Cyberkrieg, Cyberterror, Cyberspionage und Cyberkriminalität:

Wenn das Internet zur Bedrohung der nationalen Sicherheit wird

Alexander Niedermeier

Alexander Niedermeier ist Wissenschaftlicher Mitarbeiter am Institut für Politische Wissenschaft der Universität Erlangen. Er befasst sich mit der Theorie der Internationalen Beziehungen sowie mit Internationalen Sicherheitsstudien, Politischer Psychologie und Entscheidungstheorie sowie dem Nahen Osten.

Zusammenfassung
Der vorliegende Beitrag befasst sich mit den vielfältigen Gefahren für die nationale Sicherheit, die in Verbindung mit dem Internet stehen. Neben zwischenstaatlichen Konflikten in Form von Cyberkriegen und der Bedrohung gesellschaftswichtiger computerbasierter Infrastrukturen durch Cyberterroristen befasst sich der Artikel mit gegen Staaten wie die Privatwirtschaft gerichteter Spionage durch das Internet sowie mit der vom transnationalen organisierten Verbrechen ausgehenden Cyberkriminalität. Dabei werden die konkreten Bedrohungen für die Sicherheit von Staat, Gesellschaft, Wirtschaft und Einzelbürger aufgezeigt, grundlegende technische Zusammenhänge erläutert und dargelegt, wie geeignete Ansätze aussehen, auf die dargestellten Herausforderungen zu reagieren.

1. Einführung

Trojaner auf PCs im Kanzleramt, Al-Qaida auf dem Weg in den Cyberspace, Cyberangriffe auf den Iran und Wenn Chinas Armee ihre Trojaner schickt – Meldungen wie diese lassen sich seit geraumer Zeit immer häufiger auf den Titelseiten unserer Gazetten finden. Da ist von *Stuxnet* und *Flame* die Rede, von *SCADA*, *Botnetzen* und *Cyber Jihad*. So allgegenwärtig das Internet heute geworden ist, so unersetzbar für unseren privaten wie geschäftlichen Alltag, so wenig ist sich die Mehrheit der Bevölkerung der Bedrohungen bewusst, die mit der alle Ebenen unserer modernen Gesellschaft durchdringenden Vernetzung verbunden sind. Hier und da liest man eine Meldung, stößt auf einen Begriff, der oft kryptisch anmutet und den man mal mehr, mal weniger versteht oder einordnen kann. Am Ende bleibt zumeist das Gesamtbild unklar. Und doch scheint man nicht mehr umherzukommen, sich all jenen die nationale Sicherheit betreffenden Begriffen zu nähern, die an sich vertraut erscheinen, wie Krieg, Terrorismus, Spionage, Kriminalität, die aber durch die neue Vorsilbe „Cyber-“ ganz neue Herausforderungen mit sich bringen.

Vor diesem Hintergrund soll es hier Ziel sein, zunächst einige grundsätzliche Anmerkungen zur Frage von Sicherheit und Bedrohung im Cyberspace zu machen, anschließend die Bereiche Cyberkrieg, Cyberterrorismus und Cyber-

spionage zu erörtern und dabei auch auf die Bedeutung von kritischen Infrastrukturen einzugehen. Schließlich soll noch der Bereich der organisierten Cyberkriminalität dargestellt und in den Kontext der drei anderen Bedrohungsarten gestellt werden. Hierauf aufbauend soll sich schließlich der Frage genähert werden, wie den Bedrohungen aus dem Cyberspace entgegengetreten werden kann.

