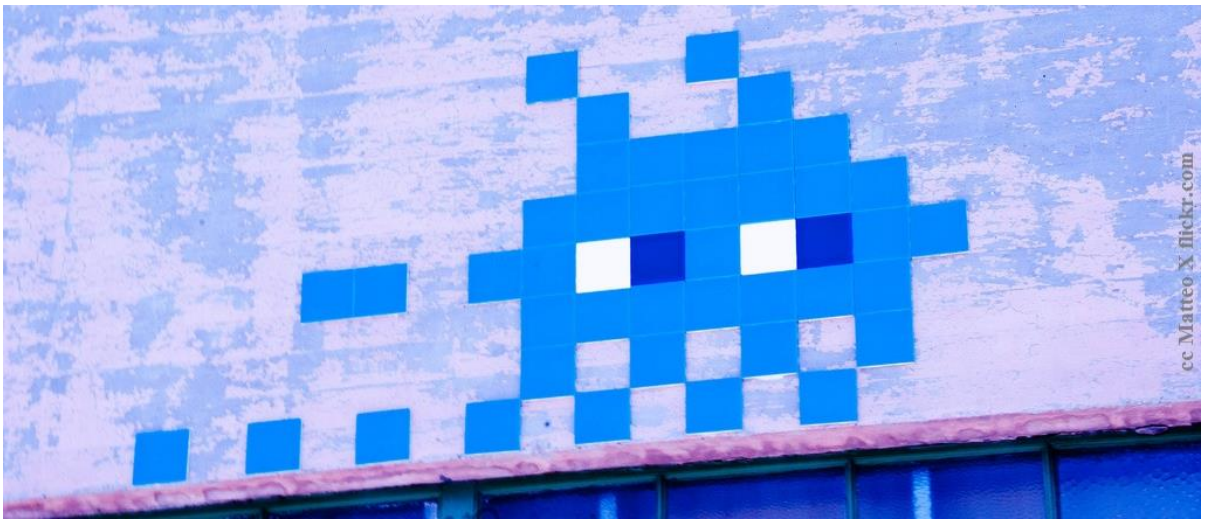
JACQUES DELORS INSTITUT
BERLIN

BLOG POST 16.03.2017

Mehr Sicherheit im Cyberraum

Plädoyer für eine Rüstungskontrolle

Björn Boening
Projektleiter bei der Stiftung Neue Verantwortung
Paul-Jasper Dittrich
Wissenschaftler beim Jacques Delors Institut – Berlin



Fakt ist: Rüstungskontrolle im konventionellen Sinn ist für den Cyberraum derzeit schwierig. Dies bedeutet jedoch nicht, dass eine Cyber-Rüstungskontrolle unmöglich ist. Es wird ein längerer diplomatischer Prozess von Nöten sein. Hierbei ist entscheidend, dass die Debatte über Sicherheit im Cyberraum nicht nur unter IT-Experten geführt und dass internationale Gesprächsformate für die Cybersicherheit gestärkt werden.

Dieser Blog Post ist in im Original am 14.03.2017 als Arbeitspapier Sicherheit Nr. 9 /2017 bei der Bundesakademie für Sicherheitspolitik (BAKS) erschienen.

Pariser Platz 6
D – 10117 Berlin
Tel.: +49 (0)30 467 26 09 – 01

Online: delorsinstitut.de
E-Mail: office@delorsinstitut.de
Twitter: @delorsinstitut

1 Der Cyberraum ist ein unwegsames Terrain

Im November 2016 hat das Bundesamt für Sicherheit in der Informationstechnik seinen jährlichen Lagebericht zur Cybersicherheit veröffentlicht. Daraus geht hervor, dass täglich etwa 20 hochspezialisierte Angriffe auf die Netzwerke der Bundesregierung stattfinden. Auch deutsche Großkonzerne, wie etwa die Telekom, Volkswagen oder ThyssenKrupp beklagen täglich mehrere solcher Angriffe. Dieser Befund wirft zwei wichtige Fragen auf: Warum ist der Cyberraum für Staaten so schwierig zu kontrollieren und wie können Staaten gegen die Bedrohungen aus dem Netz international zusammenarbeiten?

