bisschen über die anderen beiden Angriffe, aber vor allem auch über diesen. Und der schreibt wörtlich, dieser Server, der frei zugänglich war, ohne irgendeinen Schutz, der enthielt Skripte und Konfigurationsdateien mit Passwörtern, Schlüsseln und Anmeldedaten, die von Microsoft-Mitarbeitern für den Zugriff auf andere interne Datenbanken und Systeme verwendet wurden. Das ist schon wirklich mega krass, weil damit hast du sozusagen eine Schublade aufgemacht mit lauter Schlüsseln drin, die man wiederum für Zugänge zu anderen Dingen bei Microsoft benutzen kann. Über diese Sicherheitslücke haben die Sicherheitsforscher Microsoft schon am 6. Februar 2024 informiert, aber erst einen fucking Monat später hat Microsoft reagiert und hat diesen Server gesichert. Also da stellen sich schon Fragen, warum sowas vier Wochen dauert. Wenn in der Zeit böswillige Akteure auf diese Daten zugreifen konnten und wer weiß, wie lange das vorher schon offen war, dann ergeben sich daraus weitere Möglichkeiten für folgenreiche Angriffe auf Microsoft-Dienste. Microsoft als Schwachstelle ist ja nicht neu, aber es scheint schon ein gewisses neues Niveau erreicht zu sein und das führt dann natürlich auch zu heftigeren Reaktionen. Also chinesische und russische Angreifer vor allem sind offenbar deutlich erfolgreicher mit dem Zugang, als man bisher so dachte. Und es ist natürlich ziemlich krass, wenn zumindest nach Meldungen Microsoft seit Monaten daran scheitert, die Hacker vollständ nutzen. Und weil ein bisschen

unklar war, was sind jetzt eigentlich die Folgen für Deutschland, wie groß ist die Betroffenheit, wie groß ist die Betroffenheit, aber auch wie abhängig ist eigentlich die Bundes-IT und wie gefährdet, deshalb hatten wir Microsoft eingeladen in den Digitalausschuss, aber auch das BMI und das BSI. Und die sind dann auch, also Microsoft zum Beispiel, in voller Mannschaftsstärke gekommen. Unter anderem Tom Bird, der Corporate Vice President, der aus den USA dazu geschaltet war und der auch in seiner Intro erstmal erzählt hat, dass es vor allem die staatlichen Akteure Russland, China, Iran und Nordkorea gäbe, Schwerpunkt Russland und China, die jeden einzelnen Tag 10.000 Fachsysteme den einzelnen von Tag 10.000 Microsoft Fachsysteme von angreifen. Microsoft angreifen. Und er hat dann so, das klang so ein bisschen wie, stellt euch vor, 10.000 jeden Tag und nur zweimal waren sie erfolgreich. Den dritten Fall hat er irgendwie gar nicht erwähnt. Aber er hat eingestanden, dass man signifikante Investitionen braucht, um besser geschützt zu sein. Dann ist er auf die Fälle, zwei Fälle nochmal eingegangen. Also einmal auf den chinesischen Hackerfall mit Storm 588. Die ordnet Microsoft dem militärischen Geheimdienst zu und er sagt, zwei Dutzend Kunden seien da betroffen, global, aus dem Privatsektor und aus Regierungen oder Behörden und man konnte das am Tag der Entdeckung sofort stoppen. Alle Betroffenen wurden informiert, drei Consumer-Accounts aus Deutschland waren auch dabei, aber keine Behörden oder staatlichen Stellen. Man hätte noch nicht so ganz verstanden, wie der Angriff abgelaufen ist. Man hat also da irgendeinen Consumer-Signing-Key verwendet, den hat China erbeutet, ein, zwei Jahre rumliegen lassen und dann später erst genutzt, um Tokens zu erzeugen, die man dann benutzen konnte, um in andere Dinge einzudringen. Tokens zu die erzeugen, man dann benutzen um in andere konnte, Dinge einzudringen. Also die diese Kette von Ursache, die ich schon Fehlern, mal erwähnt habe, die