2. Sicherheit und Bedrohung im Cyberspace

Bedrohungen aus dem Cyberspace sind zu einer neuen, handfesten Dimension der nationalen Sicherheit geworden. Ein wesentlicher Faktor hierfür ist, dass das Internet ursprünglich nicht für seine heutige Nutzung geplant wurde und noch immer nicht dafür ausgelegt ist. Diente es ursprünglich der Datenübertragung zwischen einer kleinen Anzahl streng geschützter Computersysteme, zunächst des Militärs, später auch ausgewählter Hochschulen, so wurde es seit den 1990ern in großem Stil zu einer zentralen Komponente der modernen Dienstleistungs- und Industriegesellschaft. Während die kommerzielle Nutzung in den Vordergrund trat blieb die Sicherheit auf der Strecke, wofür kurzfristige Profitinteressen ebenso verantwortlich zeichnen wie kompromittierte Bauteile und nicht zuletzt die Nachlässigkeit zahlloser Benutzer, die unrechtmäßig erworbene Software verwenden und so keine Updates erhalten oder solche schlichtweg verweigern. Gleichzeitig ist den wenigsten Menschen bewusst, wie weit das Internet in ihren Alltag hineinreicht, auch wenn sie nicht selbst vor dem Rechner sitzen. Von Ampeln, Aufzügen und Fotokopierern bis hin zur Aufbereitung von Trinkwasser und der Erzeugung von Elektrizität reicht die Abhängigkeit vom Internet; von Telekommunikation, Zug- und Luftverkehr ganz zu schweigen.

kommerzielle Nutzung

Terrorangriff

Die Vorstellung eines Terrorangriffs wird zwar im Alltag regelmäßig verdrängt, ist aber spätestens seit dem 11. September 2001 ein realistisches Szenario. Doch war 9-11 trotz seines Ausmaßes, der zahlreichen Opfer und der kollektiven Traumatisierung der USA und des Westens ein begrenztes Ereignis. Ein Cyber-Angriff auf die lebenswichtigen Infrastrukturen eines Landes indes kann sich weitaus verheerender auf den Alltag auswirken und das Leben, so wie es Millionen Menschen kennen, für Tage, Wochen oder gar Monate radikal verändern. Denn ein Leben ohne Strom wäre, wie es ein Experte der US-Regierung einmal ausgedrückt hat, kein Rückfall in die Mitte des 20. Jahrhunderts, die Zeit vor dem Internet, sondern vielmehr in die Mitte des 19. Jahrhunderts, nämlich die Ära vor der Elektrizität – und das mit allen Konsequenzen. Unvorstellbar? Vielleicht. Unrealistisch dagegen ist diese Gefahr nicht. Mag die Cyberwelt auch Sache hochspezialisierter Computerexperten sein, die Konsequenzen ihrer Handlungen sind Sache eines jeden von uns – und auch die Möglichkeiten, an der Vorbeugung gegen die Bedrohungen der nationalen Sicherheit aus dem Cyberspace mitzuwirken. Um dieses Bewusstsein zu entwickeln ist nicht zuletzt auch ein höheres Maß an Wissen um Art, Umfang und Wirkungsweisen unterschiedlicher Cyberbedrohungen notwendig. Nachfolgend sollen daher die Dimensionen Cyberkrieg, Cyberterrorismus, Cyberspio-

lebenswichtige Infrastrukturen

nage und organisierte Cyberkriminalität analysiert und ihre Implikationen beziehungsweise Möglichkeiten, damit umzugehen, aufgezeigt werden.

3. Cyberkrieg: Die fünfte Dimension zwischenstaatlicher Konflikte

bewaffnete Konflikte

Unter Cyberkrieg wird die fünfte Dimension zwischenstaatlicher bewaffneter Konflikte verstanden. Diese tritt neben die Bereiche der Land-, See-, Luft- und Weltraumverteidigung. Auch wenn lange Zeit von offizieller Seite unterschätzt, zeigt sich die militärische Bedeutung mittlerweile nicht zuletzt darin, dass etwa in den USA neben einem zentralen Cyber-Command auch alle Waffengattungen eigene Cyber-Kommandostrukturen eingerichtet haben. Die US-Marine hat sogar eine eigene Flotte gegründet, die zwar über keine Schiffe, aber über ein hohes Maß an Expertise für den Cyberkrieg verfügt. Und diese Kompetenz ist auch nötig, um auf die Bedrohungen zu reagieren, welche paradoxerweise erst durch eine Entwicklung hervorgerufen wurden, die auf Jahre hinaus die Überlegenheit der westlichen Streitkräfte sichern sollte: das vernetzte Schlachtfeld. Basierend auf computergestützten, integrierten und interoperablen Waffensystemen sollte ein nie gekanntes Maß an Zusammenwirken einzelner Waffengattungen und -systemen und somit höchste militärische Effizienz erreicht werden. Jedoch zeigte sich bald, dass just in jener enormen Abhängigkeit von Computerisierung und Netzwerken die Achillesverse der modernen Kriegführung liegt. Mittlerweile ist die wichtigste Person, die es bei einem Angriff auf eine Militäreinrichtung zu finden und auszuschalten gilt, der Systemadministrator, nicht mehr der Kommandeur, wie es ein hoher Offizier der US-Streitkräfte einmal ausdrückte.

