KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen

Cyberwar - Das Internet als Waffe

Von Matthias Becker

Sendung: Montag, 6. April 2020, 8:30 Uhr
Redaktion: Sonja Striegl
Regie: Günter Maurer
Produktion: SWR 2020

Neben Land, Luft und Wasser ist ein weiteres Schlachtfeld eröffnet: das digitale. Wie soll sich Deutschland für den Cyberkrieg wappnen? Oder muss es Regeln für den Cyberpeace geben?

SWR2 Wissen können Sie auch im **SWR2 Webradio** unter www.SWR2.de und auf Mobilgeräten in der **SWR2 App** hören – oder als **Podcast** nachhören:
https://www.swr.de/~podcast/swr2/programm/swr2-wissen-podcast-102.xml

---

MANUSKRIPT

Musik: (martialische elektronische Musik, unter den O-Tönen)

O-Ton 1 Felgentreu:
Jetzt stellen Sie sich mal vor, es würde gelingen, über einen Hackerangriff das deutsche Stromnetz für eine Woche abzuschalten, was das für Folgen hätte. Da fliegt nicht eine einzige Bombe, aber die Wirkung wäre schlimmer als eine Serie terroristischer Anschläge übers ganze Land verteilt.

O-Ton 2 Kleinwächter**:**
Neue Angriffswaffen werden produziert, die dann die Entwicklung neuer Verteidigungswaffen auslösen, und wir haben so etwas wie ein Wettrüsten im Cyberspace.

O-Ton 3 Domscheit-Berg:
Das Problem mit diesen Cyberangriffen ist, dass man sie zwar deklariert als Verteidigungsfall, dass man im Unterschied zu konventionellen Angriffen – gar nicht genau sagen kann, wo dieser Angriff herkam. Das heißt, ich schlage zurück, ich hole aus zum Gegenschlag, ohne zu wissen, wer eigentlich wirklich der eigentliche Täter war!

Atmo: (Musik weg)

Sprecher 2:
„Cyberwar – Das Internet als Waffe“ von Matthias Becker

Sprecher:
Im Dezember 2019 koppelte sich die Justus-Liebig-Universität in Gießen vom Internet ab – unfreiwillig. Das heute-Journal berichtete:

O-Ton 4 Heute-Journal:
Die Computer in der Bibliothek heruntergefahren, digitale Recherche nicht möglich, das Internet gekappt. Nach einem Hackerangriff vor mehr als einer Woche sind 28.000 Studierende und über 5000 Mitarbeiter an der Universität Gießen noch immer *offline*.

Sprecher:
In den Computernetzwerken der Uni hatte sich Schadsoftware eingenistet. Als die Mitarbeiter im Rechenzentrum dies schließlich bemerkten, konnten sie nur noch die *Server* abschalten. Mit drastischen Folgen: die Webseite der Uni war nicht erreichbar, Studierende konnten keine Emails mehr über ihre Uni-Adresse verschicken, selbst das WLAN ging nicht. Aus Sicherheitsgründen setzten die Administratoren alle Passwörter zurück. Den Studierenden und Mitarbeitern wurden neue Zugangsdaten nur persönlich, auf Papier ausgehändigt.

O-Ton 5 Heute-Journal (Studentin):
„Ja, wenn man gerade dabei ist, seine Examensarbeit zu schreiben, und dann auf einmal keinen Zugriff mehr auf Internet-Ressourcen hat, also *Ebooks* und so weiter, ist schon schwierig.“ Bei dem Virus handelt es sich wohl um den Trojaner Emotet, er ist in einer Email versteckt. An der Universität Gießen könnte es noch Wochen dauern, bis die Systeme wieder laufen.

Sprecher:
Die Hochschule war nicht das einzige Opfer. Emotet legte im vergangenen Winter zahlreiche Behörden und Unternehmen lahm. Und im Zuge der Corona-Krise werden aktuell verstärkt Krankenhäuser mit sogenannter Ransom-Ware angegriffen. Dabei handelt es sich um Software, die den Inhalt der Festplatten verschlüsselt, um für diese Daten von den Nutzern sozusagen Lösegeld zu erpressen.

Internetkriminalität ist zu einer globalen, umsatzstarken und arbeitsteilig differenzierten Branche geworden. Das weiß auch Andreas Könen. Er leitet die Abteilung Cyber- und Informationssicherheit im Bundesinnenministerium.