Seit November 23 hat man auch generelle Gegenmaßnahmen angefangen, nämlich einmal KI einzusetzen, um Cyberattacken zu entdecken, aber auch sie zu bekämpfen. Man hat diesen ganzen Engineering-Prozess verändert. Und als Drittes möchte man darauf hinarbeiten, dass es die Adoption internationaler Norms of Nation-State-Conduct gibt. Das richtet sich an die Nationalstaaten, was die also tun sollen, nicht Microsoft. Das hat er später noch ein bisschen ausführlicher in der Debatte erklärt. Das nehme ich jetzt gerade mal ein bisschen vorneweg. Er hat sich dann nämlich beschwert über die vielen Staaten, die tatenlos zugucken, obwohl sie eigentlich alle betroffen sind. Und deswegen ist Microsoft auch diplomatisch viel

unterwegs und es soll mehr staatliche Maßnahmen geben. Zum Beispiel könnte er sich vorstellen, dass Staaten da so allgemeine Vereinbarungen treffen, dass sie auch mit Sanktionen vorgehen gegen notorische Angreiferstaaten. Zu dem zweiten Fall, dem russischen Hackerfall, hat der Microsoft-Vertreter also erstmal dem Angreifer Respekt und Anerkennung gezollt und hat gesagt, das ist der beste und fähigste Nation-State-Actor. Und dann hat er mich ein bisschen verwirrt, weil er gesagt hat, alleine dieser russische eine Angreifer würde 10.000 Angriffe täglich machen. Kurz davor war davon die Rede, dass es 10.000 täglich sind von Russland, China, Iran und Nordkorea. Und jetzt ist dieser eine russische, macht auch 10.000 täglich am Tag. Kann man ja auch mal ein bisschen durcheinander kommen. Aber er hat gesagt, da hatte der Akteur eine Testanwendung gefunden, die ziemlich viele Befugnisse eröffnet hat, die ausgenutzt worden sind. Und man hat dann vor allem E-Mails von Security-Verantwortlichen, aber auch von Führungsetagen abgezogen und hat außerdem noch Zugang zu Source-Code bekommen, aber nur lesenden, nicht schreibenden Zugriff. Also verändern am Source-Code konnten die nichts. Aber sie können natürlich auch Zugang zu Informationen erlangt haben, die bei weiteren Angriffen genutzt werden könnten. Also zum Beispiel Credentials, wenn die in irgendwelchen E-Mails erwähnt waren. Seit Januar, hat der Microsoft-Vertreter betont, sind mehrere tausende Fachleute damit befasst, A, den Angreifer abzuwehren, aber B, auch den Schaden zu beheben beziehungsweise alles sicherer zu machen. Der Angreifer würde aber nicht aufgeben und jeden Tag weiter Angriffe fahren und man müsse also immer sich Mühe geben, quasi einen Schritt schneller zu sein als der. Später hat er noch ergänzt, dass es nie einen Zugriff auf Kundensysteme gegeben hat. Also es war ausschließlich das Microsoft-Netzwerk und Microsoft-Ressourcen betroffen. Und es gäbe aggressive Angriffe mit sämtlichen Mitteln und Methoden, auch während des Angriffs erbeutete Informationen werden dafür verwendet. Und man kann nicht mit Sicherheit sagen, dass der Angreifer raus ist aus dem Netzwerk. Aber natürlich würde man das sehr genau beobachten. Wir sind jetzt alle total beruhigt, vor allem, wenn an keiner Stelle erwähnt worden ist, welchen Source-Code die eigentlich eingesehen haben. Weil vielleicht haben die da ja auch einfach eine Sicherheitslücke gefunden. Dazu reicht lesender Zugriff. eine Sicherheitslücke gefunden. Dazu reicht lesender Zugriff. In der Debatte hat dann ein Abgeordneter Microsoft gefragt, warum sie sich eigentlich dem chinesischen Sicherheitsgesetz unterworfen haben. Das ist nämlich ein besonders fieses Sicherheitsgesetz. Das verpflichtet nämlich Unternehmen, Sicherheitslücken, die sie

