Evangelische Akademie Loccum

“Cyberwarfare – Cyberpeacebuilding“

Auf der Suche nach einer kooperativen Sicherheitsarchitektur im Cyberspace

Internationale Veranstaltungsreihe, April – Juni 2021

In den vergangenen Jahren haben Cyberbedrohungen deutlich zugenommen. Ein Rüstungswettlauf im digitalen Raum ist längst im Gange. Fast täglich wird über neue Cyberattacken in den Medien berichtet. Vor diesem Hintergrund organisierte die Evangelische Akademie Loccum von April bis Juni 2021 eine sechsteilige digitale Veranstaltungsreihe mit internationalen Cyber-Expert*innen mit dem Titel *Cyberwarfare - Cyberpeacebuilding: On a Search for a Cooperative Security Architecture in Cyberspace*.

Das Feld der Cyberbedrohung ist weitläufig und umfasst unterschiedliche Phänomene wie beispielsweise digitale Desinformationskampagnen, Cyberkriminalität, Digitalüberwachung oder Cyberspionage. In der Veranstaltungsreihe wurden vor allem staatliche Cyberkonflikte in den Fokus genommen sowie die inter- und transnationalen Bemühungen zur Deeskalation, Regulierung und Einhegung von militärischen Cyberattacken.

Dieser Veranstaltungsbericht fasst in aller Kürze die wichtigsten Ergebnisse der Tagung zusammen. Die hier dargelegten Perspektiven spiegeln nicht unbedingt die Ansichten aller teilnehmenden Personen und Institutionen wieder.

Ausführlicher Tagungsbericht

Cyberangriffe im Wandel: mehr, komplexer und potenziell gefährlicher

Die an der Veranstaltung mitwirkenden Expert*innen teilten übereinstimmend die Einschätzung, dass die Bedrohungslage im Cyberraum in den vergangenen Jahren klar erkennbar zugenommen hat. Cyberangriffe würden nicht nur häufiger, sondern seien auch in der Vorgehensweise ausgeklügelter als in der Vergangenheit.

Grundsätzlich resultieren Cyberangriffe aus digitalen Verwundbarkeiten und IT-Sicherheitslücken und lassen sich vor diesem Hintergrund in drei Kategorien mit variierenden Bedrohungspotenzialen unterteilen, so die teilnehmenden Panelisten. Diese dreistufige Einteilung sei jedoch nicht in Stein gemeißelt. Vielmehr zeichne sich in letzter Zeit eine Verschiebung in der Bedeutung der drei Kategorien ab.

In der ersten und hinsichtlich ihres Bedrohungspotenzials untersten Kategorie rangieren Cyberangriffe, die bekannte IT-Sicherheitslücken ausnutzen und darüber Schaden verursachen. Militärische und nachrichtendienstliche Akteure seien auf dieser Ebene weniger anzutreffen. Vielmehr sei dies das vorrangige Feld von Cyberkriminellen. Größtenteils würden auf dieser Ebene einfache, wenig zielgenaue und kostengünstige Angriffscodes verwendet, die jedoch massenhaft eingesetzt würden. Es seien vorwiegend *Ransomware*-Banden, die im digitalen Raum Lösegeld erpressen und Kapital aus nachlässiger *update*-Praxis, veralteten IT-Sicherheitssystemen oder unbedarftem Verhalten der *Enduser* schlagen (bspw. unprofessioneller Umgang mit *Phising*-Emails). Fahrlässigkeit der *Enduser* sei aber nicht die alleinige Grundlage für das Fortbestehen bekannter IT-Sicherheitslücken. In Unternehmen und Behörden sowie zunehmend im privaten Bereich würden im Alltag mittlerweile eine Vielzahl von interagierenden IT-Systemen verwendet. Um das reibungslose Zusammenspiel dieser Systeme nicht zu erschweren, würden umfassende updates häufig nur zögerlich vorgenommen und bekannte IT-Sicherheitslücken deshalb nicht geschlossen. Insbesondere mit der fortschreitenden Digitalisierung sei zu vermuten, dass offene IT-Sicherheitslücken aufgrund von Inter-operationalitätzwängen zunehmen werden, so die Einschätzung der Expert*innen. Diese erste Kategorie an Cybergefahren mache weltweit mit deutlichem Abstand das Gros der Cyberangriffe aus. Es sei unwahrscheinlich, dass sich an dieser Situation in den kommenden Jahren grundlegend etwas ändern würde, so die Diskutanten.