O-Ton 6 Könen:
Emotet zeigt, dass es Angriffe gibt, die sich immer mehr professionalisieren, und dann verschiedene Methoden etwa der Erpressung oder der Spionage miteinander vereinen. Das ist eine neue Entwicklung. Wir sehen also, dass das, was früher als APT-Angriffe nur staatlichen, nachrichtendienstlichen Stellen zur Verfügung stand, jetzt auch der organisierten Kriminalität mittlerweile zur Verfügung steht.

Sprecher:
Die sogenannten Cyberangriffe sind in gewisser Weise die Kehrseite der Digitalisierung. Immer mehr Geräte sind mit Prozessoren ausgestattet, ferngesteuert, miteinander vernetzt. Immer mehr alltägliche Abläufe werden über das Internet organisiert. Aber unsere digitale Infrastruktur ist verwundbar.

Das ist nicht nur für Kriminelle interessant, sondern auch für andere Staaten, erklärt Andreas Könen.

O-Ton 7 Könen:
Bei staatlichen Akteuren ist es so, dass eine Entwicklung zu sehen ist, die bei der klassischen Cyber-Spionage beginnt, aber auch da stärker in Sabotage-Szenarien geht. Wir sehen immer mehr, dass Produktionstechnologie und ähnliches durch Cyberangriffe attackiert wird, die offenbar auch von staatlichen Akteuren stammen.

Sprecher:
Wer hat die Universität Gießen angegriffen? Stecken hinter einer Schadsoftware wie Emotet Staaten oder Kriminelle? Oder: beide? Befinden wir uns bereits in einer Art Kriegszustand, einem „Cyberkrieg“?

Eine gezielte Attacke könnte große Teile Deutschlands lahmlegen, warnt jedenfalls der leitende Beamte aus dem Bundesinnenministerium:

O-Ton 8 Könen:
Stellen Sie sich vor, eine kritische Infrastruktur, Energie oder Wasser würde durch einen potenten Angreifer in solch einer Weise attackiert, dass tatsächlich die Versorgungsleistungen nicht mehr zur Verfügung stehen. Ein Energieverteilzentrum fällt aus, in Deutschland gibt's vier von denen, das heißt also, grob ein Viertel der Bundesrepublik oder angrenzender Staaten wäre durch einen solchen Ausfall unmittelbar betroffen, und wir müssen dann sehen, welche Mittel benötigen wir, um solcher Angriffe Herr zu werden.

Atmo

Sprecher:
Über das Internet können Eindringlinge nicht nur Informationen abgreifen, sondern auch Infrastrukturen lahmlegen. Die Angriffe sind vielfältig – wie aktuelle Schlagzeilen aus der Presse deutlich machen.

Sprecher 2 (Schlagzeilen):
Russische Hacker greifen Wahlkampfteam des französischen Präsidenten an.

Cyber-Attacke auf österreichisches Außenministerium – Bundesheer hilft.

Iran meldet Abwehr eines Internet-Angriffs.

Atmo:(Musikakzent)

Sprecher:
Bisher gab es weltweit nur eine Handvoll von Vorfällen, bei denen Gegenstände oder Personen zu Schaden kamen. Dokumentiert sind allerdings zahlreiche Versuche, in die Steuerungssoftware von Industrieanlagen und kritischen Infrastrukturen vorzudringen.

Andreas Könen vom Bundesinnenministerium und sein Minister Horst Seehofer wollen aus diesem Grund neue Befugnisse für die Sicherheitsbehörden.

O-Ton 9 Könen:
Netzblockaden, dem Angreifer den Zugang verwehren, die kritischen Infrastrukturen vom Netz weitestgehend trennen. Und dann vielleicht in einem letzten Fall, wo keine dieser Gegenwehrmöglichkeiten mehr hilft, dann in eine aktive Maßnahme einzusteigen. Entweder, dass der Angriff an sich beendet wird, dass also die Programme, die dort auf einem Server laufen, nicht mehr ihren Angriff verüben können, oder auch einen solchen Server ausschalten durch einen eigenen Cyber-Angriff.