computergestützte Waffensysteme

Und in der Tat ist das Störpotenzial enorm. Durch das Eindringen in militärische Netzwerke lassen sich Überwachungs- und Leitsysteme manipulieren. In der Folge erscheinen keine Kampfflugzeuge, Drohnen oder Raketen mehr auf den Radarschirmen der Verteidiger, obgleich sich solche im Anflug befinden – so geschehen als Israels Luftwaffe 2007 unbehelligt Ziele in Syrien angreifen konnte – oder aber Lenkflugkörper erhalten durch die Eingabe des Gegners den Befehl, Ziele des Angreifers selbst zu attackieren. Ein wesentlicher Effekt hierbei ist zudem die Verwirrung und daraus resultierende Verunsicherung des Gegners, weil unter Umständen davon ausgegangen werden muss, dass die angezeigte Lage eigener oder gegnerischer Schiffe, Flugzeuge etc. oder gar die eigene Position nicht der tatsächlichen entspricht. Neben dieser Art der Manipulation ist auch die gänzliche Ausschaltung von Waffensystemen oder die vollständige Unterbrechung der Kommunikationsstrukturen des Gegners möglich.

Unterbrechung der Kommunikationsstrukturen

Besonders fatal ist auch, dass sich das Kräfteverhältnis von Staaten durch den Cyberkrieg stark verschieben kann und gerade rückständige, oft politisch instabile Staaten, deren Infrastruktur nur mäßig entwickelt ist, erhebliche relative Vorteile erlangen können, da sie, wenn sie genug in offensive Cyberkapazitäten investieren, den Gegner lähmen können, bevor er sein volles Potenzial

entfalten kann, während sie aufgrund ihrer eigenen geringen Vernetzung nur sehr bedingt verwundbar sind. Hierbei gilt zu beachten, dass der Aufbau offensiver Cyberkapazitäten signifikant billiger ist als die Rüstung im kinetischen Bereich, sei es konventionell oder gar nicht-konventionell. So geht die Bemerkung eines nicht genannt werden wollenden Experten etwa dahin, dass die Kosten für den Aufbau des japanischen Cyberprogramms in etwa so hoch seien wie die Rundungsfehler bei herkömmlichen Raketenprogrammen. Vor diesem Hintergrund leuchtet auch ein, dass die Etablierung der Cyberkriegsführung zugleich auch eine nicht unwesentliche Gefahr der Konflikteskalation mit sich gebracht hat. Denn die Gefahr, dass ein im kinetischen Bereich unterlegener Angreifer durch einen elektronischen Erstschlag die Schlagkraft des defensiven Gegners stark dezimieren kann, kann einen sich bedroht fühlenden Verteidiger zu vorschnellen Offensivhandlungen veranlassen. Dies gilt umso mehr, wenn man sich das oben erwähnte Problem der potenziellen Unsicherheit der zur Verfügung stehenden handlungsleitenden Informationen vor Augen führt, die dem ohnehin unter Druck stehenden Entscheider zur Verfügung stehen.

offensive Cyberkapazitäten billiger

Doch sind es keineswegs nur militärische Systeme und Einrichtungen die im Rahmen von Cyberkriegführung attackiert werden. Vielmehr geht es gerade auch um kritische zivile Infrastrukturen. Diese sind omnipräsent, bilden das unverzichtbare Rückgrat moderner Gesellschaften – und sind in höchstem Maße empfindlich für potenzielle Attacken aus dem Internet. Dies macht sie sowohl für staatliche Cybersoldaten als auch für Cyberterroristen zu bevorzugten Angriffszielen.