Ein Blick auf die Struktur des Cyberraums und die beteiligten Akteure zeigt, dass gemeinsam akzeptierte Verfahren und Standards – sozusagen eine Cyber-Rüstungskontrolle – nötig wären, um mehr Sicherheit in diesem vergleichsweise wenig reglementierten Raum zu erlangen. Bereits im vergangenen August rief der damalige deutsche Außenminister Frank-Walter Steinmeier zu einem Neustart der konventionellen Rüstungskontrolle auf. Dabei erwähnte er ausdrücklich „offensive Cyberfähigkeiten“ als neue Technologie, die erhebliche Gefahren berge. Es bedürfe internationaler Zusammenarbeit, um diesen neuen Gefahren zu begegnen. Der Cyberraum weist jedoch einige besondere technische Merkmale auf, die eine internationale sicherheitspolitische Zusammenarbeit erschweren.

Die Schwierigkeit der Kontrolle im Cyberraum beginnt mit der Architektur der Netzwerke, insbesondere seiner Größe und Anzahl der Nutzer. Vor etwa 50 Jahren haben Wissenschaftler in den USA und Europa erstmals zwei Computer miteinander verbunden und damit die ersten Computernetzwerke aufgebaut. Die Netzwerke wurden rasch größer und stabiler und ermöglichten es, Informationen jeder Art in bisher unbekannter Geschwindigkeit und über nahezu alle politischen Grenzen hinweg auszutauschen. Die Aufgabe von Computern änderte sich dadurch fundamental vom Rechnen hin zum Austausch und der Verwaltung von Informationen.

Man könnte überspitzt sagen seitdem habe sich grundlegend nicht viel geändert. Auch heute lassen sich über das Internet Informationen speichern und teilen. Der Unterschied zwischen den frühen Netzwerken der Sechzigerjahre und der heutigen Netzwerkarchitektur besteht im Wesentlichen in dem stetigen Wachstum der Informationsflüsse (Datenvolumen) und der Anzahl der Nutzer und Geräte (Knotenpunkte) im Netzwerk. Im Jahr 2016 waren etwa 3,2 Milliarden Menschen weltweit, oder fast die Hälfte der Menschheit, mit dem Internet verbunden. Doch auch ohne den Menschen verbinden sich immer mehr Geräte mit dem Internet, um Informationen untereinander auszutauschen, zum Beispiel Überwachungskameras, Autos oder Haushaltsgeräte. Die Anzahl der mit dem Internet verbundenen Geräte hat in 2016 laut verschiedener Studien etwa sieben Milliarden erreicht. Durch das sich entwickelnde

sogenannte Internet der Dinge könnte es laut einiger Prognosen bis 2020 bereits um die 20 Milliarden vernetzte Geräte geben.

Je größer und unwegsamer ein zu verteidigendes Territorium ist, umso schwieriger ist es, dieses vor Angriffen zu schützen. Dieser Grundsatz gilt auch für den digitalen Raum: Je mehr Informationen in Netzwerken gespeichert werden, desto größer ist der Anreiz, hier nach sensiblen Informationen zu suchen. Immer größer und komplexer werdende Netzwerke machen es Angreifern oft leichter, eine Sicherheitslücke zu finden.

Vollständige staatliche Kontrolle ist utopisch

De facto kann kein Staat den Cyberraum vollständig kontrollieren – weder technisch noch politisch. Neben der schieren Größe des Cyberraums hat dies im Wesentlichen drei Gründe. Diese sind erstens die dynamische Architektur der Netzwerke, zweitens die Zusammensetzung der beteiligten Akteure und drittens die nicht zweifelsfrei mögliche Zuordnung (Attribution) der Angriffe zu den Akteuren.