Sprecher:
Welche Behörde diese Maßnahmen durchführen würde, ist unklar. Das Problem: für einen solchen „Gegenangriff“ müssten die Beamten im Zielsystem Passwörter erzeugen sowie Verschlüsselung und Zugangssperren überwinden. Kritiker sprechen deshalb vom „*Hackback*“ (*englisch aussprechen*). Davor warnt Anke Domscheit-Berg, parteilose Bundestagsabgeordnete für Die Linke und Expertin für Netzpolitik.

O-Ton 10 Domscheit-Berg:
Jede Art von Phantasie, uns durch Angriff zu verteidigen, ist verurteilt dazu, nach hinten loszugehen und mehr Schaden anzurichten als sie nützt. Es muss also ein Bekenntnis zur friedlichen IT-Sicherheit geben.

Sprecher:
Anke Domscheit-Berg ist gegen digitale Gegenschläge. Sie argumentiert, dass solche Aktionen die Falschen treffen könnten.

O-Ton 11 Domscheit-Berg:
Ich treffe vielleicht einen Server, von dem ich denke, von diesem Server ging was aus und das können auch völlig zivile Server sein, die in Krankenhäusern, Behörden oder sonst wo stehen. Ich kann da in anderen Ländern kritische Infrastruktur schädigen, und die anderen Länder können das, ganz zurecht, als Angriff interpretieren. Und schon bin ich in einer schwer wieder aufzuhaltenden Spirale von Eskalation, vielleicht auch einer militärischen Eskalation, die dann auch ganz schnell in das Analoge umschlagen kann.

Sprecher:
Wer hat mich angegriffen? Aktionen einer Schadsoftware einwandfrei bestimmten Personen zuzuschreiben, ist äußerst schwierig. Gesteuert werden die Programme über hintereinander geschaltete Internetserver. Die eigenen Spuren zu verwischen und falsche Fährten zu legen, dass Lernen Hacker als allererstes. Selbstverständlich verschlüsseln sie ihre Datenübertragung. IT-Fachleute können später nur Indizien zusammentragen, wer dahintersteckt – genug, um einen Gegenangriff zu begründen?

Hinzu kommt ein weiteres Problem: um einen digitalen Angriff zu beenden, müssten die Beamten erst einmal in das angreifende Computersystem eindringen und dort die Kontrolle übernehmen, Das geht aber nur, indem sie Sicherheitslücken im dortigen Betriebssystem ausnutzen.

O-Ton 12 Domscheit-Berg:
Also, das halte ich für extrem gefährlich, weil ein *Hackback* ohne geheimgehaltene Sicherheitslücken nicht funktioniert. Und in dem Moment, wo ich Sicherheitslücken mir in die Schublade lege, um sie eines späteren schönen Tages für Gegenangriffe oder andere Dinge einzusetzen, verhindere ich, dass diese Sicherheitslücke geschlossen wird. Faktisch ist das ein Angriff auf unser aller IT-Sicherheit!

Sprecher:
Schwachstellen im Betriebssystem eines Computers, die noch nicht öffentlich bekannt sind, sind der Dreh- und Angelpunkt im *Cyberwar*.

Ohne sie können Kriminelle nicht erpressen, Nachrichtendienste nicht spionieren und Polizisten nicht überwachen. Neue Sicherheitslücken wollen *alle* haben: russische Kriminelle, nordkoreanische Agenten, deutsche Polizisten und amerikanische Militärs.

Atmo Offensive-Con: (Stimmengewirr in der Hotel-Lobby) / (Sprecher über Atmo)

Sprecher:
Berlin im Februar. In der Halle des Hilton-Hotels ist es eng und laut.

Atmo: Offensive-Con

O-Ton 13 Ungeheuer:
Wir haben hier Gäste aus der ganzen Welt, also es gibt, glaub ich, wenig Länder auf der Welt, die hier nicht vertreten sind.

(Sprecher über Atmo)

Sprecher:
Patrick Ungeheuer arbeitet für die Firma *Blue Frost*, die die *Offensive-Con* veranstaltet. Die Konferenz will „die Hacker-Community zusammenbringen“. In Workshops und Vorträgen vermitteln international bekannte Experten neue Methoden, um in Betriebssysteme einzudringen und Digitaltechnik aller Art zu übernehmen.