kritische zivile Infrastrukturen

4. Cyberkrieg, Cyberterrorismus und das Problem der kritischen Infrastrukturen

Alltagsgesellschaft

Das Schlachtfeld ist somit unsere Alltagsgesellschaft, die bis in nahezu jede nur erdenkliche Kleinigkeit direkt oder indirekt von einem funktionierenden Netzwerk und funktionierenden untergeordneten Systemen und Geräten abhängt, die ihrerseits computergesteuert sind. Die heutige Gesellschaften stützenden und letztlich erst ermöglichenden Kernbestandteile werden als kritische Infrastrukturen bezeichnet. Diese umfassen die Erzeugung, Übertragung und Verteilung von Elektrizität, Öl, Gas, Telekommunikation, Wasseraufbereitung sowie Ver-/Entsorgung, Nahrungsmittel, Heizung, das Gesundheits- sowie das Transportwesen zu Lande, zu Wasser und in der Luft, das Finanzwesen und das öffentliche Sicherheitswesen. Bevorzugtes Ziel für Cyberangriffe sind die jeweiligen Steuerungssysteme (sog. SCADA), die aus Kosten- und Effizienzgründen bewusst auf Interoperabilität hin ausgelegt sind, was sie noch mehr in die globale Netzwerkstruktur einbindet und somit noch verwundbarer macht. Beispiele vorsätzlich oder ungewollt herbeigeführter SCADA-Zwischenfälle haben sich schon in allen Bereichen der kritischen Infrastruktur ereignet. So sind Pipelines explodiert, in Kalifornien wegen eines Softwarefehlers, in Russland als Folge eines gezielten Cyberangriffs. In Atomanlagen des Iran

SCADA

wurde das Stuxnet-Virus eingeschleust, das die Zentrifugen zur Urananreicherung zerstörte. 2008 kam es durch ein Virus im Kontrollsystem der Luftraumüberwachung zu einem Flugzeugabsturz in Spanien. Ein als Sicherheitstest durchgeführtes Eindringen in das SCADA-System der Kraftstoffbunkertanks einer kanadischen Raffinerie – nur mit Laptop und Standardhackerwerkzeugen, wie sie problemlos im Internet zu bekommen sind – zeigte, dass unbemerkt Manipulationen durchgeführt werden konnten, durch welche die gesamte Anlage hätte zerstört werden können. Die Liste derartiger Beispiele ließe sich endlos fortsetzen und die immensen Schäden, die durch das Eindringen in Atom- oder Chemieanlagen, Staudämme etc. angerichtet werden können, sind enorm, nicht zuletzt wenn man noch berücksichtigt, dass ein Angriff auf ein Element der kritischen Infrastruktur kaskadisierende Effekte haben kann (vgl. Verton 2003: 21f, 35). Die Stromausfälle vom 14. August 2003 an der amerikanischen Ostküste, bei denen bis heute umstritten ist, ob sie die Folge einer Cyberattacke oder „nur" auf ein Naturereignis zurückzuführen waren, lösten eine Kettenreaktion aus, deren Folgeschaden auf bis zu 10 Milliarden US-Dollar beziffert wurde.

Stuxnet-Virus

Ein weiteres Problem ist, dass die meisten kritischen Infrastrukturen in privater Hand liegen und das dortige Interesse an nationaler Sicherheit in dem Maße abnimmt, wie es die private Seite Geld kostet und somit den Profitinteressen entgegensteht. Da Maßnahmen zur Cybersicherheit in Unternehmen äußerst kostspielig sind und weit über die bloße Errichtung von Firewalls hinausgehen, sind viele Unternehmen geneigt, den Schutz zu minimieren.

Infrastrukturen in privater Hand

Erstmals in der Geschichte liegt die nationale Sicherheit zu einem bedeutenden Teil mit in den Händen zahlloser Privatunternehmen, denen es aufgrund des Zögerns der Regierungen, gesetzliche Vorschriften für die Betreiber kritischer Infrastrukturen zu erlassen, allein obliegt, die erforderlichen Sicherheitsmaßnahmen zu ergreifen. Von besonderer Tragweite wirkt sich das im Bereich der Energiewirtschaft aus. Das Stromnetz gilt als Herzstück der modernen Gesellschaft. Aus Gründen des kostengünstigen und effizienten Betriebs ist es ans Internet angeschlossen. John McClelland, Direktor der amerikanischen Energiebehörde FERC, die für die Überwachung der Stromnetze zuständig ist, hat schon mehrfach vor der immensen Bedrohung von Cyberattacken gewarnt, und auch ein vielfaches Eindringen in die Steuerungsnetze wurde bislang nachgewiesen. Dennoch haben die Behörden größte Mühen, die Stromversorger dazu zu bringen, ihre Netze besser zu sichern. Der ehemalige CIA-Direktor und jetzige Verteidigungsminister Panetta sprach daher in diesem Zusammenhang bei seinem Confirmation Hearing am 9. Juni 2011 im Senat nicht grundlos vom nächsten Pearl Harbor.