entdecken, zuerst chinesischen Stellen zu melden, damit die die ausnutzen können zum Rumhecken. Und zwar bevor sie sie veröffentlichen oder an andere, zum Beispiel an den Hersteller einer Software melden. Das wäre natürlich sehr, sehr krass, wenn Microsoft sowas macht. Aber sie haben das offenbar unterschrieben. Der Kollege von Microsoft hat aber gesagt, in keinem einzigen Fall hätte Microsoft jemals an China Sicherheitslücken vorab gemeldet, sondern, und das klingt jetzt als total, ist überhaupt nicht mehr schlimm, Ironie off, immer gleichzeitig an andere relevante Akteure, manchmal vielleicht sogar an diese vorab wurde einschränkend hinterhergeschobenelfall gleichzeitig. Dass dann natürlich trotzdem die Patches gar nicht so schnell kommen können, wie China vielleicht so eine Lücke ausnutzt, liegt auf der Hand. Das finde ich also schon ziemlich kacke von Microsoft, dass die sowas machen. Über BSI und die Rolle des BMI haben wir auch gesprochen. Das BSI hat uns erklärt, dass es schon vor der Veröffentlichung durch Microsoft immer vorab informiert worden ist, mal mit ein bisschen mehr, mal mit ein bisschen weniger Vorlauf. Und sie haben eigentlich auch trotz eigener Recherchen keine anderen Informationen zur Betroffenheit von Deutschland. Also bei Storm 588 diese drei Einzelaccounts und bei dem anderen gar keine deutschen Betroffenen. Wobei sie sagen, 100 Prozent sicher kann man sich natürlich nicht sein, ob nicht doch mehr kompromittiert ist. Es würde einen sehr engen Austausch geben zwischen der US Cyber Security und Infrastructure Security Agency. Die hat nämlich, vielleicht habt ihr es mitbekommen, eine Emergency Directive herausgegeben und hat alle US-Behörden gewarnt und zu speziellen Prüfungen aufgefordert. Als wir dann gefragt haben, ja, warum macht denn das BSI sowas nicht, erklärte das BSI uns, dass es dafür keine Veranlassung gab, weil in den USA waren ja Behörden-E-Mails betroffen und bei uns aber kein einziger Behördenkunde. Das ist faktisch wahrscheinlich so, aber es gibt auch Medienberichte, zum Beispiel bei Heise, die reden von einer Beißhemmung des BSI gegenüber Microsoft. Ich verlinke euch den Text mal in den Shownotes. Insofern wirkt es manchmal schon, als würde das BSI da sehr zart mit Microsoft umgehen und die Tonlage in den USA auf staatlicher Ebene da schon noch eine andere ist. Das BSI hat auch analysiert, dass die Strategie der Hacker-Group ein bisschen anders wäre jetzt. Also nach der Entdeckung der Microsoft-Angriffe im Februar hat sich die Angriffsintensität verzehnfacht. Und im Prinzip haben die eine Sieben-Tage-Woche gehabt, also die Attacker. Normalerweise würde bei so einer Entdeckung eines Angriffs ein sofortiger Rückzug erfolgen und alle Spuren würden gelöscht werden. Da war es genau andersrum. Also da hieß es einfach nur jetzt extra Attacke und deswegen kämpft auch

Microsoft offenbar immer noch gegen die. Das BSI hat uns auch erklärt, die sind sogar nach Redmond gefahren, haben da also mit Microsoft einen Workshop gemacht, um tiefer zu verstehen, was die Ursachen und die Folgen sind. Für das BSI sind aber diese Sicherheitsprobleme also nicht neu und auch nicht mehr geworden. Und die wiesen darauf hin, dass es zum Beispiel in Deutschland 17.000 Microsoft-Exchange-Server gibt mit offenen, nicht gepatchten Sicherheitslücken, die auch das BSI offen kommuniziert. Aber da passiert halt offenbar wenig. Das ist natürlich auf User-Seite auch ein Problem. Problematisch am Umgang von Microsoft fand das BSI, dass manchmal die Offenlegung auch erst auf Druck erfolgt ist. Das war also schon bei der Börsenaufsicht in den USA so, aber auch das BSI musste schon den rechtlichen Weg nutzen, um Infos zu erhalten, woraufhin Microsoft sich verteidigte. Das war doch alles nur Missverständnis. Immer würde man total gerne alle Informationen rausgeben, aber da musste man es halt doch mit Zwang tun. Und es sei um die interessante Frage gegangen, sind oder waren die Angriffe auf souveräne Clouds im Rahmen von diesem Storm 588, also 588 Attacke möglich? Da habe ich dann mal nachgefragt,