Die zweite Kategorie von Cyberangriffen basiere auf den sogenannten *zero day vulerabilites*. Es handelt sich dabei um IT-Softwarelücke die denjenigen, die an ihrer Behebung interessiert sind – in der Regel die Softwarehersteller und die Masse der Konsumenten – nicht bekannt sind. Diese unveröffentlichten Sicherheitslücken sind häufig mit nur geringem Aufwand aufzustöbern und können zum Teil für geringe Summen auf dem Schwarzmarkt erworben werden. Es ist aber auch nicht ungewöhnlich, dass *zero day vulnerabilities* von militärischen und nachrichtendienstlichen Akteuren gezielt gekauft und geheim gehalten werden, um diese im Cyberkonfliktfall für disruptive Aktionen im digitalen Raum einsetzen zu können. Diese Kategorie von Cyberangriffen hat ein höheres Gefährdungspotenzial – schon allein deswegen, weil zum Zeitpunkt, an dem ein Angriff detektiert wird, noch keine IT-Sicherheitsupdates verfügbar sind, mit den der verursachte Schaden eingedämmt werden könnte.

Die dritte und hinsichtlich ihrer Gefährdungspotenziale gravierendste Stufe von Cyberaktivitäten basiert auf konstruierten Sicherheitslücken, die zu Angriffszwecken verdeckt in Software eingebaut wird. Zwischen der Platzierung dieser IT-Sicherheitslücken – auch

digital backdoors genannt – und ihrer tatsächlichen Aktivierung können zum Teil erhebliche Zeitabstände liegen. *Supply Chain* Angriffe, wie beispielsweise der Solarwind Hack im Dezember 2020 bei dem Tausende Computersystem vor allem von US-Behörden betroffen waren, fallen beispielsweise in diese Kategorie. Schädliche digitale Codes werden bei diesem Angriffstyp zu einem frühen Zeitpunkt in die Lieferkette von Softwareprodukten platziert und gelangen dann unbemerkt im weiteren Verarbeitungsprozess in das eigentliche IT-Zielsystem. *Supply Chain* Attacken benötigen zwar ein hohes Organisationsniveau und relativ viel Vorbereitung aufseiten der Angreifenden, sind jedoch schwer zu detektieren und verwenden aufgrund der verdeckten Platzierung häufig einen vergleichsweise einfachen Angriffscode. Die teilnehmenden Expert*innen betonten, dass es schwer einzuschätzen sei, wie viele Aktivitäten auf dieser dritten und höchsten Komplexitätsstufte tatsächlich stattfinden, da dies ein Bereich sei, der vor allem im Kontext von militärischen und geheimdienstlichen Cyberprogrammen stattfände und daher weitestgehend der Öffentlichkeit entzogen sei. Dennoch könne beobachtet werden, dass die Zurückhaltung gegenüber dieser digitalen Angriffsform in den letzten Jahren abnimmt. Insbesondere *Supply Chain Angriffe* wurden von den Panelisten als bedeutender und wachsender Trend der Zukunft gewertet.

Abschließend und mit Blick auf alle drei Kategorien von Cyberattacken wurde betont, dass die Gefahr komplexer Cyberangriffe der dritten Kategorie in den kommenden Jahren vermutlich steigen werde, während die Attacken vor allem auf den beiden niedrigeren Stufen auf absehbare Zeit weiterhin relevant und auch quantitativ dominant bleiben dürften. Angesichts der zentralen Stellung von IT-Sicherheitslücken für Cyberangriffe wurde ferner von den Expert*innen betont, dass diese der digitalen Welt inhärent und ein fester systemischer Bestandteil des Cyberraums seien. Der digitale Raum sei in den letzten Jahrzehnten immer weitergewachsen, ohne dass Sicherheitsaspekte im gleichen Ausmaß Schritt gehalten hätten. Die Bereitschaft der IT-Kunden – ganz unabhängig, ob es sich um private, staatliche oder kommerzielle Akteure handele – höhere Preise für sichere Softwarelösungen zu zahlen, sei auf absehbare Zeit nicht vorhanden. Unsicherheit sei damit tief im System verankert und erstrecke sich auch auf Software, die zum Betrieb kritischer Infrastrukturen verwendet würden – worunter Systeme zu verstehen sind, die für das Funktionieren von Gesellschaften von zentraler Bedeutung sind (wie bspw. Stromversorgung, Wahlsysteme oder die akute Gesundheitsversorgung).