Energiewirtschaft

Ein solches könnte dabei ebenso gut von feindlich gesinnten Staaten wie auch von Cyberterroristen ausgelöst werden. Denn auch deren Ansatz zielt auf Angriffe auf Computersysteme, Daten und SCADA ab und umfasst zudem physische Angriffe auf zentrale Anlagen der EDV, etwa Computernetzknoten etc. Wie beim Cyberkrieg spielt auch beim Cyberterrorismus das Zusammenwirken der physischen und der Cyberwelt die zentrale Rolle. Lange wurde davon ausgegangen, dass eine effiziente Nutzung des Internets für terroristische Ziele noch weit außerhalb der Reichweite der Terrororganisationen liege.

Doch zeigte sich, dass mit entsprechenden finanziellen Mitteln die Expertise etwa in Form exzellent ausgebildeter russischer Computerexperten einkaufen lässt beziehungsweise mittlerweile auch eigene Experten geschult werden, wie von den Geheimdiensten durchgeführte Auswertungen zeigen. Der Weg des Jihad von al-Qaida hat längst vom Khyber-Pass in den Cyberspace geführt.

Informationen offen im Netz verfügbar

Erleichtert wird das Agieren der Terroristen auch dadurch, dass etwa 80% kritischer Informationen, die auch von potenziellen Angreifern genutzt werden können, offen im Netz verfügbar sind (vgl. Weimann 2006: 112). Viele Internetseiten erweisen sich aufgrund der darin enthaltenen, teils höchst detaillierten Informationen zu Fahrplänen bzw. Lageplänen für Häfen, Flughäfen, Transportsysteme, Kraftwerke, Atom- oder Chemieanlagen, Raffinerien etc. geradezu als Fundgruben für potenzielle Terroristen. Gleiches gilt für die Möglichkeiten, die das Internet nicht nur zum Bau von schmutzigen Bomben bietet, sondern auch dafür, wie man an die Materialien gelangt, die zu diesem Bau nötig sind, etwa wo der Erwerb radioaktiven Materials möglich ist oder auf welchen Wegen Atommüll transportiert wird. Auch Wege, über die schweres Kriegsgerät – wahlweise neu oder gebraucht – erworben werden kann, gibt es im Internet.

ökonomische Modelle

Ebenfalls ist zu beobachten, dass ökonomische Modelle zusehends auch für die Strukturierung von Terrororganisationen genutzt werden. So findet mithilfe des Internet die Rekrutierung und Mobilisierung von Anhängern ebenso statt wie die Planung und Koordinierung von Aktivitäten und sogar das Fund Raising (vgl. Weimann 2006: 114-145).

Lange Zeit waren auch terroristische Anschläge der Größenordnung des 11. September für unmöglich gehalten worden – und die westlichen Gesellschaften wurden kalt erwischt. Höchste Zeit also, sich den Gefahren des internetgestützten Terrorismus gewahr zu werden, wo der richtige Tastaturbefehl mindestens so wirkungsvoll sein kann, wie der Sprengstoffgürtel eines Selbstmordattentäters.

5. Cyberspionage: Der Krieg um Informationen und Wissen im Verborgenen

Sprengstoff ganz anderer Art, aber nicht minder schädigend für Unternehmen wie Gesellschaften, geht von der Cyberspionage aus. Doch sollen die Schädigungen hier nicht öffentlich sichtbar werden, obwohl sie ökonomisch wie auch hinsichtlich der nationalen Sicherheit ungleich höher sein können.