Atmo: Offensive-Con

O-Ton 14 Ungeheuer:
Die Konferenz ist sehr stark *research*-ausgelegt, das heißt es geht in Richtung Schwachstellen finden, sogenannte 0-days-Schwachstellenanalysen, Schwachstellen in verschiedenen Produkten, Microsoft-Produkten, Techniken, wie kann ich Schwachstellen ausnutzen. Es ist sehr stark praxisgetrieben.

(Sprecher über Atmo)

Sprecher:
Die offensiven Fähigkeiten nutzen viele der Konferenzbesucher für das *Pentesting (Aussprache: englisch)*. Im Auftrag von Unternehmen dringen sie in deren Netzwerke ein.

Solche Penetrationstests erfüllen die gleiche Rolle wie Crashtests in der Automobilindustrie: Sie zeigen, wie sicher ein Computer-System wirklich ist und wo nachgebessert werden muss.

Atmo 4: Offensive-Con Vortrag

Sprecher:
Die Konferenz dient zur Kontaktpflege, Fortbildung – und als *Marktplatz*. Hauptsponsor ist die amerikanische Firma *Zerodium.* Sie handelt mit Schwachstellen.

O-Ton 15 Ungeheuer:
Genau. Äh … (Kichern)

Sprecher:
Patrick Ungeheuer will die Geschäfte von *Zerodium* nicht kommentieren. Eine Interviewanfrage lehnt die Firma ab.

O-Ton 16 Schröder – geteilt:
Der Handel mit Schwachstellen ist ein ziemlich lukratives Geschäft geworden für viele. Da haben sich Firmen auf dem Markt etabliert, die handeln mit Schwachstellen, das heißt, die werben gezielt auf Hacker-Veranstaltungen und sagen halt: Hier, wenn ihr mal eine Sicherheitslücke gefunden habt, dann meldet die doch nicht an den Hersteller, sondern kommt zu uns.

Sprecher:
Die Rolle von Broker-Firmen wie Zerodium erklärt der IT-Sicherheitsforscher Thorsten Schröder, er ist Geschäftsführer der Firma *Modzero (englisch aussprechen)*, die auf Computersicherheit spezialisiert ist.

O-Ton 17 Schröder:
Und dann überbieten die sich dann gegenseitig auf den Hacker-Veranstaltungen. Ich sag mal, für so ein *Exploit* gehen halt locker 500.000 Dollar über den Tisch. Und dann gibt es halt unabhängige Forscher, die sagen: „Ich kann davon prima leben. Wenn ich einmal im Jahr eine fetten *bug* finde in diesen großen, breit eingesetzten Produkten, dann verkauf ich die halt für eine halbe Million oder 200.000, und damit komm ich gut über die Runden."

Sprecher:
Eine Ursache der steigenden Preise ist die wachsende staatliche Nachfrage, erklärt Thorsten Schröder.

Er kritisiert, dass Broker-Firmen wie *Zerodium* keineswegs nur demokratische Rechtsstaaten beliefern.

O-Ton 18 Schröder:
Ich find, das ist halt unglaublich unsympathisch auch also ich kann dieser Branche überhaupt nichts abgewinnen. Denen ist es halt auch völlig egal, ob Leute zu Schaden kommen. Die beliefern eben auch Dienste und Staaten, die auch offenkundig Dissidenten jagen und umbringen. Das ist eben ein Grund, weswegen ich mit dieser Branche so nichts zu tun haben will.

(Musikakzent)

Sprecher:
Die Bundesregierung will seit längerem Cyber-Fähigkeiten aufbauen. Der sogenannte Hackback für die zivilen Sicherheitsbehörden ist nur ein Baustein: Im Jahr 2017 gründete die Bundeswehr das Kommando Cyber- und Informationsraum, das auch Cyberoperationen durchführen soll.

Im selben Jahr wurde die Zentrale Stelle für Informationstechnik im Sicherheitsbereich eingerichtet, die sozusagen als Hacking-Behörde Bundeswehr, Nachrichtendiensten und Polizei zuarbeitet.

O-Ton19 Felgentreu:
Der Grundgedanke ist: Wie können wir eine Verteidigungsfähigkeit im Cyberraum aufbauen. Das ist ja unser großes Problem, dass über den Cyberraum auf einmal Bedrohungen entstanden sind, die die Schwelle eines normalen Hacker-Angriffs überschreiten können, sodass sie die Qualität eines militärischen Angriffs bekommen.