Die dynamische Architektur der Netzwerke beruht auf einem Paradigmenwechsel in der Telekommunikation. Im Gegensatz zur klassischen Telefonie basieren Netzwerke heute auf der sogenannten Paketvermittlung. Eine E-Mail wird nicht als Ganzes durch das Netz geschickt, sondern in kleine Datenpakete zerlegt, die mit Adresse und Absender versehen sind. Erst beim Adressaten werden diese Pakete wieder zusammengesetzt. Die einzelnen Pakete können dabei unterschiedliche Wege gehen, um zum Adressaten zu gelangen. Diese dezentrale Struktur erlaubt hohe Flexibilität und Resilienz. Gleichzeitig bedeutet es einen erheblichen Aufwand, den Inhalt der Pakete und ihre Routen zu kontrollieren. Nur wenige Firmen oder staatliche Einrichtungen sind hierzu in der Lage.

Das zweite Problem ist, dass der Staat im Cyberraum nur einer von vielen Akteuren ist. Ein Großteil der physischen Infrastruktur des Internets besteht aus den Telekommunikationsnetzen innerhalb der einzelnen Staaten. Im Zuge der Verbreitung der Telefonie und später des Mobilfunks wurde in vielen Ländern eine umfassende Infrastruktur aufgebaut, welche heute meist von privaten Akteuren, den sogenannten Internet Service Providern, für den Datenverkehr genutzt wird. Sie verwalten die Datenströme innerhalb ihres eigenen Netzwerks und leiten die Pakete an andere Netzwerke weiter (Routing). Die Verbindung zweier oder mehrerer privater Netzwerke unterliegt in den meisten Staaten allerdings der Vertragsfreiheit und geschieht wenig transparent. Innerhalb seines Territoriums kann jeder Staat zwar Regeln für die Nutzung seiner Netze aufstellen, sofern er dies wünscht. Sobald aber Datenpakete an ein Netzwerk außerhalb des Staatsgebiets geleitet werden, also der Anschluss an das globale Netz geschieht, ist die Staatsgewalt eingeschränkt.

Selbst wenn ein Staat in der Lage wäre, die Dynamik der riesigen Datenströme zu überblicken und die Zugänge zu seinem regionalen „Internet-Anteil“ zu kontrollieren, indem er beispielsweise die Netzwerke verstaatlicht, gibt es bisher dennoch keine Möglichkeit, alle Teilnehmer im Netzwerk vor Schadsoftware effektiv zu schützen. Ein konkretes Beispiel dafür ist der „chinesische Teil“ des Internets. Es wird angenommen, dass chinesische Behörden in der Lage sind, den Großteil ihrer regionalen Netzwerkinfrastruktur zu überwachen, zum Beispiel die Zu- und Abgänge („The Great Firewall“). Gleichzeitig jedoch ist China das Land mit den meisten von Viren befallenen Computern weltweit. Bis zu 70 Prozent der Systeme werden mit raubkopierter Software betrieben, welche keine Sicherheitsupdates erhalten – ein gefundenes Fressen für jeden Angreifer.

Eine dritte Besonderheit im Cyberraum erschwert es den Staaten, dort ihr Gewaltmonopol auszuüben. Im Gegensatz zu konventionellen Waffen ist die Zuordnung (Attribution) von digitalen Angriffen zu einem Akteur schwierig. Es gibt im Gegensatz zur physischen Welt keine eindeutigen forensischen Anhaltspunkte, wie etwa eine bestimmte Munitionsart oder Satellitenaufnahmen, die einen Raketenstart dokumentieren. Spuren eines Angriffs zu verwischen, oder die Behörden auf eine falsche Fährte hinsichtlich der Identität des Angreifers zu locken (False Flag) gelingt deshalb bereits mit erstaunlich einfachen Mitteln.