Cyberkonflikte: Eskalation – aber (derzeit) nicht auf allen Ebenen

Cyberangriffe sind zentrale Bestandteile von Cyberkonflikten – worunter Computerbasierte Auseinandersetzungen im digitalen Raum zwischen zwei oder mehreren Kontrahenten zu verstehen sind. Cyberkonflikte finden nicht im Vakuum statt, sondern sind digitale Begleiterscheinungen bestehender geopolitischer Rivalitäten und realer Konfrontationen, so die an der Veranstaltung teilnehmenden Expert*innen. Daher sei es nicht verwunderlich, dass in den aktuellen Cyberkonflikten neben den USA und Israel vor allem Nordkorea, China, Russland und der Iran dominieren würden.

Auffallend sei, so die Meinung der Expert*innen, dass im Cyberraum autokratische Mächte über deutlich mehr Eskalationsdominanz verfügen würden als demokratische Staaten. Offene Gesellschaften seien durch Cyberangriffe verwundbarer und im höheren Maße digitalen Disruptionen ausgeliefert als nicht-demokratische Staaten, die sich digital problemloser abschirmen ließen. Als Beispiel wurde hier vor allem Chinas *Great Firewall* angeführt. Chinas in weiten Teilen autarkes und vom weltweiten Netz abgekoppeltes Internet diene nicht nur der Zensur und Überwachung der eigenen Bevölkerung, sondern biete auch einen besseren Schutz im Cyberkonfliktfall. Diese asymmetrische Verwundbarkeit führe dazu, so die Panelisten, dass liberal-demokratische Staaten hinsichtlich militärischer Cyberaktivitäten mehr Zurückhaltung

und Stabilitätsorientierung an den Tag legen, während autokratische Staaten mit disruptiven und subversiven Aktionen im digitalen Raum dominieren würden. Vor diesem Hintergrund und mit Blick auf zukünftige Konfrontationen im digitalen Raum sei es für westliche Staaten eine große Zukunftsaufgabe, Wege zu finden, wie vorhandene Cyberfähigkeiten besser nutzbar gemacht werden könnten, so die Meinung der Expert*innen.

Ferner schilderten die teilnehmenden Panelisten, dass Cyberkonflikte keine gänzlich neuen Phänomene sein. In den letzten Jahren sei allerdings ein Wandlungsprozess mit einem Trend zur Eskalation erkennbar, der jedoch nicht unausweichlich sei, eine differenzierte Bewertung verlange und sich einer vereinfachten alarmistischen Betrachtung entziehen würde. Im Cyberraum sei es wichtig, zwischen zwei Formen der Eskalation zu unterscheiden – der direkten Eskalation, die unmittelbar zwischen zwei oder mehreren Akteuren stattfindet und der generellen systemischen Eskalation.

Hinsichtlich direkter Cyber-Auseinandersetzungen ist bisher noch kein Fall bekannt, bei dem es tatsächlich zu einer Eskalationsspirale – im Sinne einer wechselseitigen Zuspitzung von konfrontativen Aktions- und Reaktionshandlungen – gekommen sei. Zwar wurden Cyberangriffe in der Vergangenheit mit digitalen Gegenmaßnahmen beantwortet, aber ohne dass dabei ein eskalatives Element erkennbar gewesen wäre. In direkten Konfrontationen werden Cyberaktionen unter anderem deshalb gewählt, weil sie – im Vergleich zu herkömmlichen Militärmaßnahmen – für den Angegriffenen weniger bedrohlich sind und für den Angreifenden somit eine Reaktionsmöglichkeit bieten, die die Gefahr einer weiteren Zuspitzung eindämmt. Diese Zusammenhänge könnten gut im jüngeren Konfliktgeschehen zwischen den USA und Iran beobachtet werden. Direkte Cyberkonfrontationen seien somit in vielen Fällen ein Wettstreit zwischen Nachrichtendiensten unterhalb einer kritischen Eskalationsschwelle, der dem Katz- und Mausspiel zwischen dem sowjetischen KGB und westlichen Diensten während des Kalten Kriegs ähnle. Zugespitzt ließe sich also sagen, dass Cyberangriffe – im Gegensatz zur öffentlichen Wahrnehmung – oft unter einem de-eskalativen Vorzeichen stünden.