Sprecher:
Fritz Felgentreu, der verteidigungspolitische Sprecher der SPD-Bundestagsfraktion.

O-Ton 20 Felgentreu:
Dass man überhaupt mal guckt, was technisch möglich ist, ist einfach nur die gebotene Vorsicht. Das find ich auch legitim.

Sprecher:
Auch die Grundlagenforschung wird gestärkt. Dieses Jahr wird die Agentur für Innovation in der Cybersicherheit ihre Arbeit aufnehmen. Sie soll sich unter anderem mit Verschlüsselungsverfahren, Künstlicher Intelligenz und Quantencomputern beschäftigen – auch für die „gezielte militärische Verwendung“, wie die Bundesregierung auf eine parlamentarische Anfrage hin mitteilte.

O-Ton 21 Felgentreu:
Die Cyberagentur wird Forschungsprojekte, die es an Universitäten gibt, möglicherweise auch in Kooperation mit der Wirtschaft bewerten, und dann entscheiden, ob sie die für förderungswürdig halten oder nicht. Also ob man das gebrauchen kann, was daraus hervor geht, und zwar im Sinne der Sicherheit.

O-Ton 22 Schulze:
Klar, da werden Realitäten geschaffen, und das heißt auch, dass man offensiver tätig sein will.

Sprecher:
So die Einschätzung von Matthias Schulze. Er ist bei der regierungsnahen Stiftung Wissenschaft und Politik in der Forschungsgruppe Sicherheitspolitik tätig und beschäftigt sich, wie er sagt, „mit der dunklen Seite der Digitalisierung“.

O-Ton 23 Schulze:
Ich bin nicht grundsätzlich gegen *Hackbacks*, ich bin gegen den leichtfertigen Einsatz davon. Wir bauen Offensiv-Fähigkeiten auf, haben aber keine Strategie, wie wir damit umgehen wollen. Denn es ist zu erwarten, wenn man sich so ein bisschen die Interaktion von Cybermächten anguckt, dass da getestet werden wird, was wir da tun. Also offensive Akteure werden testen, wie es mit unserem politischen Willen bestellt ist, diese Fähigkeiten auch zu benutzen.

Sprecher:
Echte Internet-Sabotage gibt es bisher kaum. Der wichtige Teil des Cyberkrieges findet unbemerkt statt: Die Akteure versuchen, sich heimlich Zugang zu den Netzen ihrer Konkurrenten zu verschaffen und dort Programmcodes zu positionieren. Diese Hintertüren benötigen sie, um bei Bedarf zugreifen – oder abschalten – zu können.

Im Jargon der Militärs wird das Platzieren von *backdoors* „Position beziehen“ beziehungsweise „das Schlachtfeld vorbereiten“ genannt. Das Ausforschen der Netzwerke übernehmen Nachrichtendienste, die eng mit militärischen Einheiten zusammenarbeiten.

O-Ton 24 Schulze:
Komplexe Cyberangriffe brauchen Ressourcen, brauchen Zeit, brauchen Knowhow, sind enorm zeitaufwändig. Also das ist nicht Lichtgeschwindigkeit Hin- und Hergeschieße von Datenpaketen, sondern das ist das Vorbereiten eines Einbruchs.

Sprecher:
Der *Cyberwar*, erklärt Matthias Schulze, gehorcht ganz anderen Regeln als ein konventioneller Krieg.

O-Ton 25 Schulze:
Auf der technischen Ebene ist das Problem, dass Spuren gefälscht werden können, und das ist Tagesgeschäft, dass gute Angreifer so tun, als wären sie jemand anders. Angreifer verwenden auch die Angriffs-Tools ihrer Konkurrenten. Die Nordkoreaner haben das amerikanische *Exploit-Tool Eternal Blue* benutzt. Und das ist auch Standardverhalten, dass die Angreifer die *Tools* von ihren Konkurrenten benutzen.

Sprecher:
Wissen ist Macht, heißt es oft. Im Bereich der Computersicherheit trifft das *nicht* zu. Dort zählt nur der *Wissensvorsprung*: Wissen, über das andere noch nicht verfügen. Daher wird die Kenntnis von Schwachstellen und digitalen Hintertüren sorgsam gehütet und geheim gehalten.

