Es handelt sich um ein Transkript der Veranstaltung "Lunch Briefing: Internationale Verhandlungen zu Cyber-Normen" mit Tim Maurer und Stefan Heumann vom 15.12.2017 in der Stiftung Neue Verantwortung. Der Text wurde zur besseren Lesbarkeit bearbeitet. Es gilt das gesprochene Wort.

-Beginn des Transkripts-

Stefan Heumann: Herzlich willkommen in der Stiftung Neue Verantwortung. Mein Name ist Stefan Heumann. Ich bin Mitglied im Vorstand hier bei der Stiftung Neue Verantwortung. Wir wollen das recht informell gestalten heute, also greifen Sie ruhig zu und essen Sie dabei Ihr Mittag. Wir haben Tim Maurer zu Gast, stelle ich gleich vor, und freuen uns, dass Sie alle in die SNV gekommen sind.

Wir beschäftigen uns bei der Stiftung Neue Verantwortung mit den Herausforderungen des technologischen Wandels, von Arbeit über digitale Infrastruktur bis über die Transformation unserer Medienlandschaft. Ein wichtiges Thema ist natürlich auch Sicherheit, insbesondere bei digitalen Technologien. Die Entwicklung des Internets hat mittlerweile eine riesige Auswirkung auch auf die Sicherheitspolitik und steht daher auch zunehmend im Fokus von Sicherheitsbehörden, auch von Militärs. Das wirft wichtige Fragen für die deutsche, für die nationale Sicherheitspolitik auf, aber auch ganz wichtige Fragen für die internationale Sicherheitspolitik.

Und ich freue mich ganz besonders, dass ich mit Tim Maurer einen absoluten Topexperten an der Schnittstelle von Digitalisierung oder, wie die Sicherheitsexperten sagen würden, dem Cyberraum und internationaler Politik hier zu Gast habe. Und Tim beschäftigt sich wirklich schon seit Jahren, seit vielen Jahren mit dieser Schnittstelle. Er hat sich sehr lange mit Themen von Internet Governance befasst, dann auch zunehmend mit Themen der Cybersicherheit. Er war Experte in ganz vielen internationalen Gremien, an denen er mitgewirkt hat. Die will ich gar nicht alle aufzählen. In den letzten Jahren hat er vor allem beim Carnegie Endowment for International Peace gewirkt und dort auch das Cyberprogramm aufgebaut und leitet es mit als Co-Direktor. Wir freuen uns ganz besonders, dass du heute hier bei uns bist, Tim, und dass du dir die Zeit genommen hast, mit uns über das Thema internationale Cybernormen zu sprechen, über die Frage, wie das Internet zunehmend auch zu einem Raum von Konflikten geworden ist, nicht nur Konflikten in sozialen Medien, die wir untereinander austragen, sondern auch wirklich in einem Raum von Konflikten zwischen Staaten und Ländern. Und würde auch direkt gleich einsteigen mit dir in die Diskussion.

Zum Ablauf: Ich würde die Veranstaltung damit beginnen, Tim einige Fragen zu stellen, um so in das Thema reinzukommen und schon mal ein paar wichtige, zentrale Fragestellungen aufzuwerfen. Und dann würde ich es auch gerne öffnen – wir haben hier auch viel Expertise im Publikum sitzen – für Kommentare, für weitere Fragen auch von Ihnen, sodass wir dann auch in ein breiteres Gespräch hier in der Gruppe übergehen können im Laufe dieses Mittags.

Internet oder Cyberraum, wie die Sicherheitsexperten sagen, wird immer wichtiger. Also das kann man auch schön in Deutschland sehen; hier in Deutschland hat die Deutsche Bundeswehr dieses Jahr auch ein Cyberkommando eingerichtet. Gerade in den letzten Tagen ging über den Ticker, dass die Nato jetzt auch offensive Cyberfähigkeiten entwickeln will. Es wird in den USA viel über den Einfluss von Russland auf die US-Wahl gesprochen und über Cyberoperationen, die auch in dem Kontext durchgeführt worden sind. Es gab in den vergangenen Jahren auch viel Berichterstattung in den Medien, zum Beispiel den ersten bekanntgewordenen Einsatz von Cyberwaffen, könnte man schon fast sagen, wenn man Stuxxnet als eine Cyberoperation versteht, wo eine Cyberwaffe zum Einsatz gekommen ist. Du beschäftigst dich schon seit vielen Jahren mit diesem Thema und ich würde gerne von dir noch einmal hören, wie du in dieses Themenfeld gekommen bist und warum es aus deiner Sicht so wichtig ist, dass wir Regeln finden für staatliches Verhalten im Cyberraum.

Tim Maurer: Ja. Erst mal Danke an dich, Stefan, und an SNV, dass ich heute hier sein darf, und an alle, an Sie, dass Sie sich die Zeit genommen haben, heute zum Mittagessen hierher zu kommen. Ich freue mich immer, wenn ich in Deutschland bin. Ich bin jetzt seit fast zehn Jahren in den USA und schaffe es aber trotzdem oder bin immer mal wieder hierher, zwei-/dreimal im Jahr.

Ich bin 2010 in das Thema mehr oder weniger reingeschlittert und das war ursprünglich durch ein Forschungsprojekt, das versucht hat, die IT-Experten vom MIT mit den nationalen Sicherheitsexperten der Harvard Kennedy School und den Anwälten der Harvard Law School zusammenzubringen. Das war ursprünglich vom Pentagon finanziert mit dem Ziel, verschiedene akademische Disziplinen zusammenzuführen, um sich mit dem Thema internationale Cybersicherheit auseinanderzusetzen. Ich glaube, das war teilweise motiviert dadurch, dass das Verteidigungsministerium, glaube ich, mehr Zugang zu verschiedenen Daten hatte und deswegen das Thema früh als eine Priorität identifiziert hatte und gemerkt hat, dass in den Universitäten zu dem Thema ganz wenig passiert ist. Und daraus ist eine Gruppe entstanden mit unter anderem Joseph Nye und anderen, die sich wirklich mit diesem Thema aufgrund teilweise auch dieser Initiative befasst haben.

Das war 2010. Das war zu Beginn der Debatte, ob Cyberwar überhaupt existiert oder nicht. Und diese Debatte hat uns wirklich, glaube ich, drei, vier Jahre beschäftigt mit dem Buch, das dann Thomas Rid auch als Antwort geschrieben hat. Und wenn wir jetzt uns anschauen, sieben Jahre sind vergangen und die Diskussion, die wir jetzt haben, und die Tatsache, dass wir jetzt hier in einem vollen Raum sitzen, zeigt, wie schnell sich das Thema in den letzten sieben Jahren entwickelt hat. Und diese Debatte damals war wirklich so der Anfang, das einer breiteren Öffentlichkeit zugänglich zu machen und jetzt sind wir in einem ganz anderen Terrain, wo gerade mit den Wahlen in den USA im vergangenen Jahr das jetzt wirklich auf oberster Ebene diskutiert wurde.

Bei Carnegie, wo ich jetzt seit zwei Jahren bin, beschäftigen wir uns vor allem mit Fragen, wie man in diesem Feld, wo sich zunehmend Staaten mit den offensiven

Möglichkeiten auseinandersetzen, ob es da Möglichkeiten gibt, das zu beschränken. James Clapper hat, bevor er aus der Regierung ausgeschieden ist vor ein paar Monaten, gesagt, dass mittlerweile…

Stefan Heumann: Vielleicht sagst du noch kurz, wer James Clapper ist.

Tim Maurer: Ach so. Ehemaliger Direktor des Office of National Intelligence der USA. Der wies darauf hin, dass wir über dreißig Staaten haben, die offensive Möglichkeiten direkt verfolgen. 2010 waren wir vielleicht bei sechs, sieben Staaten, also Russland, China, die USA, Israel, Großbritannien, Frankreich. Deutschland hat jetzt mit Cyber begonnen, das gehört, glaube ich, eher zu den dreißig plus. Das heißt, wir sehen innerhalb der letzten sieben Jahre mit Blick auf die Proliferation nicht nur der Malware sondern auch der Staaten, die ein aktives Interesse haben, eine rasante Entwicklung. Und wir überlegen uns, gibt es da Möglichkeiten, wo es trotz der großen Unterschiede zwischen den Staaten, wie sie über dieses Thema nachdenken, trotzdem Gemeinsamkeiten, wo man langsam anfangen kann, gemeinsames Regelwerk zu finden. Das Auswärtige Amt hatte da in den vergangenen achtzehn Monaten eine Federführung gerade bei den Vereinten Nationen aber auch in der UN Group of Governmental Experts. Und da werde ich nicht darüber sprechen, sondern werde dann an die Kollegen im Raum entsprechend verweisen.