Trotzdem sollten direkte Cyberkonfrontationen wachsam beobachtet werden, so die Panelisten. Generelle Beschwichtigungen wären hier verfehlt. Denn die allgemein akzeptierte Zurückhaltung der letzten Jahre sei kein Selbstläufer und schütze vor allem nicht vor unbeabsichtigten Eskalationen, die bspw. schnell aus dem Umstand erwachsen könne, dass digitale Spionage und militärische Cyberattacken nur schwer voneinander zu unterscheiden seien. Auch wenn beide Formen von Cyberaktionen unterschiedliche Intentionen verfolgen und hinsichtlich ihres Gefährdungspotenzials deutlich variieren, sind sie im digitalen Erscheinungsbild größtenteils nur schwer zu unterscheiden und könnten somit schnell in eine konfrontative Zuspitzung münden. Zudem gelte die Einschätzung der reduzierten eskalativen Natur von Cyberkonflikten nur für Friedenszeiten. Zu zukünftigen bewaffneten Konflikten wird erwartet, dass sie stets von einer starken Cyber-Dimension begleitet werden. Mit Blick auf die nähere Zukunft werden direkte Cyber-Eskalation von den an der Veranstaltung mitwirkenden Expert*inne am ehesten zwischen Israel und Iran oder zwischen Indien und Pakistan erwartet.

Anders als in direkten Cyber-Konfrontationen seien – laut Einschätzung der Diskutanten – auf systemischer Ebene durch aus eskalative Tendenzen zu beobachten. So ist beispielsweise die Zahl der Staaten, die militärische Cyberprogramme betreiben, in den letzten Jahren kontinuierlich angestiegen. Derzeit wird vermutet, dass es weltweit ca. 140 derartige Programme gibt. Disruptive und subversive Cyber-Attacken nehmen zahlen mäßig zu. Zudem sei zu beobachten, dass Normen über verantwortungsvolles staatliches Handeln im digitalen Raum in den letzten Jahren zunehmen erodieren. Vor einigen Jahren hätten digitale Angriffe auf kritische Infrastrukturen noch als nicht zu überschreitende „rote Linien“ gegolten. Mittlerweile sei diese Norm häufig missachtet

worden. Kritische Infrastrukturen stünden zunehmend im Fadenkreuz digitaler Attacken und es sei zu vermuten, dass die derzeit geltenden „roten Linien" – wie bspw. Hackerangriffe auf die Kontroll- und Kommandostrukturen von Atomwaffen – in der Zukunft ebenfalls überschritten werden könnten, sollte die Hemmschwelle weiter sinken.

Auch wenn in der systemischen Betrachtung die Gefahren- und Eskalationspotenziale zunehmen, zogen die Expert*innen keine durchweg pessimistische Zukunftsaussicht. Hoffnungsvoll wird vor allem auf die technologischen und wissenschaftlichen Fortschritte im IT-Bereich geblickt, die in der Zukunft die Detektionsfähigkeit gegenüber der Masse an kriminellen Cyberangriffen verbessern könnte. Auch wird erwartet, dass die allgemeine Cyber-Resilienz in den kommenden Jahren weiter steigen wird. In der Zukunft dürften Wirtschaft, Gesellschaft und öffentliche Verwaltung durch verschiedene technologische Neuerungen und Anpassung in der Verhaltensweise mehr digitale Widerstandsfähigkeiten entwickeln und die Schäden von Cyberattacken leichter verkraften können, als dies derzeit der Fall ist.

Kein Vertrag aber Cybernormen: die inter- und transnationalen Bemühungen zu Einhegung von Cyberkonflikten

Mit Blick auf die wachsenden Bedrohungs- und Gefährdungspotenziale wird auf inter- und transnationaler Ebene seit einiger Zeit versucht, Cyberkonflikte einzuhegen und zu regulieren. Neben staatlichen Akteuren, die vor allem im UN-Rahmen aktiv sind, gibt es mittlerweile eine Reihe von transnationalen Initiativen – wie bspw. den *Tech-Accord*, den *Paris Call*, die *Charta of Trust* oder die *Global Commission on the Stability of Cyberspace*. Hier spielen ganz vorwiegend die Akteure aus der Tech-Industrie, die interessierte Zivilgesellschaft oder Akademiker*innen und Fachexpert*innen aus dem IT-Bereich und den Computerwissenschaften eine zentrale Rolle.