2 Das weltweite Wettrüsten hat längst begonnen

Was also kann ein Staat tun, um im Cyberraum Kontrolle zu erlangen und Bedrohungen effektiv abzuwenden? Er kann sich zunächst besser rüsten. Wichtig ist dabei die Unterscheidung in defensive und offensive Cyberfähigkeiten. Für mehr Sicherheit in der Netzinfrastruktur sind in der Regel Investitionen in defensive Maßnahmen sinnvoll und nötig. Es ist jedoch bekannt, dass viele Staaten auch offensive Fähigkeiten (Cyberwaffen) entwickeln. Der ehemalige US-Präsident Barack Obama hat schon 2009 den Auftakt zu einem digitalen Wettrüsten gegeben. In einer Pressekonferenz im Weißen Haus sagte er, dass „Cyber-Sicherheitsrisiken zu den schwerwiegendsten Bedrohungen für die wirtschaftliche und nationale Sicherheit im 21. Jahrhundert“ gehören. Seitdem haben allein die USA etwa 60 Milliarden Dollar in ihre defensiven und offensiven Cyberfähigkeiten investiert.

Zahlreiche Regierungen haben diese Position übernommen und investieren ihrerseits großzügig in Rüstungsvorhaben für die Cyberdomäne. Im vergangenen Jahr hat beispielsweise Großbritannien angekündigt, zwei Milliarden Euro in Cybersicherheitsprogramme zu investieren; Frankreich, die Vereinigten Arabischen Emirate und Australien planen mit jeweils etwa einer Milliarde. Auch die Bundesregierung hat im vergangenen Jahr den Aufbau einer Reihe neuer Einrichtungen angekündigt. So ist etwa für die Bundeswehr eine zentralisierte Cyber-Abteilung mit etwa 13.500 Stellen (davon jedoch nur 300 Neueinstellungen) geplant, und

auch zivile Behörden insbesondere im Geschäftsbereich des Bundesinnenministeriums werden mit zahlreichen neuen Stellen und Fähigkeiten ausgestattet.

Viele Staaten geben dabei vor, lediglich in Maßnahmen zur Abwehr von Bedrohungen zu investieren. Sicher ist jedoch, dass die anfangs genannten 20 hochspezialisierten Angriffe auf deutsche Regierungsnetzwerke nicht nur durch einzelne private Hacker geschehen. Ein spezialisierter Angriff erfordert erhebliche Ressourcen und ein Team mit vielseitiger Expertise. Das Bundesamt für Sicherheit in der Informationstechnik geht in seinem Bericht deshalb davon aus, dass etwa fünf der täglichen Angriffe einen nachrichtendienstlichen Hintergrund haben, also durch andere Staaten initiiert wurden.

Cyberwaffen sind der neue Standard

Das aktuell eifrige Aufrüsten der Staaten im Cyberraum wurde mehrmals mit der Situation zu Beginn des atomaren Wettrüstens verglichen. Der ehemalige Direktor der CIA und der NSA Michael Hayden zieht sogar Parallelen zwischen dem Abwurf der US-Atombombe über Hiroshima im August 1945 und dem Einsatz des Computervirus Stuxnet durch CIA und NSA zur Lahmlegung des iranischen Atomprogramms. In beiden Fällen gelte, so Hayden: „Wenn Amerikaner eine neue Waffe benutzen, dann weiß der Rest der Welt, dies ist der neue Standard. Andere fühlen sich legitimiert, Cyberwaffen zu entwickeln und einzusetzen. Es fehlt an Einsatzregeln sowie internationalen Normen und Standards“.