Stefan Heumann: Da kommen wir auch gleich noch dazu. Bevor wir auch über die Diskussionen im UN-Kontext reden, wäre es vielleicht auch noch mal ganz gut, darüber zu sprechen, was die Frage von Proliferation und Cyberwaffen so kompliziert und komplex macht. Es gibt ja auch, und damit hat sich ja auch Carnegie auch schon lange beschäftigt, das Problem der Rüstungskontrolle, der Aufrüstung an Staaten, konventionelle Waffen. Was macht es so besonders schwierig, Regulierungen und Absprachen zu finden, wie man mit Cyberwaffen umgehen soll? Vielleicht erklärst du noch mal kurz, wie eigentlich eine Cyberwaffe zu verstehen ist, was da eigentlich dahinter steckt und was auch deiner Sicht auch ein entscheidender Unterschied zu Panzern oder Mittelstreckenraketen oder Atomwaffen ist.

Tim Maurer: Ja, also zum ersten Mal ist der Kostenunterschied ja riesig. Wenn wir uns einfach anschauen, was eine Cyberoperation kostet, dann sind wir ja im sechsstelligen, im siebenstelligen Bereich, immer noch im sehr niedrigen siebenstelligen Bereich. Wenn man das mit konventionellen Waffen vergleicht, ist das ein riesen Unterschied.

Stefan Heumann: Warum ist das so? Warum ist das so günstig, Cyberoperationen durchzuführen?

Tim Maurer: Weil es letzten Endes nur darum geht oder ‚nur' darum geht, ob man das Wissen hat und die Expertise, die Software zu schreiben und den Code zu schreiben und ob man das Wissen hat, wie ein bestimmtes System funktioniert, das, wenn man es einmal gehackt hat, in der Lage ist, bestimmte Effekte zu erreichen. Das heißt, es geht weniger darum, wie viel Stahl man hat oder ob man Zugang zu Uranium hat, sondern es geht vielmehr darum, ob man wirklich die Leute hat, die

das Know-how haben, um das entsprechend durchzuführen.

Ein kleiner Zusatz dazu ist, wenn es um Supply Chain Integrity geht. Und ich muss mich entschuldigen, weil manchmal gibt es Wörter, die ich im deutschen nicht entsprechend übersetzen kann, weil ich in Deutsch wenig arbeite, aber Supply Chain Integrity.

Stefan Heumann: Die Integrität von Wertschöpfungsketten.

Tim Maurer: Wertschöpfungskette, danke. Da gibt es einen klaren Unterschied, dass einige Staaten einfach Möglichkeiten haben, über die Wertschöpfungskette auch Schwachstellen einzubauen, die andere Staaten nicht haben. Das ist dann schon mal kostenintensiver. Aber wenn es jetzt um beispielsweise WannaCry geht, die Malware, die Anfang des Jahres Schlagzeilen gemacht hat und unter anderem Krankenhäuser in Großbritannien in Mitleidenschaft gezogen hat, sodass Systeme nicht verfügbar waren und die Krankenhäuser tatsächlich Patienten abweisen mussten, da ist die Vermutung, dass es ein Akteur war, der nicht besonders gut ist und diese Malware eingesetzt hat, ohne zu wissen, dass es wirklich zu so einem großflächigen Effekt kommen könnte. Also von daher ist es sehr günstig. Es kommt auf Leute an, die wissen, was Sie tun und weniger darauf, wie viel Material man hat. Und wenn wir auf die diplomatische Ebene schauen, ist das Problem, da Fortschritte zu machen mit Blick auf Abrüstungsverhandlungen, dass wir, selbst wenn es um Definitionen geht, ganz andere Definitionen verwenden.

Russland hat Ende der 90er Jahre einen Vorschlag für ein internationales Abkommen zur Cybersicherheit gemacht und benutzt nicht den Begriff Cybersicherheit, sondern Informationssicherheit und definiert Cybersicherheit nicht, wie wir das hier tun, vor allem als Hacking oder als technische Frage, sondern beinhaltet eine größere Definition, die auch Inhalte beinhaltet. Also das heißt, Moskau versucht, über diese Debatte zur Informationssicherheit auch die Kontrolle über die Medien und Kontrolle über Informationen voranzutreiben. Die Chinesen tun das genauso.

Letzte Woche kam ein Bericht raus, dass Moskau Washington den Vorschlag unterbreitet hat, dass es ein Abkommen geben soll zwischen Washington und Moskau, das nicht jeweils in dem gegenseitigen Territorium eingreift über Informations- und Kommunikationsmittel. Das Problem ist, es ist unklar, was man mit so einem Abkommen wirklich meint: Aus amerikanischer Sicht würde es bedeuten, dass wir sicherstellen wollen, dass die Russen nicht noch einmal versuchen, die Wahlen zu manipulieren und zu hacken. Aus russischer Sicht heißt das unter Umständen, dass beispielsweise Secretary Clinton keine Kommentare machen soll, wenn es auf einmal russischkritische Kommentare von russischen Bürgern gibt, die einen Protest gegen Wladimir Putin in Moskau organisieren. Und dadurch, dass es diese grundsätzlichen Interessenunterschiede gibt, ist es schwer, auf internationaler Ebene da wirklich Fortschritte zu machen.

Stefan Heumann: Ich will noch aber auf einen anderen Punkt hinaus, der es aus meiner Sicht auch sehr komplex macht, zu Fortschritten zu kommen und Einigkeit

zwischen den Staaten und da kann ich auch geschickt noch einen Werbeblock für dein Buch einschieben, weil du kommst ja nächstes Jahr mit einem Buch raus und hast dich sehr stark damit befasst, wie Staaten eigentlich diese Kapazitäten entwickeln für Cyberoperationen und dass sie dabei oftmals mit nichtstaatlichen Akteuren zusammenarbeiten. Das ist ja auch das, was man öfters in der Zeitung liest. Da wird ja nicht gesagt, Russland hat die demokratische Partei gehackt, sondern es waren Russland, dem russischen Geheimdienst nahestehende Gruppen oder so und das liest man ja immer wieder auch im Kontext, wenn der Iran genannt wird. Das ist dann nicht der iranische Staat, sondern es sind irgendwelche unabhängigen oder nicht ganz so unabhängigen Hackergruppen. Kannst du dazu etwas sagen, was du, glaube ich, als Proxys bezeichnest, die es auch noch mal schwieriger machen, zu verstehen, wie Staaten dort agieren und die sicherlich auch noch mal verkomplizieren, staatliches Verhalten in diesem Bereich zu definieren und auch Regelungen zu finden?

Tim Maurer: Ja und das war wirklich spannend. Also ich habe vor vier Jahren angefangen, dieses Buch zu schreiben. Wie viele von Ihnen würden sich als Hacker oder der Technical Community zugehörig fühlen? Gut, keiner vom CCC. Ja, gut. Weil einer der Gründe, warum ich mich entschieden habe, das Buch zu Proxy-Akteuren zu schreiben, war, wenn ich mich mit Leuten, die dem CCC nahestehen oder einfach der Hackercommunity angehören oder auch mich mit Leuten in den Strafverfolgungsbehörden unterhalten habe, wurde sehr schnell klar, dass vor allem die technischen Leute darauf hingewiesen haben, dass es in diesem Raum nicht nur um staatliche Akteure geht, sondern dass auch nichtstaatliche Akteure durchaus einfach Kapazitäten haben, die aus nationalen Sicherheitsinteressen bedenklich sind, weil es eben so kostengünstig ist und weil es wirklich darauf ankommt, ob man jemanden hat, der weiß, wie man so etwas umsetzen muss. Und vor vier Jahren waren wir noch mitten in dieser Cyberwar-Debatte und ob es Cyberkrieg gibt oder nicht und das war extrem staatenzentriert, sodass ich angefangen habe, dieses Buch zu schreiben, teilweise mit dem Gedanken, mir anzuschauen, was für Kapazitäten nichtstaatliche Akteure haben. Und ich wollte mir dann auch spezifisch anschauen, wie Staaten diese nichtstaatlichen Akteure nutzen, um ihre Macht auszuüben. Iran ist ein super Beispiel.