Cyberspionage ist, wie herkömmliche Spionage auch, darauf ausgerichtet, in den Besitz von staatlichen, militärischen und strategischen Geheimnissen eines Landes zu gelangen. Zudem ist sie, analog zur herkömmlichen Wirtschaftsspionage, darauf angelegt, ökonomische Geheimnisse von staatlichen und privaten Unternehmen und Forschungseinrichtungen zu erlangen. Computernetzwerke und damit verbundene Datenspeicher bieten aufgrund der zahlreichen Sicherheitslücken und allzu häufig gravierenden vermeidbaren Sicherheitsmängeln, exzellente Möglichkeiten für Datenspionage. Hierbei spielt nicht

nur einfaches Hacking eine Rolle, sondern auch manipulierte USB-Sticks sowie die Ausnutzung menschlicher Schwächen, das sogenannte Social Engineering, wo Mitarbeiter der Zieleinrichtungen überwacht und ausspioniert werden, um dann ihr Vertrauen zu erschleichen und sie instrumentell zu nutzen.

Social Engineering

Im Mai 2007 etwa wurde bekannt, dass es zu virtuellen Einbrüchen und Manipulationen in die deutsche Regierungszentrale kam. Mithilfe gefälschter E-Mails an das Bundeskanzleramt, deren jeweiliger Anhang ein Virus enthielt, erlangten die Angreifer, deren Spur nach China führt, Zugriff auf die Netzwerke und Datenbanken der Bundesregierung. Ähnliches unberechtigtes Eindringen in staatliche Systeme gab es auch in allen anderen westlichen Staaten, und auch dort führte die Spur regelmäßig in die Volksrepublik, der vielfach intensive Spionage vorgeworfen wird.

So gravierend diese Vorfälle sind, verschlimmert werden sie noch durch die staatlich sanktionierte Industriespionage im großen Stil, welche neben China auch von einer Vielzahl auch westlicher Staaten betrieben wird. Besonders beliebtes Ziel der Spionageangriffe ist Deutschland, das aufgrund seines Mangels an natürlichen Rohstoffen in besonderem Maße auf seine technologische Innovationskraft angewiesen ist. Die so gewonnenen Erkenntnisse wecken Begehrlichkeiten im Ausland. Opfer der oft staatlich betriebenen (Cyber-)Spionage sind Unternehmen jeder Größe, insbesondere solche im Technologie- und Entwicklungsbereich. Gerade dem Mittelstand ist die Gefährdung, die durch die nicht hinreichende Sicherung von Netzwerken und elektronisch gespeicherten Daten entsteht, oft nicht bewusst. Und nicht wenige Unternehmen mussten für diese Nachlässigkeit in der Cybersicherheit teuer bezahlen, wie etwa die Erlanger Firma *clearaudio electronic GmbH*, die auf Tonabnehmer spezialisiert ist. Die Daten einer 100.000 Euro teuren die Weltmarktführerschaft bedeutenden Entwicklung, wurden von Cyberspionen entwendet, ohne dass dies bemerkt wurde. Auf einer Fachmesse stieß die Firma dann auf das fertige Produkt, das von einem chinesischen Unternehmen präsentiert wurde – mit bis aufs i-Tüpfelchen identischen technischen Spezifika. Fälle wie diese, wo unbemerkt virtuell in Unternehmen eingebrochen wird, auch solche, die Rüstungsgüter herstellen, gibt es viele. Schadprogramme, die Daten und Dokumente von Festplatten infizierter Rechner kopieren und an vorgegeben Adressen senden, sind Legion.

staatlich sanktionierte Industriespionage

Nicht selten steht neben Unternehmen und Regierungen auch das organisierte Verbrechen hinter derartigen Aktionen. Und auch dieses kann durch seine Cyberaktivitäten eine Bedrohung der Sicherheit von Staat und Gesellschaft bewirken.

organisiertes Verbrechen

6. Cyberkriminalität: Eine neue Industrie gefährdet Sicherheit und Wohlstand

Das Verbrechen im Internet beschränkt sich keineswegs auf Kleinbetrüger und Gelegenheitshacker. Vielmehr existieren gerade in Russland und anderen Staaten der ehemaligen Sowjetunion große Verbrechersyndikate, die sich auf Cy-