Aber solche Kenntnisse wandern, von Kriminellen zu Nachrichtendiensten und zurück. Schließlich wird der einstige Wissensvorsprung zum Allgemeingut.
Denn wer eine Software-Infiltration bemerkt, kann sie analysieren, den Programmcode kopieren, vielleicht verändern und dann selbst einsetzen.

So verbreitete sich *Eternal Blue,* eine Eigenentwicklung des amerikanischen Nachrichtendienstes NSA, zunächst zu den Nordkoreanern, dann zu Russen und Chinesen. Mittlerweile ist das Programm übers Internet leicht zugänglich und wurde möglicherweise auch bei dem Cyberangriff auf die Universität Gießen benutzt.

Die Moral der Geschichte von *Eternal Blue*: Ein Cyberangriff steigert die Angriffsmöglichkeiten des *Gegners*. Umgekehrt kann dieser Gegner *entwaffnet* werden, wenn ein Cyberkrieger sich selbst entwaffnet – das heißt: seinen Wissensvorsprung preisgibt und so den Software-Herstellern ermöglicht, eine Sicherheitslücke zu schließen.

(Musik: Kreuzblende mit O-Ton)

O-Ton 26 Pence:
Resilience though isn‘t enough. We also must be prepared to respond …

(O-Ton: unter Sprecher)

Sprecher:
US-Vizepräsident Mike Pence hielt vor anderthalb Jahren eine Rede über die amerikanische Cyber-Strategie.

O-Ton 26 Pence:
Our administration has taken action to elevate the United States Cyber Command to a combatant command …

Sprecher 2 (Voice-Over 26):
Unsere Regierung hat begonnen, das Cyber-Kommando der Vereinigten Staaten mit den anderen Teilstreitkräften gleichzustellen. Die Zeiten, in denen unsere Gegner uns ungestraft mit Cyberattacken angreifen konnten, sind vorbei. Unser Ziel bleibt: amerikanische Sicherheitsbehörden werden in der digitalen Welt genauso dominant sein wie in der physischen.

O-Ton 26 Pence:
… American security will be as dominant in the digital world as we are in the physical world.

(Applaus unter Sprecher ausblenden)

Sprecher:
Seit drei Jahren verfolgt die amerikanische Regierung eine neue Cyberstrategie, erklärt Matthias Schulze von der Stiftung Wissenschaft und Politik.

O-Ton 27 Schulze:
Das ist eine sehr aggressive, offensive Cyberdoktrin. Im Gegensatz zu den westeuropäischen Doktrinen, die eher defensiv und auf Verteidigung ausgelegt sind, argumentieren die Amerikaner: Okay, Abschreckung funktioniert im digitalen Raum sowieso nicht. Deswegen versuchen wir das ganze operativ zu lösen, indem wir die Angreifer des Gegners permanent binden, weil wir sie damit beschäftigen, unsere eigenen Cyberangriffe abwehren zu müssen.

Sprecher:
In dem entsprechenden Strategiepapier des Verteidigungsministeriums wird dieser Ansatz mit *persistent engagement* und *defending forward* beschrieben: „Dauerhafte Konfrontation“ und „Vorwärtsverteidigung“.

O-Ton 28 Schulze:
Das heißt, das findet nicht mehr nur im eigenen Netzwerk statt, sondern auch im Netzwerk des Gegners und auch in alliierten Netzwerken.

Kann also durchaus sein, dass amerikanische *Cyber-Command-Hacker* in deutschen oder europäischen Netzwerken *defend forward* spielen und mit russischen oder iranischen Hackern interagieren.

Sprecher:
Sind amerikanische Hacker in deutschen Computer-Netzwerken aktiv? Platzieren sie hier womöglich digitale Hintertüren? Andreas Könen, im Bundesinnenministerium zuständig für Cybersicherheit, mag das nicht glauben:

O-Ton 29 Könen:
Schadsoftware in deutschen Systemen ist sicher eine unakzeptable Sache, egal von wem sie implementiert wird oder woher sie kommt. Ich sehe keinen Punkt, wo so etwas von unseren amerikanischen Freunden auch nur verlangt oder auch nur intendiert würde.