Als Teil meiner Recherchen und dann im vergangenen Jahr hat die amerikanische Regierung auch ein Indictment veröffentlicht, also einen Strafbefehl. Wo darauf hingewiesen wurde, dass 2012/2013 mehrere amerikanische Großbanken von massiven DDoS-Attacken getroffen wurden. Die DDoS-Attacken waren so hoch, dass die Großbanken selbst an die Grenzen gestoßen sind von dem, was sie im Rahmen ihrer IT-Sicherheit leisten konnten. Und das sind mit die größten Finanzinstitute weltweit, das heißt, die investieren wirklich Millionen in ihre IT-Sicherheit. Sie haben sich an das Weiße Haus gewendet, unter anderem, um besser geschützt zu sein. Und was jetzt herausgekommen ist, ist, dass man die vier Leute, die über diesen Strafbefehl öffentlich gemacht worden sind, die Namen, das sind vier Leute in ihren Mitzwanzigern. Und ich habe mir dann mal angeschaut, was ich denn so über das Internet über die Leute herausfinden kann und habe dann festgestellt, dass deren Pseudonyme, die sie verwandt haben, zwei Jahre vor der DDoS-Attacke, die sich an

amerikanische Finanzinstitute gerichtet hatte, dass sich diese Leute über ihre Web Defacements gebrüstet haben. Also Web Defacements ist, wenn man eine Website hackt und dann statt jetzt irgendwie der Seite der SNV auf einmal steht da irgendwie ‚Kauf bei uns'. Auf jeden Fall machen das viele politische Hacktivisten, die dann ihre politische Nachricht auf solchen Webseiten hinterlassen wollen. Und diese vier Leute haben das wirklich von 2010 bis 2012 auf einer Website für Hacker öffentlich hinterlegt und sich gebrüstet, wie viele von amerikanischen Regierungswebseiten sie in der Lage waren, zu übernehmen. Und dann 2012 verschwinden die auf einmal.

Nach 2012 findet man auf dieser Website Zone-H, die aus Estland betrieben wird von einem Italiener, keine Nachweise mehr, dass diese Hacktivisten sich öffentlich brüsten, dass sie da Webseiten auf einmal übernommen haben. Und das ist zufällig die Zeit, wo laut dem Strafbefehl des amerikanischen Justizministeriums diese vier Leute angefangen haben, sich mit drei weiteren Leuten zusammenzutun, die der Iranischen Revolutionsgarde angehören und dann diese massive DDoS-Attacke gegenüber Finanzinstituten durchgeführt haben. Das Spannende daran ist, dass dieser Mechanismus, dass Teheran sich nichtstaatlicher Akteure bedient, um Macht umzusetzen, nicht notwendigerweise neu ist. Wenn man sich anschaut die Geschichte Ende der 70er Jahre, als die Iraner die Amerikanische Botschaft übernommen haben, war das sehr ähnlich, weil es den Mob gab, der die Botschaft übernommen hat und die Regierung zuerst gesagt hat: „Damit haben wir nichts zu tun." Und dann aber gemerkt hat, das ist im Interesse der Führung und dann letzten Endes diese Aktion der Studenten gutgeheißen hat. Und wir sehen jetzt sehr ähnlich im Cyberbereich ein ähnliches Verhalten, was die iranische Führung an den Tag legt.

Stefan Heumann: Also das sind diese Cyberproxys. Hast du dir außer Iran noch weitere Länder angeschaut, wo man ähnliche Dynamiken feststellen kann? Also Russland würde man wahrscheinlich ähnlich beschreiben. Darüber hatten wir auch schon eine Veranstaltung mit Andrei Soldatow, der auch beschrieben hat, wie der russische Staat zum Teil auch Kriminelle, Cyberkriminelle zwingt, mit ihnen zusammenzuarbeiten, weil er ihnen Strafverfolgung androht, um sie zur Kooperation zu nötigen. Gibt es noch weitere Beispiele, mit denen du dich beschäftigt hast?

Tim Maurer: Ja, ich habe mir Russland als Fallstudie angeschaut, private Sicherheitsunternehmen in den USA und inwieweit die amerikanische Regierung Unternehmen benutzt und habe mir dann auch angeschaut, welche Entwicklung es in China gab und wie Peking über die letzten zwanzig Jahre sehr viel stärker versucht hat, Kontrolle über diese nichtstaatlichen Akteure durchzuführen.

In Russland ist spannend, ich war 2015 in Kiew in der Ukraine, weil mich interessiert hat, inwieweit im Rahmen des politischen Konflikts kriminelle Akteure politisiert worden waren und sich unter anderem für eine Seite entschieden haben und mir wurde in Gesprächen von Leuten dort gesagt, dass es tatsächlich aufgrund der russischen Regierung, die versucht Einfluss auf Hacker zu nehmen, Migrationswellen gibt. Dass russische Hacker beispielsweise nach Südostasien ziehen, weil sie nicht wollen, dass der FSB irgendwann an der Tür klingelt und sagt: „So, wir wissen, was du die letzten zwei Jahre gemacht hast, du kannst jetzt entweder ins Gefängnis

gehen oder du arbeitest mit uns zusammen.“ Das waren Gespräche, die konnte ich schwer in das Buch einbauen, sodass ich mich gefreut habe, dass dann wiederum ein Jahr später die amerikanische Regierung sehr viel transparenter geworden ist mit ihren Informationen, die sie über andere Quellen bekommen hat und dann über einen weitere Strafbefehl im Falle von Yahoo.

Yahoo wurde ja gehackt zu einem Ausmaße, dass der Deal, der mit Yahoo geschlossen wurde, wieder neu verhandelt werden musste und 300 Millionen vom Verkaufspreis reduziert worden waren, weil dieser Hack so ein entscheidendes Ausmaß auf den Wert von Yahoo hatte. Und in diesem Strafbefehl werden zwei FSB-Agenten genannt, die einen russischen Kriminellen benutzt haben, der per Strafbefehl von den Amerikanern gesucht worden war, in einem europäischen Land verhaftet worden ist, aber dann, bevor ihnen der Prozess gemacht werden konnte, es geschafft haben, nach Russland zu fliehen. Und dann, nachdem er nach Russland zurückgekommen war, von dem FSB-Agenten dafür genutzt wurde, Yahoo zu hacken. Und der Deal war, die russischen Strafverfolgungsbehörden werden die Anschuldigung gegen ihn nicht weiter verfolgen. Er hat dafür Yahoo-Konten gehackt und durfte nebenher über die Daten, die er gesammelt hat, Geld machen, über Spamming und andere kriminelle Aktivitäten. Die Yahoo-Konten, die dadurch gewonnen worden sind, waren teilweise nicht genug. Wenn das besonders interessante Personen waren, hatte der russische Geheimdienst ein Interesse daran, auch herauszufinden, ob diese Personen andere E-Mail-Konten benutzt haben, sodass dann dieselben beiden FSB-Agenten eine weitere Person in Kanada, einen 22-jährigen angeworben haben, der dann auf Kommission gearbeitet hat. Dem wurden dann Yahoo-Konten gegeben von den Personen und der Auftrag war dann: „Kannst du herausfinden, ob du auch die anderen Konten von den Personen hacken kannst?“ Und er hat dafür dann entsprechend Geld bekommen. Das ist ein bisschen ein anderes Format als die Iraner, weil es mehr wie das ist, was die Piraten vor 300, 400 Jahren, gemacht haben, die Freibeuter. Im Gegensatz zum Iran, wo das sehr viel politisch motivierter zu sein scheint.

Stefan Heumann: Web Defacements sind natürlich ärgerlich und auch peinlich, wenn dann die Website des amerikanischen Verteidigungsministeriums von Islamisten übernommen wird und es ist natürlich auch ein Problem, wenn E-Mails gehackt werden und sensible Daten erbeutet werden. Aber wir verknüpfen ja mittlerweile auch immer mehr Hardware und Infrastruktur mit dem Netz und machen sie angreifbar. Wir hatten Stuxnet kurz angesprochen, das sich gegen das amerikanische Atomprogramm gerichtet hat und wo am Ende Siemens Maschinen, Zentrifugen angegriffen wurden und auch sabotiert worden sind. Du hast die Ukraine genannt, wo es Angriffe auf das Stromnetz gab. In Deutschland gab es einen Bericht, dass ein Stahlwerk angegriffen wurde. Also sozusagen die Konsequenzen auch von dem, was du beschreibst und beobachtest seit Jahren, die werden größer für uns. Also eigentlich müsste auch dadurch der Druck größer werden, in der Staatengemeinschaft zu sagen: „Hey, Stopp, was machen wir hier eigentlich? Wir vernetzen uns alle immer mehr, wir werden dadurch auch alle immer verwundbarer von dieser Infrastruktur. Können wir nicht uns irgendwie auf so ein paar Grundregeln einigen, dass wir nicht unsere zivile Infrastruktur angreifen, dass nicht

Krankenhäuser ausfallen?“ Und da sind wir ja bei dieser Diskussion, die auch im Rahmen bei der UN geführt worden ist.