was war denn eigentlich die Antwort, die da erzwungen worden ist von Microsoft? Sind Angriffe auf die souveräne Cloud mit Microsoft möglich oder ausgeschlossen? Und das BSI hat dann erklärt, das war dass scary, die Diskussionen dazu noch laufen, dass technische Fragen zu klären sind und dass das noch bis Mai dauern Also kann. es ist nicht geklärt, ob die souveräne Cloud sicher ist vor solchen Angriffen. Das Einzige, was das BSI noch klargestellt hat, ist, dass die geplante Delos-Cloud für den Bund, dass die sicher sei vor solchen Angriffen, dass es um die Klärung ging, ob Angriffe auf die Clouds von anderen möglich sind oder ob die auch sicher sind. Souveräne Clouds, wie gesagt. Ich würde dann nochmal anmerken, dass die Abhängigkeit vom proprietären Produkt natürlich trotzdem bleibt, auch wenn ich eine Delos-Cloud mache, denn Delos ist zwar ein deutsches Unternehmen, aber die Cloud von Delos basiert auf Azure von Microsoft und da wäre es doch deutlich besser, man würde wirklich gemäß der Verwaltungsstrategie, Verwaltungs-Cloud-Strategie auf Open-Source setzen mit einem europäischen Dienstleister. Um Cloud ging es dann auch noch ein bisschen und auch um das Thema Souveränität und Abhängigkeit vom Bund.

wurde Microsoft gefragt, die wollen ja für alle Kunden ab 2025 nur noch Dienste in der Cloud anbieten. Die wollen also alle in die Cloud zwingen und die Frage war, ist denn das unter der

aktuellen Sicherheitslage überhaupt angemessen? Aber Microsoft findet es angemessen. Ich lese euch mal vor, was die wörtlich gesagt haben. Das habe ich mir aufgeschrieben, weil ich es so krass fand. It's an absolutely right and strategic move to go to the cloud. Microsoft or other, we can provide best security in the cloud. Warum nochmal? Haben wir die eigentlich in den Digitalausschuss eingeladen? Ich muss nochmal drüber nachdenken. Irgendwas mit Sicherheit. Naja, aber we bring the power of AI to the Cloud. Also mit KI gibt es kein Problem mehr. Ist klar, glauben wir alle. Wir wollten natürlich auch wissen vom Innenministerium, wie kann man denn jetzt die Abhängigkeiten verringern? Aber die neue, nagelneue Abteilungsleiterin für das Thema Cybersicherheit im BMI hatte leider keinen Ton und ihr Kollege im Raum, der kannte sich da nicht aus. Wir haben also diese Antwort nicht vom BMI beantwortet bekommen.

Ich habe dann mal Microsoft

Microsoft Deutschland antwortete sehr zynisch, nämlich wir zwingen doch niemanden, mit uns Verträge abzuschließen. gar es gibt ja überhaupt kein Nö, Login. nicht, So eine Antwort finde ich absolut frech. Ich habe also nochmal nachgehakt und habe gefragt, werden Verträge möglich sein ohne cloudbasiertes Office 365? das kann ich aus meiner Rolle heraus nicht sagen. Antwort, Die Verhandlungen laufen ja noch. Verhandlungen. Hm, Ich wollte mit wissen, wem verhandeln Sie denn da? Mit dem BMI war die Antwort. BMI ist ja interessant. Ich habe nämlich gerade dieser Tage eine schriftliche Frage zurückgekriegt, wo ich gefragt habe nach den Verhandlungen zu dem Rahmenvertrag 2025. Da das BMI verhandelt stand, überhaupt nichts mit Microsoft. Ich verlinke euch die Frage in den Shownotes. Und da meinte doch tatsächlich dieser Kollege, ich muss gleich wieder lachen, dann ja, wird man da wohl von Gesprächen reden müssen, nicht von Verhandlungen. Da weiß ich dann auch nicht mehr. Muss ich jetzt meine schriftlichen Fragen zweimal stellen, mal nach Verhandlungen, mal nach Gesprächen fragen, um eine Antwort zu kriegen, die irgendwie Sinn macht? Manchmal ist das Leben als Abgeordnete wirklich ermüdend. Aber wo wir von digitaler Souveränität reden. Ich wusste ja, dass die Kollegin vom BMI akustisch beschnitten war. Die konnte schlicht nichts sagen, war von der Ferne zugeschaltet. Deswegen habe ich denen eine Frage mitgegeben, die wir dann aber leider nur schriftlich bekommen werden, nämlich ob diese Microsoft-Hacks die Stärkung digitaler Souveränität im Bund beschleunigen würden. Das Zendes ist jetzt