(Musikakzent, Kreuzblende)

***Atmo / Internet Governance Forum /** unter Sprecher*

Sprecher:
Eine Sicherheitskontrolle wie am Flughafen. Die Besucher werden abgetastet, Taschen durchsucht. Neben dem Sicherheitspersonal in schwarzen Anzügen und Knopfkopfhörern im Ohr stehen zwei Soldaten in der Uniform der Vereinten Nationen. Das *Internet Governance Forum* wird von der UNO mit veranstaltet.

O-Ton 30 Eröffnung Internet Governance Forum Moderatorin:
„I am now handing over the stage to Her Excellency, the Chancellor of the Federal Republic of Germany, Dr. Angela Merkel …

Atmo: (Applaus)

Sprecher:
Auf dem *Internet Governance Forum* treffen sich Delegierte aus aller Welt und debattieren über Regeln für den weltweiten Datenaustausch. 2019 fand es in Deutschland statt, und Angela Merkel hielt die Eröffnungsrede.

O-Ton 31 Eröffnung Internet Governance Forum (Merkel):
One world, one net, one vision. Das diesjährige Leitmotiv bringt auf den Punkt, worum es geht. Nämlich darum, ein gemeinsames Verständnis zu fördern, wie die Zukunft des Internets aussehen soll. Der Angriff auf die Internetkonnektivität ist zu einem gefährlichen Instrument der Politik geworden.

Sprecher:
Mit dabei war auch der Kommunikationswissenschaftler Wolfgang Kleinwächter, der sich seit langem mit digitalem Recht und Cybersicherheit beschäftigt.

O-Ton 32 Kleinwächter:
Also neue Angriffswaffen werden produziert, die dann die Entwicklung neuer Verteidigungswaffen auslösen, und wir haben so etwas wie ein Wettrüsten im *Cyberspace*. Das Problematische ist, dass es sich um schwierig zu identifizierende Waffen handelt. Also einen Panzer oder eine Kalaschnikow oder ein Flugzeug können sie leichter identifizieren als einen Computer-Virus, der vor einem Jahr irgendwo in einem Kraftwerk deponiert worden ist und dann durch einen bestimmten Befehl aktiviert wird und dann erheblichen Schaden anrichten kann.

Sprecher:
Wolfgang Kleinwächter war lange im Vorstand der ICANN tätig, die internationale Internetverwaltung, die unter anderem die Verteilung der Web-Adressen organisiert. Er beklagt, dass staatliche Cyberoperationen in einem völkerrechtlichen Graubereich stattfinden. Als Beispiel nennt er eine Aktion des amerikanischen Cyber-Kommandos gegen eine russische Einheit, die angeblich Internetpropaganda in den Vereinigten Staaten verbreitete.

O-Ton 33 Kleinwächter:
Manchmal wollen sie zeigen, was sie können, um auch abschreckend zu wirken. Zum Beispiel hat eben die *Cyber Command* in den USA acht Wochen nach ihrem Angriff auf die sogenannte Trollfabrik in St. Petersburg das veröffentlicht, was sie da gemacht hat. Und sie haben eben gesagt:
Wir haben das und das gemacht, und eine Reihe von Tagen haben die Server in St. Petersburg nicht funktioniert. Das war ein klares Signal: Wir können das, wenn wir das wollen. So etwas triggert natürlich häufig bei der anderen Seite: Wir müssen das auch entwickeln.

Sprecher:
Mit großem Aufwand versuchen die Vereinigten Staaten, ihren Vorsprung im Cyberbereich zu halten. Experten zählen China und Russland zu den Cybergroßmächten. Nun wollen aber immer mehr Mittelmächte – wie Deutschland, Polen, Indien, Österreich oder Mexiko – offensive Cyber-Fähigkeiten entwickeln.

Im Vergleich zu anderen Rüstungsgütern sind diese billig. Im Nahen Osten loten die Konfliktparteien Iran, Saudi-Arabien und Israel gegenwärtig die Möglichkeiten der Cyber-Sabotage aus. Cyberangriffe werden zu einem Instrument der Geopolitik.

Die Lage wird zunehmend unübersichtlich. Bestätigt Chris Painter, zwischen 2011 und 2017 der oberste Beamte der amerikanischen Regierung für „Cyberangelegenheiten“. Heute ist er im diplomatischen Dienst tätig.

O-Ton 34 Painter:
Look, every country in the world that can – and really every country – is trying to develop cyber-operation capabilities...