Tim Maurer: Ja.

Stefan Heumann: Und da würde mich dann schon noch mal interessieren, was deine Einschätzung dazu ist? Weil diesen Sommer sind die Gespräche ja geendet, ohne ein konkretes Ergebnis, also es gab keinen Abschlussbericht, auf den man sich einigen konnte. Was ist deine Einschätzung, wo man international, aber vor allem auf UN-Ebene, auf der Diskussion, wie das Völkerrecht vielleicht angewendet werden kann, um Regeln zu definieren, wie Staaten sich zu verhalten haben, wo die Diskussion steht und auch deine Analyse, woran es gelegen hat, dass man kein besseres Ergebnis erzielen konnte?

Tim Maurer: Also da hat sich in den letzten Jahren unglaublich viel getan, weil trotz dieser Unterschiede, was Cybersicherheit überhaupt heißt, es trotzdem möglich war, im Rahmen der UNO Konsensberichte zu verabschieden. 2013 war der erste Meilenstein, der erreicht worden war, weil bis 2013 es noch nicht mal eine Übereinstimmung gab, ob existierendes Völkerrecht auf das Internet angewandt werden sollte. Die Chinesen haben sich lange gesträubt, dem zuzustimmen. Das Gegenargument war, das Internet ist etwas ganz Neues, wir können da nicht das existierende Völkerrecht nehmen, wir brauchen etwas Neues. Die Gegenargumentation war, warum nehmen wir nicht das, was wir schon haben, und das Völkerrecht mit Blick auf, wenn wir jetzt in Kriegssituationen sind, lasst uns da anfangen, lasst uns sagen, das besteht auch im Internet und dann finden wir heraus, wo gibt es Lücken. Das hat sich erst 2013 ergeben, dass die Chinesen gesagt haben, okay, das Völkerrecht besteht auch im Internet.

2015 war dann der zweite Meilenstein, wo der Bericht darüber hinaus auch eine Reihe von freiwilligen Normen, Absichtserklärungen verabschiedet hat. Eine sagt beispielsweise, dass sich diese zwanzig Staaten, die Teil dieser Gruppe waren, darüber verständigt haben, dass man in Friedenszeiten keine kritischen Infrastrukturen angreifen würde, die zu einem Ausfall von Funktionen für die Öffentlichkeit führen würden. Das war ein weiterer Schritt, um ein bisschen Klarheit zu schaffen, wie die internationale Staatengemeinschaft darüber nachdenkt, wie sie ihre offensiven Kapazitäten in Zukunft nutzt. Und dann war da die Frage, soll es eine neue Gruppe geben oder nicht? – Das war letztes Jahr die Debatte, weil man 2013 und 2015 so viele Fortschritte gemacht hat.

Die russische Föderation war aber sehr darauf bedacht, eine neue Gruppe ins Leben zu rufen, andere Staaten auch, sodass es eine neue Gruppe gab, die von zwanzig auf fünfundzwanzig Mitglieder erweitert worden ist. Das hat einige Länder irritiert, weil die Sorge war, je breiter man es macht, umso weniger Staaten wird es geben, wo die Experten wirklich wissen, um was es geht, und auch die Leute, die vorher schon Teil dieser Diskussion waren, einfach über mehrere Jahre wissen, um was in der Diskussion geht und man Zeit verliert, wenn man jetzt diesen Kreis erweitert. Andererseits war das Argument: „Ja, aber wenn wir das immer nur unter fünfzehn

oder zwanzig diskutieren, dann fehlt die Legitimität, weil das ist letzten Endes immer noch die UNO und dann werden die anderen Staaten sagen, warum sollen wir dem zustimmen, wenn wir nie wirklich am Tisch saßen."

Und der Prozess ist im Juni auseinandergefallen, trotz der starken Bemühungen gerade von deutscher Seite, die den Vorsitz innehatte. Und einer der Knackpunkte war die Frage zum Völkerrecht, nicht ob es angewandt werden kann, weil 2013 gab es ja die Übereinstimmung, dass es angewendet wird, sondern viel mehr, man wollte konkreter werden. Man wollte eine konkretere Übereinstimmung dazu haben, beispielsweise ob das Recht auf Selbstverteidigung auch im Internet gelten sollte. Und da haben verschiedene Staaten gesagt, das wollen sie so spezifisch nicht in dem Bericht stehen haben. Die kubanische Regierung war da sehr lautstark, aber auch die russische Regierung, die chinesische Regierung hatten Bedenken. Auf der anderen Seite waren die Amerikaner sehr darauf bedacht, den Rahmen dieses Berichts einzuhalten. Es gab Bemühungen, diesen Bericht zu erweitern und von daher war die Interessenskonstellation in den letzten zwei Jahren, glaube ich, so, dass da schon von Anfang an es gewisse Sorgen gab, dass es keinen Bericht geben würde und der ist letzten Endes nicht zustande gekommen. Dass wir jetzt einen neuen Präsidenten im Weißen Haus sitzen haben, dessen Mitarbeiter grundsätzlich solchen multilateralen Behandlungen kritisch gegenüberstehen – und das ist, glaube ich, noch positiv formuliert – hat dem nicht zugetragen.

Stefan Heumann: Ja und zusätzlich noch hat er ja das Cyberbüro im US-amerikanischen Außenministerium aufgelöst, wenn ich das richtig verstanden habe und die Person, die es geleitet hat, ist auch nicht mehr im Außenministerium. Es gibt also dort auch die Befürchtung, dass die Expertise, die auf US-Seite im Außenministerium dazu da war, in der Form jetzt nicht mehr dort ist.

Tim Maurer: Ja und vielleicht noch kurz, wir sind bei Carnegie auch teilweise etwas kritisch gegenüber dem Prozess und diesen Normen, weil es gibt da sehr spannende intellektuelle Fragen, die mit den bisherigen Übereinstimmungen einfach im Raum stehen. Wenn wir die Norm nehmen mit Blick auf kritische Infrastrukturen, die Übereinkunft, die 2015 in dem Bericht aufgenommen wurde, sagt, dass sich Staaten verpflichten, nicht wissentlich kritische Infrastrukturen mit offensiven Kapazitäten anzugreifen. Wenn wir jetzt das Beispiel WannaCry nehmen, eine Malware, die unter Umstände von einem staatlichen Akteur eingesetzt worden war und von dem wir ausgehen können, dass der staatliche Akteur, der WannaCry eingesetzt hat, wahrscheinlich nicht, hoffentlich nicht davon ausgegangen ist, dass es wirklich auf so großer Ebene so einen Einfluss haben würde und dass die Krankenhäuser in Großbritannien wirklich davon betroffen sind, dann stellt sich die Frage, wenn der Staat nicht wusste, dass es diesen Effekt haben würde, würde das bedeuten, dass diese Norm, die man 2015 getroffen hat, nicht wirklich verletzt worden ist, weil der Staat wahrscheinlich nichtwissentlich das durchgeführt hat. Das heißt, wenn wir so eine Situation haben, wo ein Staat die Möglichkeit hat, offensiv vorzugehen und aufgrund der Unwägbarkeiten, wie eine Cyberwaffe sich letzten Endes auswirkt, von so einem Abkommen nicht wirklich betroffen ist, dann stellt sich diese, inwieweit wird das wirklich einen substanziellen Effekt haben mit Blick auf die Staaten, die

diese Mittel in Zukunft nutzen werden.