Die verschiedenen Bemühungen um Regulierung von Cyberkonflikten sollten aber nicht mit Kategorien aus dem Bereich der Rüstungskontrolle verglichen werden. Dies geschehe häufig in der öffentlichen Debatte, sei aber eine unpassende Analogie, die zu falschen Erwartungen führe, so die Meinung der an der Veranstaltung teilnehmenden Panelisten. So würden die verschiedenen inter- und transnationalen Bemühungen mittel- bis langfristig nicht in einen verbindlichen Cyber-Vertrag münden, wie dies in vielen Kontexten der Rüstungskontrolle und Abrüstungspolitik üblich ist. Auch wenn China und Russland immer wieder die Option eines völkerrechtlichen Vertrages in die Diskussion einbringen, sei der Wunsch unter allen anderen maßgeblichen Akteuren nach einem förmlichen Abkommen eher gering. Allein die Aushandlung einer solchen völkerrechtlichen Vereinbarung würde Jahre in Anspruch nehmen und liefe – mit Blick auf die schnellen technologischen Wandlungsprozesse im IT-Bereich – nach Fertigstellung Gefahr, in kürzester Zeit überholt zu sein. Zudem resultiere das Interesse Russlands und Chinas an einem internationalen Übereinkommen – so die Einschätzung der Expert*innen – vorwiegend dem Begehren Überwachung, Unterbindung von Regierungskritik (insbesondere aus dem Ausland) und staatliche Informationskontrolle verbindlich zu verankern – ein Anliegen, dass von demokratischen Staaten aus verständlichen Gründen abgelehnt wird.

Angesichts dieser Situation würden internationale Cyber-Normen über verantwortliches Verhalten von Staaten im digitalen Raum derzeit die beste Option in puncto Einhegung von Cyberkonflikten darstellen. Hier sind in den vergangenen Jahren durchaus Fortschritte erzielt worden. In diesem Zusammenhang sei besonders der Verhandlungsprozess auf UN-Ebene zu erwähnen – die sog. *United Nations Group of Governmental Experts on Information Security* (UNGGE), die seit 2012 in bisher fünf Runden zu Gesprächen zusammengefunden hat und mittlerweile einen allgemein akzeptierten Konsens an Cyber-Normen erschaffen hat. Entscheidend war hier der Abschlussbericht der dritten UNGGE-Runde aus dem Jahr 2015 in dem elf Cybernormen benannt wurden, die konsensual von der UN-

Vollversammlung verbindlich angenommen wurden und derzeit das wichtigste Rahmenwerk für die Cyber-Diplomatie darstellt. In diesem UN-Dokument sind bspw. Normen zur Kooperation im Falle eines Cyberangriffes, zur Prävention von Cyberkriminalität, zum Schutz von kritischer Infrastruktur und zur gegenseitigen Hilfeleistung im Cybernotfall verankert.

Cyber-Normen sind zwar politisch, nicht aber rechtlich verbindlich. Sie gelten somit nicht als Völkerrecht im engeren Sinne. Die Panelisten betonten jedoch, dass rechtliche Argumentationen in den internationalen Beziehungen grundsätzlich weniger Tragkraft haben als im innerstaatlichen Raum und dass deshalb dem fehlenden völkerrechtlichen Status der Cyber-Normen in der Debatte nicht zu viel Bedeutung beigemessen werden sollte.