komplett unterfinanziert, das spricht dagegen und ich wollte wissen, ist dann eine Exit-Strategie in Arbeit? Ein Kollege hat übrigens dann auch noch erzählt, dass er nicht mal herausgefunden hat, welche Anzahl Microsoft Lizenzen es im Bund gibt. Und das müsste man ja eigentlich wissen, um eine Risikobewertung vernünftig machen zu können, aber kein Rankommen an diese Zahl. Dieser Kollege hat auch vorgeschlagen, dass wir regelmäßig im Digitalausschuss Microsoft vorladen und auch die Bundesregierung, denn er meint, Microsoft und die Abhängigkeit von Microsoft sind ein Sicherheitsrisiko für den Staat. Mit Open Source könnte man sich ja besser schützen und daraufhin meinte das BMI nur, wir sind ja nicht auf Microsoft festgelegt. Nee, sind sie nicht, aber irgendwie gibt es da schon so eine Microsoft-First-Strategie, könnte man meinen. Das BSI habe ich noch gefragt, wenn dieses Cyber Security Review Board von Biden sagt, Microsoft ist eine National Security Liability, wie sieht denn das das BSI? Das BSI sagte dann, war früher schon genauso schlimm, ist jetzt gar nichts anders, aber wir sind ja ganz toll aufgestellt in Deutschland. Und lustigerweise kam dann, wir haben ja das Zendes, wir entwickeln den Open-Source-Arbeitsplatz. Hallo, ihr lasst das Zendes verhungern. Ihr entwickelt zu wenig Open-Source. Sehr, sehr wenig. Das habe ich euch ja auch schon in anderen Podcasts erklärt. Und es wurde gesagt, neu sei aber jetzt, dass es große Angriffe auf Cloud-Infrastrukturen gäbe. Und deshalb sei die Multi-Cloud-Strategie so wichtig. Dann könne man nämlich ganz schnell bei Angriffen wechseln zu anderen Anbietern. Also das, ehrlich gesagt, halte ich für eine totale Illusion. Da wäre es schon besser, vielleicht von Anfang an, nicht auf so einen Mega-Honeypot Microsoft zu setzen. Kleiner Fun-Fact, Microsoft hat noch erzählt, sie wollen die sicherste Corporate Environment in der ganzen Welt werden und in der nächsten Woche, also um den 1. Mai herum, wollen sie ein Big Announcement machen, was sie da alles für Maßnahmen machen. Super Investments, totaler Kulturwandel, Security First Strategy. Vielleicht lest ihr da ja irgendwas. Kleines Fazit, die Abhängigkeit von Microsoft ist und bleibt ein Sicherheitsrisiko. Der Bund ist wahnsinnig intransparent, selbst zum Grad der Abhängigkeit, und das ist bitter, also wenn man nicht mal die Anzahl Lizenzen rauskriegt, ist schon schlimm. Und Multicloud-Strategie in Deutschland beim Bund heißt Microsoft-First-Cloud-Strategie, trotz Hackerangriffen. Und das frustriert parteiübergreifend. Das war also im Digitalausschuss ganz klar erkennbar. Auch der Wunsch nach einer Exit-Strategie kam keineswegs nur von mir. Und das zeigt, wie wichtig es ist, mehr Open Source zu fördern, auch durch den Bund, aber auch zu nutzen. die Sicherheitsprobleme und ich hoffe da frage ich nochmal nach, sehr, dass bei den in Anführungsstrichen Gesprächen