Stefan Heumann: Du hast schon angesprochen, dass die Verhandlungen auf UN-Ebene sehr schwierig sind. Wir haben generell das Problem, dass Russland und China und Iran, Europa, USA, dass es in dieser Konstellation sehr schwierig ist, Konsens zu erzielen und wahrscheinlich jetzt auch mit vielleicht dem Vorzeichen der US-Politik das noch mal komplizierter geworden ist. Haben wir Alternativen? Viele gucken ja auch sehr kritisch zur UN und das sind Prozesse, die dauern über Jahrzehnte und da wird an einzelnen Definitionen jahrelang gestritten, dabei entwickelt sich diese Technologie rasant. Und die Fragen um die Cyberattacken und Angriffe nehmen jetzt schon massiv zu und wir müssen ja irgendwie in das Gespräch kommen, wie wir damit umgehen und wir müssen das international lösen, weil das ein global vernetzter Kommunikations- und Informationsraum ist. Was gibt es für Ansätze und wie denkt man auch bei Carnegie darüber nach, was es für Alternativen gibt zu dieser UN-Level-Diskussion, das Thema Cybernorm und wie Staaten sich verhalten sollten, wie man da vorwärtskommen kann?

Tim Maurer: Ja. Also das ist dieses Jahr richtig spannend jetzt geworden, teilweise wegen des Kollaps des VN-Prozesses im Juni und im Moment gibt es aus meiner Sicht drei Pfade, die sich jetzt offen gelegt haben. Der erste ist eine Fortführung des VN-Prozesses. Der geht zurück auf diesen russischen Entwurfsvorschlag von Ende der 90er Jahren, dass man einen internationalen Vertrag braucht. Dem haben sich die westlichen Staaten seitdem gegengesetzt und gesagt, ein Vertrag funktioniert in diesem Bereich nicht, aus verschiedenen Gründen. – Die können wir auch diskutieren. Aber dieser Prozess war darauf konzentriert, Normen zu schaffen. Der ist jetzt kollabiert.
Microsoft hat seit vergangenem Jahr den Vorschlag einer digitalen Genfer Konvention gemacht. Das ist der zweite Pfad, der sehr viel weiter geht und dem ursprünglichen russischen Vorschlag, dass es ein Vertragswerk geben muss, sehr viel näher ist, obwohl es da substanziell natürlich Unterschiede sind. Der Microsoft-Vorschlag ist wahrscheinlich der ambitionierteste, den es derzeit gibt. Wenn man mit westlichen Regierungen spricht, gibt es ein gesundes Niveau an Skepsis, dass das in naher Zukunft passieren wird. Ich glaube, das fasst es gut zusammen.
Und der dritte Pfad ist das, was ich als, was wir bei Carnegie zurzeit versuchen, beschreiben würde. Wir haben vor zwei Jahren gesagt, es ist gut, dass es den VN-Prozess gibt. Der ist sehr umfassend und versucht, ein umfassendes Regelwerk zu entwickeln. Wir arbeiten seit zwanzig Jahren daran, die Bedrohungslage hat sich in den letzten Jahren rapide verschlimmert und es ist unwahrscheinlich, dass die diplomatische Zeitleiste mit der sich rapide verschlechternden Bedrohungslage Schritt halten wird. Deswegen haben wir gesagt, okay, dann schauen wir an, gibt es Bereiche, wo wir glauben, dass es eine Gemengelage gibt, wo man schneller Fortschritte machen kann unter den Großmächten trotz der Interessensunterschiede und haben ein Projekt ins Leben gerufen, das sich vor allem auf Finanzstabilität und Cybersicherheit konzentriert.

Wir haben das vor zwei Jahren angefangen und der Hintergedanke war, dass Finanzstabilität etwas ist, worauf in China auf jeden Fall besonders Wert gelegt wird,

weil man einerseits weiterhin großes Wirtschaftswachstum haben will, man möchte andererseits auch keine sozialen Unruhen haben, wenn es jetzt auf einmal einen Run on the Bank gibt, weil irgendwie kein Vertrauen in die Banken mehr besteht. Und wenn es Finanzinstabilität in China gibt, dann können wir auch der amerikanischen Wirtschaft bald wieder gute Nacht sagen. Von daher ist das ein Thema, wo wir glauben, im Gegensatz zu anderen kritischen Infrastrukturen ist das ein interessantes Feld.

Und wir haben dann einen vertraulichen Vorschlag entwickelt, weil wir nicht immer direkt als Thinktank veröffentlichen, was wir erarbeitet haben, mit Blick auf unsere Forschung. Und wir haben uns an verschiedene Regierungen gewandt im Rahmen der G20, weil die G20 ja mit Finanzstabilität, sich darauf konzentriert und 2015 sich auch mit dem Thema Cybersicherheit schon beschäftigt hat, nachdem Präsident Xi und Präsident Obama ein Abkommen getroffen haben. Und wir haben jetzt im März gesehen, dass unter dem deutschen G20-Vorsitz es zum ersten Mal einen Paragrafen gab von den G20-Finanzministern, der sich konzentriert hat auf Cybersicherheit und Finanzstabilität. Da geht es sehr viel mehr um Resilienz und wie man es schafft, den Bankensektor und die Finanzinstitute generell besser zu schützen. Es gab aber auch Diskussionen; wir hatten Minister Schäuble eingeladen bei Carnegie, wo er dann im April gesprochen hat und Herr Dr. Schäuble hat bei der Veranstaltung auch darauf hingewiesen, dass es neben dem Text, den es im März gab, Verhandlungen gab zu einer politischen Wohlverhaltenserklärung, was ähnlich des Vorschlags ist, den wir entwickelt haben und den wir dann im März als Bericht veröffentlicht haben und jetzt mit verschiedenen Ländern weiter besprechen.

Stefan Heumann: Also der ambitionierte Ansatz wäre, nicht nur sagen, der Finanzsektor muss besser geschützt werden, sondern das zu ächten, dass Finanzinstitutionen überhaupt angegriffen werden. Richtig?

Tim Maurer: Genau. Und um jetzt ein bisschen technischer zu werden, unser Vorschlag ist konkret, dass sich die G20-Staaten darauf einigen, nicht die Integrität von Daten von Finanzinstitutionen zu manipulieren, also dass man auf einmal nicht mehr genau weiß, ob die Daten und die Werte der Daten von Finanzinstitutionen noch akkurat sind oder nicht und dass sich die G20-Daten darauf verständigen, die Verfügbarkeit von kritischen Systemen zu unterminieren, weil auch da Bedenken und Sorge besteht, dass das unter Umständen ein Risiko für Finanzstabilität beinhaltet.

Was wir herausgenommen haben, ist die Vertraulichkeit von Daten. Einige Staaten würden das wahrscheinlich gerne sehen, aber das würde bedeuten, wenn man das in so ein Abkommen mit reinnimmt, dass man Staaten bitten würde, zu sagen, dass sie keine Spionage betreiben, die sich um Finanzinstitute kümmern. Entweder hat man dann Staaten, die so einem Abkommen zustimmen, aber sich nicht daran halten, oder man hat Staaten, die sagen: „Nein, wir werden dem nie zustimmen, weil wir weiter Spionage betreiben wollen.“ Und da es unser Ziel ist, das Risiko von Finanzinstabilität zu minimieren, haben wir gesagt, okay, dann nehmen wir das raus, um die politische Wahrscheinlichkeit für so ein Abkommen zu erhöhen. Und wir

können uns vielleicht in fünf Jahren noch mal hier unterhalten, dann sehen wir, wie weit wir gekommen sind.

Stefan Heumann: Ich habe noch viele Fragen für Tim, ich will es aber nicht komplett monopolisieren und deswegen würde ich Sie gerne einladen, wenn Sie eine Rückfrage haben oder ein bestimmtes Thema, das Ihnen zu kurz gekommen ist, ansprechen wollen, oder auch ein Kommentar zu dem, was Tim gesagt hat, bitte.

Teilnehmer: Ich hätte eine kurze Frage, wie es denn im Rahmen der Vereinten Nationen weitergehen könnte Ihrer Meinung nach? Dass die GGEs dieses Jahr keinen Bericht verfassen konnte, ist natürlich sehr, sehr schade, aber für uns ist es weiterhin das wichtigste Forum in der internationalen Zusammenarbeit. Also was wäre eine Möglichkeit, dass wir da an dem Thema weiter arbeiten? Wäre eine Option auch, dass man die Gespräche mehr in Richtung Multi-Stakeholder-Diskussion irgendwie erweitert? Natürlich müssen die Nationalstaaten am Ende ein Agreement finden, aber der Microsoft-Vorschlag zeigt ja auch, dass auch Vorschläge aus der Privatwirtschaft, teilweise auch aus der Zivilgesellschaft kommen.