Normen entfalten Wirkung und politisches Gewicht, wenn sie eine kritische Masse an Unterstützern haben. Derzeit werden die vereinbarten Cybernormen in vielen Fällen verletzt und ihre allgemeine handlungsleitende Wirkung ist bei Weitem noch nicht erreicht. Aus der Normenforschung ist bekannt, dass dies Jahre und in der Regel sogar Jahrzehnte dauern kann. Das Wissen über den langwierigen Reifungsprozess von Normen und ihre politische Wirkungsweise helfe in der Debatte, die aktuellen Verstöße gegen Cyber-Normen besser einzuordnen und ermahne zu mehr Gelassenheit sowie zur Fokussierung auf eine mittel- und langfristige Zielperspektive – so die Meinung der Expert*innen. Zudem müsse bedacht werden, dass einige Staaten – insbesondere aus dem Globalen Süden – die vereinbarten Cybernormen oftmals aus Mangel an ausreichenden digitalen Kapazitäten nicht befolgen. Diese Art von Normenverstößen müsse anders bewertet werden und unterstreiche vor allem die Bedeutung von *capacity building* als ein wichtiges Begleitinstrument in der Cyberdiplomatie. Ferner sei bei näherer Betrachtung nicht jeder Cyberangriff einen Verstoß gegen die im UN-Rahmen von 2015. So gelten die Cybernormen beispielsweise ausdrücklich nur für Friedenszeiten. Im Kriegsfall fände das normale Kriegsvölkerrecht Anwendung – auch im digitalen Raum. Darüber hinaus stehen bei digitalen Attacken häufig Einrichtungen im Fokus, die nicht als kritische Infrastruktur gelten. Auch hier ist der Bestand der vereinbarten Cybernormen des UN-Rahmens von 2015 nicht berührt und es handelt sich im engeren Sinne nicht um Normenverstöße. Für die lang- und mittelfristige Etablierung von Normen können aber auch Verstöße hilfreich sein, solange diese nicht dominierend sind. So seien Zuwiderhandlungen und vor allem die Gegenreaktionen der Normenunterstützer förderlich damit sich die Gebote und Vorgaben der Cyber-Normen im politischen Bewusstsein verankern und Verhaltensänderungen vorantreiben, so die Einschätzung der Expert*innen.

Ausblick: Vorschläge zur Weiter- und Fortentwicklung der Cybernormen

Trotz dieser Einschränkungen, die hinsichtlich der aktuellen Normenverstöße gemacht werden können, betonten die Panelisten, dass eine Fort- und Weiterentwicklung der Cybernormen dringend erforderlich sei, wenn diese mittel- bis langfristig politische Wirkung entfalten sollen. Die Fortsetzung des Verhandlungsprozesses sowohl auf UN-Ebene als auch in den verschiedenen transnationalen Foren sei hierfür zentral. Zukünftig sei hier vor allem wichtig, die Inklusivität des Prozesses zu erhöhen, so die Einschätzung der teilnehmenden Expert*innen. Schließlich befände sich die digitale Infrastruktur überwiegend in Hand der privaten Tech-Industrie und unterläge nur punktuell staatlicher Hoheit. Neben der industriellen Perspektive sei aber auch die Einbeziehung zivilgesellschaftlicher Akteure entscheidend, weil sie wichtige Lobby-Aufgaben wahrnehmen und gegenüber den jeweiligen Regierungen den Wunsch nach einem sicheren Internet verfechten würden.

Trotz klarer Verbesserungen in den vergangenen Jahren in puncto Inklusivität – wie beispielsweise die Etablierung der Openended Working Group auf an der anders als bei der UNGGE alle UN-

Mitgliedsstaaten teilnehmen können – gäbe es bei der Beteiligung maßgeblicher nicht-staatlicher *stakeholder* im Verhandlungsprozess zu den Cybernormen noch „Luft nach oben“. Hier eine Verbesserung zu erzielen, sei nicht immer einfach insbesondere, weil autokratische Staaten einer stärkeren Mitwirkung privatwirtschaftlicher und zivilgesellschaftlicher Akteure eher ablehnend gegenüberstehen würden. Zielführender sei es daher, in Zukunft an einem engeren Austausch und an einer Harmonisierung zwischen den offiziellen Gesprächen auf UN-Ebene und den verschiedenen informellen Foren zu etablieren, in denen die relevanten nicht-staatlichen Akteure an Fragen der Cyberdiplomatie arbeiten.

Neben der Inklusivität müsse auch die Reaktion gegenüber Normenverstößen verbessert werden. Eine Option, die sich leicht realisieren ließe, bestünde in einer deutlicheren Benennung der Normen, die durch Cyberangriffe verletzt werden. Derzeit sei es so, dass in offiziellen Bekanntmachungen von Cyberattacken viel Information über Art des Angriffs, Schadensumfang und über die mögliche Urheberschaft geliefert wird. Ein Bezug zu den vereinbarten Cyber-Normen, die verletzt worden sind, würde in diesen offiziellen Statements jedoch selten bis nie hergestellt. Laut der Einschätzung der Expert*innen sei dies allerdings ein notwendiger Schritt, wenn die Cybernormen dauerhaft gestärkt werden sollen.