Das Kriegsvölkerrecht entstand in einer Zeit, in der Waffen noch rein auf ihr physisches Zerstörungspotential hin gedacht wurden. Cyberangriffe müssen jedoch nicht zwangsläufig in einer physischen Zerstörung enden. Wie weit können wir gehen, bevor etwas als ein Angriff definiert wird? „Die derzeitige Norm ist: Tu alles womit du davon kommst“, fasst ein ehemaliger Angehöriger des US-Cyberkommandos die derzeit vorherrschende Auffassung zusammen. Dieses Problem wird anhand eines Beispiels deutlich. Im Jahr 2007 sorgten russische Hackergruppen dafür, dass estnische Regierungswebseiten für einige Tage nicht erreichbar waren. Die estnische Regierung sah sich angegriffen und bat bei ihren NATO-Verbündeten um Unterstützung. Die Frage, ob dieser Fall bereits einen Angriff im klassischen Sinne darstellt, bleibt international umstritten.

Cyber-Rüstungskontrolle: Der Anfang ist schwierig

Wettrüsten, auch im Cyberraum, ist langfristig ein Nullsummenspiel. Um dem zu entgehen, sollte gegenseitiges Vertrauen aufgebaut werden. Die Geschichte zeigt: Bevor es gemeinsame Regeln, ein Abkommen oder sogar einen Rüstungskontrollvertrag gibt, müssen zu Beginn grundsätzliche Definitionen gefunden werden, zum Beispiel darüber, was einen Angriff im Cyberraum konstituiert. Gerade dieser Vorgang erweist sich jedoch als politisch besonders

schwierig, da viele Akteure sich unterschiedlich bedroht fühlen. Gegenwärtig arbeiten verschiedene Gruppen, zum Beispiel bei den Vereinten Nationen oder der OSZE an Definitionen für das Agieren staatlicher und nichtstaatlicher Akteure im Cyberraum. Sollte ein politischer Konsens für eine Definition ausbleiben, könnten IT-Experten zumindest technische Definitionen und Standards etablieren. Die Definitionsprobleme zeigen sich etwa beim 2013 vorgelegten sogenannten Tallinn Manual der NATO. Darin werden Cyberangriffe als „cyber activities that proximately result in death, injury, or significant destruction" definiert. Nach Ansicht einiger Fachleute greift diese Definition jedoch zu kurz. Entscheidende Merkmale von Cyberangriffen seien nicht ausreichend berücksichtigt. So erfolgten viele Angriffe indirekt, zeitverzögert oder über die Manipulation von Teilsystemen, sodass ein Angreifer nur selten einwandfrei identifiziert und zugeordnet werden kann.

Selbst wenn man sich auf eine Definition einigt und den Angreifer aufspüren kann, bleibt unklar, wie mit dem Täter umzugehen ist. Ist der Angreifer ein Kombattant nach dem Kriegsvölkerrecht oder ist er ein Zivilist, der nach strafrechtlichen Gesichtspunkten zur Rechenschaft gezogen werden muss? Man darf davon ausgehen, dass staatliche Stellen bisweilen unter dem Deckmantel der Kriminalität agieren, um die ungewisse Situation zu ihrem Vorteil auszunutzen und dabei ihre Spuren zu verwischen. Diese und viele weitere offenen Fragen zeigen, dass wir uns noch ganz am Anfang eines langen Prozesses zur Errichtung eines Cyber-Rüstungskontrollregimes befinden. Bei der Kontrolle des Handels mit Cyberwaffen gibt es bereits erste konkrete Lösungen für vertiefte Zusammenarbeit: So wurde das 1995 abgeschlossene WassenaarAbkommen, das der Exportkontrolle von konventionellen Waffen und dual use-Gütern dient, 2013 um Software, mit der in IT-Systeme eingedrungen werden kann (Intrusion Software), erweitert. International anerkannte Definitionen bleiben dennoch der Schlüssel, um weitere Verhandlungen zu ermöglichen.