Und meine zweite Frage wäre, warum ist man im Westen so skeptisch gegenüber festen Regeln? Ich verstehe, dass wir das Problem der unterschiedlichen Definitionen haben und dass auch der Microsoft-Vorschlag noch nicht ganz ausgereift ist, aber die Frage ist doch, ob wir nicht langfristig auch das Völkerrecht ergänzen müssten und feste Regeln schaffen müssen. Danke.

Tim Maurer: Zur ersten Frage mit Blick auf den VN-Prozess. Es hat verschiedene Vorschläge gegeben, wie man den Prozess weiterführen kann. Option A ist, noch einmal eine neue Gruppe in naher Zeit in das Leben zu rufen. Die zweite Option ist, die Conference on Disarmament, ob das dahin getragen werden soll oder eine offenstehende Arbeitsgruppe. Es gibt verschiedene Pros und Cons für jede Option.

Mein Eindruck, wenn es nur nach mir ginge, was es Gott sei Dank nicht tut, würde ich erst mal ein bisschen auf die Bremse treten mit Blick darauf, den neuen Bericht zu erweitern, weil ich glaube, dass die politische Gemengelage im Moment gerade auch in Washington so ist, dass ich nicht weiß, was der große Unterschied wäre zu dem, was man jetzt im vergangenen Jahr gemacht hat. Ich glaube, es gibt einfach eine Möglichkeit, sich darauf zu konzentrieren, was man vor allem in 2015 schon erreicht hat und versucht, das zu implementieren.

Die Tatsache, dass man beispielsweise weiterhin keinen Konsens hat, ob der Stromausfall in der Westukraine – im Dezember 2015 war das – eine Verletzung der Norm aus dem Bericht von 2015 war, besorgt mich. Die amerikanische Regierung, Michele Markoff, die führende Person auf amerikanischer Seite hat gesagt, aus ihrer Sicht war es keine Verletzung der Norm, weil sich die Ukraine und Russland offiziell in einem Kriegszustand befinden und die Norm, die 2015 verabschiedet worden war, für Friedenszeiten gilt. Es gibt aber auch verschiedene andere ehemalige Regierungsbeamte, die sagen, nein, das war eine Verletzung der Norm und das ist nur innerhalb des US-Kontextes. Das heißt, wenn wir noch nicht mal wissen, was

jetzt eine Verletzung der Norm bedeutet, die wir 2015 schon vereinbart haben, gibt es da, glaube ich, einfach sehr viel, das man machen kann, ohne dass es jetzt einen nächsten Prozess gibt, vor allen Dingen wenn die offene Frage ist, was dieser neue Prozess in den nächsten ein oder zwei Jahren erreichen würde.

Mein Eindruck ist, dass begleitende Prozesse, beispielsweise ähnlich dem, den wir verfolgen mit Blick auf die G20, wo wir glauben, dass man in bestimmten Bereichen schneller Fortschritte machen kann, das man das verfolgen sollte. Das Gegenargument hier ist von verschiedenen Seiten, dass ein sektorenspezifisches Abkommen, beispielsweise nur auf den Finanzsektor, nicht gewünscht ist, weil man nicht möchte, dass man ein umfassendes Regelwerk damit unterminiert. Unsere Ansicht ist, das wird eher die breiteren Verhandlungen unterstützen, wenn man in bestimmten Bereichen, wo es gemeinsame Interessen gibt, weiterhin Fortschritt machen kann und sich dann über die Zeit positiv einfach Spill-over-Effekte bilden und dass es da keine Nullsummen gibt.

Die zweite Frage zu den nichtstaatlichen Akteuren. Als nichtstaatlicher Akteur, der in dem Bereich Vorschläge macht, würde ich mir natürlich wünschen, dass solche Vorschläge da direkt aufgenommen werden. Für Microsoft wird sich, glaube ich, die Frage stellen in den nächsten Monaten, inwieweit sich die Arbeit, die Microsoft nicht jetzt schon im vergangenen Jahr, seitdem Brad Smith sich für das Thema sehr persönlich interessiert, sondern die Arbeit, die sie seit jetzt acht Jahren in dem Bereich schon machen, die aus meiner Sicht wirklich darüber hinausgeht, was man normalerweise von Unternehmen erwartet, in so Public-Policy-Feldern zu machen und wofür ich Microsoft auch wirklich Kredit zolle, aber für Microsoft wird sich die Frage stellen: Bleibt es nur eine Microsoft-Initiative oder sehen wir jetzt wirklich, dass sich andere Unternehmen dem anschließen? Weil wenn es weiterhin nur eine Microsoft-Initiative bleibt, dann fragt sich, warum und gibt es da keine andere Anstrengung. Auf den Punkt komme ich später noch einmal zurück.

Teilnehmer: Genau, es geht noch mal um die Initiative von Microsoft, weil Sie haben die jetzt sozusagen sehr herausgehoben und auch gemeint, dass sich Microsoft da sehr engagiert. Im politischen Berlin hört man eher, dass das ein PR-Gag von Microsoft wäre. Da würde mich Ihre Einschätzung interessieren.

Tim Maurer: Ja. Ja und nein. Also Microsoft ist ein Privatunternehmen, das natürlich profitorientiert ist und eigene Interessen verfolgt. Google und Facebook sind sehr viel aktiver, wenn es um die Surveillance-Debatte und Menschenrecht geht, teilweise wegen dem Snowden-Effekt. Also das ist auch interessant zu sehen, dass verschiedene Unternehmen verschiedene Lieblingsprojekte haben. Ich glaube, es ist aber auch fair, zu sagen, wenn man sich anschaut, wie lange Microsoft sich mit dem Thema schon befasst hat und wie viel Leute Teil von diesem Unternehmen sind, Teil dieser Einheit sind, die sich mit dem Thema befassen, dass es schon ein bisschen darüber hinausgeht aus meiner Sicht, was man als reguläre Lobbyarbeit sieht. Aber man muss sich auch die Frage stellen jetzt mit dieser Digital Geneva Convention, Microsoft war das erste Unternehmen, das nach Snowden verschiedene

Transparenzzentren aufgebaut hat, das in den Datenlokalisierungsdebatten relativ flexibel ist.

Genau, von daher ist da definitiv Eigeninteresse, aber es ist einer der wenigen Akteure, der in dieser internationale Debatte neue Impulse gibt. Und ich glaube, wenn man sich anschaut, wie sich die Sicherheitslage in den letzten Jahren verschlechtert hat, bin ich eher jemand, der generell positiv jedem Akteur gegenübersteht, der neue Impulse gibt und neue Ideen vorbringt, weil wir einfach bisher es nicht geschafft haben, mit der Bedrohungslage umzugehen.

Teilnehmer: Ich würde gerne anknüpfen an die schwierige Unterscheidung zwischen staatlichen und nichtstaatlichen Akteuren. Sie haben ja auch schon die Proxys genannt und dann über Gegenmaßnahmen gesprochen, also es sind Stichworte wie Strafbefehle gefallen. Das sind ja eigentlich keine Verteidigungsmaßnahmen sondern Law-Enforcement-Maßnahmen. Es gibt in dem Bereich Cyberkriminalität ja schon länger Diskussionen und auch ein Vertragswerk beim Council of Europe und es gab vorher von Russland auch Bewegungen, dann eben ein Vertragswerk anzuregen, das ein bisschen in Konkurrenz steht zu der Council of Europe Cybercrime Convention.

Von daher würde ich gerne zwei Fragen stellen. Einmal: Warum glauben Sie, dass jetzt diese Cyber-Defence-Initiative erfolgreicher sein könnte als die Cybercrime-Diskussion, warum man da nicht vielleicht in dieselben Schwierigkeiten hereintappt, in die man vorher reingetappt ist? Und die zweite Frage: Wenn man es schafft, ist das überhaupt sinnvoll, diese Unterscheidung zu machen, oder wird man in der Praxis nicht ohnehin irgendwelche Hacker vor sich haben, wo man nicht unterscheiden kann, ob sie staatlich oder nichtstaatlich sind? Und man muss dann ohnehin die Maßnahmen der Strafverfolgung ergreifen, wie man es jetzt auch schon tut und hat von einem Cyber-Defence-Treaty eigentlich gar nichts.

Stefan Heumann: Wir nehmen die zweite Frage noch mit dazu.

Teilnehmer: Sie hatten, da stimme ich Ihnen vollkommen zu, aufgeführt, dass ein Verbot praktisch nicht konsensfähig ist. Deswegen wunderte mich ein bisschen, dass Sie als Beispiele, analytische Beispiele das Hacking des Bundestages und das Hacking der DNC Server genommen haben, denn das sind ja nun typische Informationsgewinnungs- und keine Zerstörungsmaßnahmen. Der beeindruckendste Film für mich auf der Berlinale 2016 war der Film ‚Zero Days'. Den kennen Sie wahrscheinlich.