Ferner sei über weitere Maßnahmen nachzudenken, wie besser auf Cyberangriffe reagiert werden könne. Die jüngst etablierte Praxis, nach Cyberangriffen Sanktionen zu verhängen sei ein Schritt in die richtige Richtung, so die Meinung der Panelist*innen. Auch wenn Cyber-bezogene Sanktionen nicht unmittelbar digitale Angriffe unterbinden, so unterstreichen sie doch deutlichen Protest gegen intolerables Verhalten im Cyberraum. Ebenfalls wichtig sei, dass die Verurteilung von Cyberangriffen von einer möglichst großen Gruppe von Staaten erfolge. Zudem solle – neben Sanktionen – das Instrumentarium an Gegenmaßnahmen weiter ausgefeilt werden. Hier sei das „Cyber Diplomacy Toolbox“ der Europäischen Union ein Schritt in die richtige Richtung.

Vertrauensbildende und de-eskaladierende Maßnahmen wurden als weitere wichtige Aspekte von den Expert*innen identifiziert. Sie sollten begleitend zur Stärkung der Cybernormen auf internationaler Ebene stattfinden. In diesem Bereich könne aus den Erfahrungen der Rüstungskontrolle und der Krisendiplomatie gelernt werden. In puncto vertrauensbildende Maßnahmen sei vor allem die Organisation für Zusammenarbeit in Europa (OSZE) interessant, die in diesem Bereich im Cyberraum bereits eine Vorreiterrolle eingenommen habe, aber dennoch über weitere Entwicklungs- und Verbesserungspotenziale verfüge. Zur Vermeidung von zukünftigen Eskalationsdynamiken im digitalen Raum könne bspw. das *Incident at Sea Agreement* interessante Anhaltspunkte liefern. Dieses Abkommen wurde im Kalten Krieg zur Vermeidung von militärischen Zwischenfällen auf Hoher See von der Sowjetunion und den USA abgeschlossen. Sollen in der Zukunft Deeskalationsinstrumente für den Cyberraum entwickelt werden, könne die Analyse dieses Abkommens ein wichtiger Impuls darstellen.

Eine weitere wichtige Zukunftsbaustelle sei die Überprüfung von Cyberangriffen durch eine unabhängige nicht-staatliche Institution. Zahlreiche staatliche Akteure wie auch einige private IT-Sicherheitsfirmen verfügen zwar über leistungsstarke analytische Fähigkeiten und können Cyberattacken mittlerweile relativ gut aufklären. Die öffentliche Identifizierung von Cyberangreifern – insbesondere wenn es sich um rivalisierende Staaten handelt – ist aber weiterhin ein politisch heikler Akt, führt in vielen Fällen zu gegenseitigen Schuldzuschreibungen und zu mangelnder Glaubwürdigkeit. Eine unabhängige nicht-staatliche Körperschaft, die sowohl die Analyse von Cyberangriffen als auch die Identifizierung der Urheberschaft vornimmt, könnte hier Abhilfe schaffen, so die Einschätzung der Expert*innen.

Evangelische Akademie Loccum

Disclaimer

Die in diesem Bericht dargelegten Ergebnisse und Informationen repräsentieren nicht notwendigerweise die Positionen und Meinungen aller Tagungsteilnehmenden und der durch sie vertretenen Institutionen. Der Bericht gibt die wichtigsten Schlussfolgerungen, Themen und Empfehlungen wieder, die während der Tagung erarbeitet wurden. Die reichhaltige und vielseitige Diskussion der dreitägigen Konferenz kann jedoch nicht in vollem Umfang erfasst werden.

Zur Evangelische Akademie Loccum

Die Evangelische Akademie Loccum ermöglicht in jährlich über 80 nationalen und internationalen Veranstaltungen mit bis zu 5000 Teilnehmenden offene und gleichzeitig kritische Begegnungen in gesellschaftspolitischen Debatten. Die Akademie versammelt interdisziplinäre Expertise, kreiert Netzwerke von Akteuren und treibt so tragfähige Lösungen voran. Damit möchte sie die Demokratie in Deutschland stärken und den Frieden bewahren. Die Evangelische Akademie Loccum ist eine Einrichtung der Evangelisch-lutherischen Landeskirche Hannovers und wurde 1946 gegründet.

Kontakt

Dr. Thomas Müller-Färber

Evangelische Akademie Loccum
Münchehäger Str. 6
31547 Rehburg-Loccum

Tel.: + 49 (0) 5766 81-109,
Fax: + 49 (0) 5766 81-900
e-mail: Thomas.Mueller-Faerber@evlka.de
Internet: http://www.loccum.de