der Bund deutlich macht, rein in der Cloud nimmt das es einfach nicht. und weil das jetzt schon ein relativ langer Podcast zu zwei harten Ja, und schweren Themen war, werde ich auf das dritte Thema AI-Akt wirklich nur kurz eingehen. Wir haben eingehen. darüber Wir haben ja auch darüber schon drölfzigmal ja auch schon geredet. drölfzigmal Es gibt geredet. nicht Es gibt nicht so wahnsinnig so wahnsinnig viel viel Neues. Neues. Ich hatte in den Podcast-Folgen 8, 12, 18, 23, 24 und 26 drüber geredet. Ich verlinke euch die nicht alle. Ihr wisst, wo ihr meine Podcast- Folgen findet. Ich verlinke euch nur die Folge 26. Da habe ich meine Kritik am AI-Act ausführlich ausgeführt. Und ansonsten erzähle ich euch jetzt nur super knapp, wie es damit weitergeht. Also zum einen gibt es ja einen Zeitplan mit unterschiedlichen In-Kraft-Tret-Zeitpunkten. Die Verbote zum Beispiel gelten direkt schon ab Mitte diesen Jahres, ab 2024. Regeln für General Purpose AI, also generative KI, die gelten Anfang 2025 und Anfang 2026, da gilt dann der ganze Rest. Innerhalb von zwölf Monaten muss sich aber die Bundesregierung schon mit Bußgeldvorschriften und Behördenstruktur gegenüber der Europäischen Kommission erklären. Es gibt da also diverse Dinge, die relativ bald passieren müssen und dafür gibt es eine interministerielle Arbeitsgruppe. Die arbeitet schon, aber hat noch praktisch nichts entschieden. Deswegen war im Gespräch im Digitalausschuss die häufigste Antwort, da sind wir noch in Abstimmung. Egal, ob es um die Aufsichtsstruktur geht, um den Umgang mit biometrischer Fernidentifikation, um Zuständigkeiten, also alles unklar. Das war auch ein öffentlicher Punkt in der Debatte. Ihr könnt euch es also auch in epischer Breite anhören, wenn ihr da genauere Dinge wissen wollt. Ansonsten weise ich euch noch gerne hin auf eine erste interessante Stellungnahme des Zentralverbands der Verbraucherschützer zur Umsetzung des AI-Acts. Verlinke ich auch in den Shownotes. Da geht es also um das Thema einfache Beschwerdeverfahren, konsequentes Verbot biometrischer Fernidentifikation. Auch unseren Antrag dazu verlinke ich euch nochmal und um das Thema KI-Beirat. Also mehr will ich euch da jetzt gar nicht nochmal neu erzählen. Wir bleiben am Thema generell aber dran. Ein paar Terminhinweise vielleicht noch am 25.04., am gleichen Tag dieser Aufzeichnung, also vor wenigen Stunden, habe ich eine Rede gehalten zu einem Antrag der Union. Da geht es um internationale Digitalpolitik. Da hat die Bundesregierung eine Strategie veröffentlicht, die ich absolut ungenügend finde. Und der Antrag der Union ist auch ungenügend. Und meine Rede verlinke ich euch. Ihr könnt euch also anhören, warum ich die Kacke finde. Und es gibt zwei öffentliche Anhörungen. Falls euch das interessiert, wie immer, könnt ihr euch mit Vor- und Nachnamen und Datum der Anhörung per E-Mail wenden an adi.bundestag.de. Einmal am

15. Mai gibt es eine Anhörung zur nationalen Umsetzung des AI-Acts. Unseren Sachverständigen haben wir bei Algorithmwatch gefunden. Vielen Dank, liebes Algorithmwatch, dass ihr uns da wieder unterstützt. Und am 26. Juni gibt es eine öffentliche Anhörung zum Thema innovative Datenpolitik. Auch dafür könnt ihr euch gerne anmelden. Und damit wünsche ich euch, wo immer ihr seid und wann immer ihr das hört, einen schönen restlichen Tag, Abend, Nacht, Morgen oder was auch immer. Bleibt gesund und bis zum nächsten Mal.