Tim Maurer: Ja.

Teilnehmer: Und da wurde ein bisschen die Gefahr beschworen, dass jetzt ein Tabubruch entstanden ist, indem man eben mit Cybermitteln physische Dinge kaputtmacht und dass da nun die ersten Länder den Bruch begangen haben. Von daher ist jetzt dieses Bedrohungsszenario mit der Entscheidung zwischen beabsichtigten und unbeabsichtigten Folgen für mich noch mal besonders scharf zu

stellen, denn wir wissen ja auch alle, dass beim Bundestrojaner und bei ähnlichen Überlegungen diese Zero-Day-Exploits nicht nur nicht geschlossen werden, sondern auch von Kriminellen durchaus gegen Geld erworben werden und natürlich in den allerbesten Absichten. Aber wenn sozusagen das Mittel selber eines ist, was nicht kontrolliert werden kann, denn zumindest der Hacker, der es verkauft hat, kann es natürlich weiter verkaufen. Das ist ja nicht eine einmalige Kopie, wir sind hier im digitalen Bereich, da gibt es kein Kopierverbot oder man kann Kopieren nicht unmöglich machen, es sei denn, man hat es jetzt mit verschränkter Arbeit, mit verschränkten Methoden zu tun. Da sehe ich eine ganz grundsätzliche Schwierigkeit. Da würde ich auch noch gerne Ihre Meinung dazu hören.

Tim Maurer: Zur Budapest-Konvention und Cyberkriminalität. Der russische Vorschlag, dass man da eine neue globale Konvention braucht für Cyberkriminalität, was, glaube ich, auch die Brasilianer und die Inder wahrscheinlich unterstützen würden, das wird in den nächsten fünf Jahren, glaube ich, nicht passieren. Weil die Inder und die Brasilianer sagen, sie hatten damals keinen Platz am Tisch, von daher möchten sie dieser Konvention nicht beitreten, weil das aus einer regionalen Organisation gekommen ist. Die Russen mögen den Paragrafen mit Blick zu grenzüberschreitenden Untersuchungen nicht und die Chinesen mögen die Konvention auch nicht. Von daher gibt es eine Gemengelage, wo man sagen würde, es gibt genug Staaten, die ein neues Instrument haben wollen. Auf der anderen Seite ist das Gegenargument, dass die westlichen Staaten und die Vereinigten Staaten sagen, wir haben eine Konvention, wir brauchen keine neue Konvention, warum sollen wir jetzt über Jahre hinweg noch einmal eine neue Konvention verhandeln, wenn es viel einfacher wäre, dass sie der beistehen. Ich sehe nicht, dass sich das in den nächsten fünf Jahren signifikant ändert, diese Gemengelage. Und was wir stattdessen wahrscheinlich sehen, ist, dass es, wie wir das jetzt auch bei der Afrikanischen Union gesehen haben, Verträge gibt, die auf regionaler Ebene geschlossen werden und die dann die Budapest-Konvention komplementieren.

Zu dem sehr interessanten Punkt, ob diese Unterscheidung, sie verschwindet, und ob man das nicht zusammenfassen sollte. Klar, die Unterscheidung mit dem Verschwinden, nicht dem Verschwinden, aber dass Grenzen weniger eine Rolle spielen, ist, glaube ich, eine große Frage. Die Strafbefehle, die ich genannt habe, ich glaube, das amerikanische Justizministerium macht sich da keine Illusionen, dass sie diese sieben iranischen Hacker in naher Zukunft irgendwann mal verhaften wird. Die wissen, auch genau zu gucken, wo es Ablieferungsabkommen gibt und nicht. Das war mehr ein Signal an die Iraner, das man feststellen kann, wer dahinter steckt, weil diese Debatte über das Attribution-Problem teilweise verschleiert hat, dass man schon unter bestimmten Bedingungen sehr genau weiß, wer dahinter steckt. Und es war ein Signal auch an die Privatunternehmen, dass man doch etwas gemacht hat.

Der andere Kommentar, den ich dazu machen würde, ist, unser Vorschlag mit Blick auf die Finanzstabilität versucht beides zu überbrücken. Der Vorschlag, dass man einerseits die Staaten dazu bringt, zu sagen, dass sie diese Finanzinstitute nicht angreifen werden, ist sehr ähnlich wie internationale Sicherheit, dass man das ächten will. Wir haben aber auch in unserem Vorschlag eine zweite Komponente,

dass die Staaten sich verpflichten würden, bei solchen Vorfällen zu kooperieren. Und die Logik dahinter ist konkret, dass der große Bedrohungsakteur im Moment eben Kriminelle sind und wir aber aufgrund der Komplikation mit der Budapest-Konvention im Moment in der Situation sind, wo es keine Kooperation gibt, wir aber glauben, wenn es zu Vorfällen kommt, die wirklich das Risiko bergen, Finanzstabilität zu unterminieren, dass man da vielleicht sogar sagen kann, dass die Russen und die Amerikaner da untereinander kooperieren würden, weil die Russen sagen: „Ihr Kriminelle, ihr dürft weiterhin westliche Ziele angreifen, weil wir auch nebenbei Geld verdienen, aber wenn ihr bestimmte Sachen macht, die über eine bestimmte Schwelle gehen und ein Risiko für Finanzstabilität besteht, da wollen wir den Deckel draufhalten und wenn es drüber geht, dann sind wir bereit, auch mit den anderen zu arbeiten und entweder ihr wählt ab oder ihr landet im russischen Gefängnis.“ Das ist so ein bisschen die Logik dahinter, dass man versucht, die beiden zu überbrücken.

Zur Frage von Spionage und dem Abkommen. Das Übereinkommen zwischen Präsident Xi und Präsident Obama war schon sehr spannend, weil es da um Wirtschaftsspionage ging und man da innerhalb der amerikanischen Diskussion schon die Unterscheidung macht, dass man in bestimmten Bereichen der Spionage sagt, bestimmte Sachen sollten nicht stattfinden und die Chinesen dem zugestimmt haben. Das ist auch übrigens aktuell das einzige Beispiel, von dem wir wissen, dass es einen signifikanten Einfluss auf das Verhalten hatte, dass man wirklich von Geheimdiensten bis hin zu den Leuten in Silicon Valley, die in den verschiedenen Großunternehmen arbeiten und Zugang zu den Daten haben, gesagt hat, man hat eine Reduktion der Aktivität von chinesischer Seite festgestellt. Aber mit Blick auf politische Spionage gibt es so viele Akteure, die dem zustimmen werden. Die Diskussion gab es nach Snowden, die wurde durchgekaut und da wird es keine Änderung in naher Zukunft geben. Ich hoffe, das beantwortet die Frage.

Teilnehmer: Es war ja dann noch die Frage dieser Zero Days und des Präzedenzfalls, dass man also den Verzicht auf den Angriff von physischer Infrastruktur eben anscheinend auch nicht als konsensfähig ausgestalten kann.

Tim Maurer: Ja, wobei es diesen Konsens jetzt gab, dass man sagt, in Friedenszeiten würde man das nicht machen mit Blick auf kritische Infrastruktur.

Teilnehmer: Ja, die Argumentation war ja eher, wir vermeiden jetzt ein Bombardement des Irans und da soll sich der Iran freuen, dass wir auf diese Weise zugeschlagen haben.

Tim Maurer: Das ist das andere Argument, das humanitäre Argument, dass es unter humanitärem Völkerrecht ist, dem Principle of Humanity and Destinction. Das ist ein interessantes Argument, ich glaube, das funktioniert aber nicht, weil die Logik, dass man Hacken einsetzen sollte, um Menschenleben zu retten, funktioniert nur, wenn man genügend Akteure hat, die die anderen Prinzipien, Unterscheidung ziviler, militärischer Ziele et cetera, sich daran halten würden. Und meine Sorge ist, wenn es um Cyberwaffen geht, müssen wir uns mehr Sorgen um Proxy und nichtstaatliche Akteure machen, die dieser Logik nicht notwendigerweise folgen. Von daher finde

ich, das ist ein interessantes Argument, dem ich aber, wie ich aus Ihrem Kommentar heraushöre, ebenfalls nicht folge und zustimme.