3 Die EU als Vorbild und Versuchslabor

Eins muss klar sein: Das Ziel ist nicht, dass nie wieder eine Cyberwaffe eingesetzt wird. Auch andere Rüstungskontrollregime werden immer wieder herausgefordert, wie die kürzlich erfolgten Raketentests im Iran und in Nordkorea gezeigt haben. Gemeinsame Regeln oder gar ein internationales Abkommen zur Regulierung des Cyberraums sowie eine fortgeschrittene Kollaboration im Kampf gegen die Verbreitung von Schadsoftware werden vermutlich eher Schlusspunkt einer längeren diplomatisch-politischen sowie technischen Anstrengung sein. Es gibt kein Patentrezept dafür, wie Rüstungskontrolle im Cyberraum entsteht. Im Moment geht es vor allem darum, konsensfähige Prozesse und Gesprächsrahmen zu entwickeln, um erste Definitionen und Standards zu entwickeln. Folgende Schritte sind hierbei wichtig:

Erstens müssen Entscheidungsträger für die zuvor beschriebenen technischen Besonderheiten im Cyberraum sensibilisiert werden. Nur mit einem grundlegenden Verständnis können

gemeinsame sicherheitspolitische Interessen im Cyberraum definiert werden, um einen Anfang für eine Rüstungskontrolle zu schaffen. So müssen viele Regierungen beispielsweise zunächst einsehen, dass sie durch die bereits weit voran geschrittene Vernetzung, insbesondere ihrer kritischen Infrastruktur, für Cyberangriffe verwundbar sind und daher ein vitales Interesse an internationaler Kooperation haben sollten. Eng damit verbunden ist die dringende Notwendigkeit, die Debatte über Cybersicherheit nicht nur in IT-Fachkreisen, sondern in der breiten Öffentlichkeit zu führen.

Folglich kann zweitens aufgrund des transnationalen Charakters des Cyberraums nur auf internationaler Ebene ein Dialog über Cybersicherheit und Rüstungskontrolle geführt werden. Diese Themen gehören in möglichst vielen internationalen Gremien auf die Tagesordnung. Neben der OSZE und den Vereinten Nationen könnte auch die G20 einen internationalen Gesprächsrahmen bieten. In diesen Gremien können beispielsweise politische Interessen im Cyberraum definiert und diplomatische Handlungsspielräume genutzt werden, um allmählich ein gemeinsames Verständnis über Bedrohungen im Cyberraum zu entwickeln.

Drittens können in regionalen Zusammenschlüssen von Staaten konkrete Definitionen und Schutzmechanismen entwickelt werden, die globalen Modellcharakter haben. Hierbei könnten Deutschland und die Europäische Union eine entscheidende Rolle spielen. Die EU versteht sich gemeinhin als Exporteur von Normen und Standards, beispielsweise beim Datenschutz. So hofft die Europäische Union etwa, dass das in der EU-Datenschutzgrundverordnung entwickelte, sehr weit gefasste Verständnis vom Schutz personenbezogener Daten weltweit Nachahmer findet. Das könnte auch in sicherheitspolitischen Bereichen gelingen. Im Bereich der Cybersicherheit ist die EU bereits tätig: Die 2016 verabschiedete Richtlinie für Netzwerks- und Informationssicherheit (NIS) hat europaweit Mindeststandards für Netzwerksicherheit und für viele Unternehmen (zum Beispiel Suchmaschinen) eine Meldepflicht von Hackerangriffen eingeführt. Außerdem wird eine strategische europäische „Kooperationsgruppe“ geschaffen, um Informationen zwischen den Mitgliedstaaten auszutauschen und gegenseitige Unterstützung beim Aufbau von nationalen Kapazitäten zur Cybersicherheit zu gewährleisten. Besonders die Meldepflicht für Cybervorfälle, zum Beispiel von Angriffen auf kritische Infrastruktur oder sensible Daten, gilt als ein erster wichtiger Schritt zur besseren Koordinierung und Wissensweitergabe unter den Mitgliedstaaten und findet weltweit Beachtung. Die Kooperation innerhalb der EU könnte langfristig Vorbild und Versuchslabor für internationale Kooperation und vertrauensbildende Maßnahmen auf dem Weg zu mehr Sicherheit im Cyberraum sein.