Sprecher 2 (Voice-Over 34):
Alle Länder, die dazu in der Lage sind, versuchen Fähigkeiten für Cyberoperationen aufzubauen, ob nun defensiv oder offensiv. Cyberoperationen gehören einfach zur heutigen Wirklichkeit.

Aber andererseits müssen wir dafür sorgen, dass Regeln und Richtlinien existieren. Denn es kann sehr destabilisierend wirken, wenn jedes Land über solche Möglichkeiten verfügt und niemand weiß, wann und auf welche Art sie eingesetzt werden.

O-Ton 34 Painter:
… if everyone has these capabilities and you don't know when and how to use them.

Sprecher:
Wolfgang Kleinwächter und Chris Painter gehörten zu einer Arbeitsgruppe der Vereinigten Nationen, der „Globalen Kommission für die Stabilität im Cyberspace."

O-Ton 35 Painter:
I worry about proliferation of offensive capabilities...

Sprecher 2 (Voice-Over 35):
Mir macht die Verbreitung von offensiven Fähigkeiten Sorgen. Ich bin Realist genug, um zu wissen, dass das passieren wird. Wir brauchen Regeln. Wir müssen darüber reden, wie wir deeskalieren können. Wir brauchen Kommunikationskanäle wie den heißen Draht im Kalten Krieg und zwischenstaatliche Gespräche, das ist wirklich wichtig.

O-Ton 35 Painter:
… having hot lines and discussions between countries, that is really important.

O-Ton 36 Kleinwächter:
Solche roten Telefone sind dabei, im Cyberspace eine Wiedergeburt zu feiern. Wenn was passiert, dass man weiß, wen kann man anrufen. Das rote Telefon: „Greift ihr uns jetzt an, ja oder nein?"

Sprecher:
Kann der *Cyberwar v*ölkerrechtlichen Regeln unterworfen werden? Viele Experten fordern vertrauensbildende Maßnahmen, auch eine stärkere internationale Zusammenarbeit für mehr Cybersicherheit und den Verzicht auf eigene Hacking-Aktionen. Sie wollen *Cyberpeace* statt *Cyberwar!*

Aber die Verhandlungen bei den Vereinten Nationen stagnieren. Im gegenwärtigen Klima zwischen den Großmächten ist an eine informationstechnische Abrüstung nicht zu denken.

Sprecher:
Wie soll sich Deutschland wappnen für den Cyberkrieg? Der Verteidigungspolitiker Fritz Felgentreu von der SPD findet, die Bundesrepublik müsse auch in diesem militärischen Bereich „auf eigenen Füßen stehen".

O-Ton 37 Felgentreu:
Es wird Zeit, dass wir da eben Strukturen schaffen, die die entsprechenden Fortschritte möglich machen.

Wenn wir da etwas uns aufbauen können, dann ist das ein Fortschritt. Und es macht uns auch beim Verhandeln mit Partnern darüber wie wir es gemeinsam machen, stärker.

Sprecher:
Ganz anders sieht das Anke Domscheit-Berg von den Linken. Sie plädiert dafür, auf strikt zivile IT-Sicherheit zu setzen.

O-Ton 38 Domscheit-Berg:
Wir kommen da eigentlich nur raus, wenn wir uns ganz streng und zu hundert Prozent ausschließlich auf die Selbstverteidigung fokussieren. Dass wir zum Beispiel auch eine Meldepflicht für Sicherheitslücken haben, denn je weniger Sicherheitslücken im Umlauf sind, umso weniger können sie ausgenutzt werden. Von Verbrechern, von Geheimdiensten, auch von militärischen Anwendern. Also je weniger Schlupflöcher da sind, umso sicherer ist das Gesamtsystem.

Sprecher:
Klar ist: Das Internet wird immer stärker zum militärischen Aufmarschgebiet, neben Land, Luft und Wasser ist ein weiteres Schlachtfeld eröffnet: das digitale. Informationstechnik ist zu einem Spielball in der internationalen Machtpolitik geworden. Mit unabsehbaren Folgen warnt Wolfgang Kleinwächter:

O-Ton 39 Kleinwächter:
Das ist eine sehr riskante Entwicklung, mit der viel Schaden angerichtet werden kann, und die Weltgemeinschaft ist sich über diese Gefahren nach meiner Ansicht noch viel zu wenig bewusst.

* * * * *