Teilnehmer: 2003 hatte schon so ein bisschen den Eindruck, dass da irgendwie viele Leute plötzlich über das Thema „Cyberwar“ reden, von dem sie wenig Ahnung haben und hat sich irgendwie heute wenig geändert. Also sozusagen viele Regierungsakteure, die mit Wörtern und Denkweisen der traditionellen Welt der zwischenstaatlichen Kriege und den Vokabeln dazu über Dinge reden, die mit Waffen nichts zu tun haben. Also sozusagen, es sind Softwarevulnerabilitäten, es gibt ein eine Nicht-Zuordenbarkeit der Attacken und deshalb stellt sich ein bisschen für mich die Sinnfrage, wenn man jetzt sagt, wir machen so eine Art Nichtangriffspakt, hat das irgendeine Wirkung bei einer Waffe, in Anführungszeichen Waffe, die gar nicht zuordenbar ist? Und vielleicht ein Alternativvorschlag, was eine Wirkung hätte, wäre eine Vereinbarung dazu, wie viel Geld, wie viel Mittel, wie viel Personalressourcen in das Absichern des Netzes fließt versus, wie viel Unsicherheit reinfließt. Also sozusagen Defensivbudget versus Offensivbudget. Und je mehr das Defensivbudget reinfließt und je weniger Offensivbudget, also ZITiS und wie sie alle heißen, reinfließt, desto sicherer wird das Netz global.

Teilnehmer: Aber auch ZITiS ist auch defensiv.

Stefan Heumann: Nein, die sollen ja Schwachstellen ausnutzen, aber das ist noch mal eine erweiterte Diskussion. Die Frage greift Tim gleich auf. Sie hatten sich auch gemeldet.

Teilnehmer: Ich würde gerne für einen Moment den Blick etwas weiten und Sie einfach fragen, wie sich diese Debatten zu Cyber Security in das größere Bild global mit globaler Normenbildung einordnen lassen? Weil bei aller Faszination für das Spezifische an diesen Cyber-Security-Debatten und auch dem Bewusstsein darum, dass natürlich einzelne technische Herausforderungen besonders sind, frage ich mich doch, ob nicht viele Probleme politisch, die man hier trifft, auch auf anderen Ebenen der Rüstungskontrolle oder auf Feldern wie der Klimapolitik bekannt sind und man nicht aus dem Vergleich zu anderen Politikfeldern erstens interessante Lehren ziehen könnte und vielleicht aber auch zu einem anderen Erwartungsmanagement kommen könnte und sollte, was die Möglichkeiten, an die ich immer noch glaube – da bin ich optimistisch – was die Möglichkeiten und auch die Grenzen internationaler Regulierung angeht.

Tim Maurer: Ja, die Debatte könnte von größerer Differenziertheit sein, aber es ist schon unglaublich nuancierter geworden. Also ich glaube, alleine in den letzten sieben Jahren, als ich angefangen habe im Vergleich zu heute, jetzt die Diskussion hier alleine und was sich in Berlin in den letzten drei, vier Jahren getan hat. Ich glaube, man hat auch mittlerweile differenzierter Argumente, was ein Cyberwar ist. Ja, es sind Schwachstellen und es gibt aber auch tatsächlich Schwachstellen, die dazu führen können, dass Leute sterben. Das haben wir noch nicht gesehen, aber ich glaube, es gibt genug Hacker, die sich darum, sagen wir, , I am the cavalry‘ in den

USA, die aus der DEFCON-Szene kommen und sich so Sorgen machen, aus der Hackerszene, um diese Fragen, gerade aus nichtstaatlicher Akteursszene, dass wir da in einer anderen Situation sind als vor ein paar Jahren.

Was ich glaube, was wir noch nicht geschafft haben, ist der Punkt, den Sie gemacht haben mit Schwachstellen. Die Gemeinsamkeit ist, dass sowohl die Person, die relativ, sei es, teilweise Web Defacement oder andere Sachen macht, was sich unterscheidet, ist nicht die Schwachstelle, sondern letzten Endes die Payload, die dann umgesetzt wird, wenn man einmal Zugang zum System hat. Und dass da Cyberwaffen diskutiert werden von FinFisher hin zu Siemens-Zentrifugen hin zu Eingriffen in der Wertschöpfungskette und das alles in einen Topf geschmissen wird und da nicht genügend differenziert wird, ich glaube, das ist weiterhin das Problem. So ein Abkommen kann, glaube ich, schon den Unterschied machen, wie wir das nach dem Xi-Obama-Abkommen gesehen haben.

Das Attribution-Problem sehe ich auch, wird mittlerweile differenzierter argumentiert. Die meisten Staaten haben nicht die Möglichkeit, herauszufinden, wer dahinter steckt. Auch die Vereinigten Staaten haben weiterhin in vielen Fällen nicht die Möglichkeit, herauszufinden, wer hinter einem Angriff steht. Die Tatsache, dass wir aber schon seit zwanzig Jahren erfolgreich von Strafverfolgungsbehörden verschiedene Urteile haben, wo vor Gericht Hacker, die nicht nur die in Deutschland operieren, sondern auch in anderen Ländern, zu Gefängnisstrafen verurteilt worden sind, suggeriert auch, dass es trotzdem genügend Möglichkeiten gibt, Beweise zu sammeln, die selbst vor Gericht unter den verschiedenen Standards, die es gibt, standhalten können. Und mit Resilienz, dem stimme ich zu, also da ist das Problem, dass das Pentagon ja nicht nur in dem Bereich, sondern in allen anderen Bereichen viel mehr Geld bekommt als jetzt das State Department oder andere Sachen. In Deutschland habe ich zur Kenntnis genommen, dass es jetzt dreizehn neue Professuren gibt für die Bundeswehr in dem Bereich. Ich glaube, es gibt keine dreizehn Professuren im Bereich Resilienz. Das könnte man vielleicht…

Globale-Norm-Diskussion. Vor allem das chinesische Beispiel mit Blick auf das Völkerrecht ist, glaube ich, ein gutes Beispiel, wo man sieht, dass sich das nicht nur mit Blick auf die Cybersicherheit konzentriert, sondern dass China auch in vielen anderen Normbereichen die liberale Ordnung infrage stellt. Es gibt auch viele Leute, die sich andere Regime angucken und inwieweit das auf Cyber angewandt werden kann. Das Wassenaar-Regime ist, glaube ich, ein gutes Beispiel, wo gezeigt worden war, warum das nicht direkt angewandt werden kann. Meine Sorge ist eher, dass es unter Umständen zu viele Leute gibt, die aus einer bestimmten Schiene kommen, nämlich der nuklearen Schiene und dass viele der Leute, die in dem VN-Prozess sind, aus der nuklearen Schiene darauf schauen und jetzt nicht beispielsweise aus der Biowaffengemeinde kommen. Weil ich glaube, viele der Fragen, die sich mit Viren beschäftigen und Biowaffen, die sehr viel ähnlicher dem Verhalten von Software und Code sind und dann auch mit Blick auf Resilienz und wie man jetzt beispielsweise über einen Virus, der sich verbreitet, was man da für Logiken hat, das wäre eine ganz andere Herangehensweise, die nicht präsent ist. Weil die Leute, die sich vor zehn Jahren damit beschäftigt haben, mit einem nuklearen Hintergrund zu dem Thema

kamen und es da jetzt Pfadabhängigkeiten gibt, die das entsprechend beeinflussen.

Stefan Heumann: Ich denke, dass durch die Diskussion mit Tim noch einmal klar geworden ist, vor was für einer großen und komplexen Herausforderung wir stehen, dass es gleichzeitig auch klar ist, dass wir uns dieser Herausforderung stellen müssen. Du hast es angesprochen, bisher sind glücklicherweise noch nicht so viele Menschen zu Schaden gekommen, aber durch die fortlaufende Vernetzung auch vor allem von physischen Geräten, die dann übernommen und manipuliert werden können, können auch wirklich große physische Schäden entstehen, also Angriffe auf ein Schienensystem oder auf Züge, die dann auf einmal aufeinander prallen, weil die Weichen manipuliert worden sind. Man kann sich da ganz viele schlimme Sachen ausmalen und ich glaube, dass deswegen die Debatte wahnsinnig wichtig ist und ich glaube, Tim auch noch mal wichtige Anhaltspunkte geliefert hat, wo man außerhalb der UN auch noch hinschauen könnte und was alternative Strategien sein könnten.

-Ende des Transkriptes-