Verbrechersyndikate

berkriminalität im großen Maßstab spezialisiert beziehungsweise diese in das Spektrum ihrer illegalen Aktivitäten aufgenommen haben. Mittlerweile kann von einer regelrechten Schadprogrammindustrie gesprochen werden (vgl. Bowden 2012: 48). Kasperksy, einer der weltgrößten Hersteller von Antivirensoftware, befasst sich täglich mit mehreren Tausend neuartigen Viren, Würmern, Trojanern und sonstigen Formen der Schadsoftware. Laut einer Auskunft des Bayerischen Verfassungsschutzes werden pro Tag etwa 55.000 neue Schadprogramme ins Internet eingespeist. Der Verkauf bereits vorprogrammierter Schadprogramme zum Zwecke krimineller Nutzung hat sich zu einem eigenständigen, lukrativen Geschäftsfeld entwickelt. Hierfür existieren spezielle Vertriebsseiten der Internet-Mafia, wo zudem gehackte Kreditkartendaten, Zugriff auf gehackte Behördenseiten etc. erworben werden können, wie etwa in der ARD-Dokumentation *„Angriff aus dem Netz. Die Wirtschaft im Visier von Onlinekriminellen"* von Birgit Kappel und Sabina Wolf berichtet wurde. Wie professionell dieses Geschäft betrieben wird, zeigt sich daran, dass für die gleichsam kommerziell vertriebene Schadsoftware sogar Kundendienst und regelmäßige Updates angeboten werden (vgl. Bowden 2012: 116). Mit dem sozusagen von der Stange zur Verfügung gestellten Instrumentarium lassen sich neben Spionage- und Angriffsszenarien auch trivialere Aktivitäten wie Erpressungen durchführen, wo gedroht wird, Webseiten lahmzulegen, Kundendaten zu veröffentlichen, Buchhaltungsdaten zu löschen etc. Die meisten Unternehmen zahlen, da der Skandal, wenn etwa bekannt würde, dass Hunderttausende sensibler Kundendaten inklusive Adresse, Bankverbindung und Kreditkartendetails gestohlen und veräußert wurden, dem Ruf eines Unternehmens sehr schaden und sogar dessen Börsenkurs negativ beeinflussen könnte. Nicht zuletzt vor diesem Hintergrund werden Hacking-Angriffe in den seltensten Fällen zur Anzeige gebracht. Die Gefahren, die unserer Gesellschaft durch die Aktivitäten der Cybermafia drohen, sind immens.

Schadsoftware

Börsenkurs

In Deutschland befassen sich unter anderem der BND und die Landesverfassungsschutzbehörden mit dieser Thematik. Ein wesentlicher Auftrag speziell des Verfassungsschutzes hierbei sind Prävention und Aufklärung. Ein Phänomen vor dem hierbei in besonderer Weise gewarnt wird, weil es im Bereich aller geschilderten Bedrohungsarten von hoher Relevanz ist, sind die sogenannten Botnetze. Dabei handelt es sich um Netzwerke von – unbemerkt von den jeweiligen Eigentümern – gekaperten Computern, die von einer zentralen Stelle aus gesteuert werden. Große Botnetze umfassen mehrere Millionen Rechner, deren Kapazität gezielt für Sabotageakte genutzt werden kann. Ziel des Zugriffs auf diese Computer ist also nicht die Schädigung des einzelnen Endgerätes, sondern dessen Nutzbarmachung zur Durchführung krimineller, terroristischer oder kriegerischer Akte über das Internet. Mit Hilfe von Botnetzen lassen sich vor allem sogenannte DDOS-Angriffe durchführen, die darauf ausgerichtet sind, dass angegriffene Internetseiten aufgrund der massenhaften, über das Botnetz koordinierten Zugriffe auf die Seite, zusammenbrechen und so nicht mehr genutzt werden können. Diese Strategie kam etwa bei den von Russland ausgehenden Angriffen auf Estland und Georgien, die als erste Cyberkriege gelten, zur Anwendung. Aber Botnetze können ebenso der Weiterverbreitung von Schadprogrammen dienen, die für andere Zwecke vorgesehen

Verfassungsschutz

Botnetze

DDOS-Angriffe

sind; auch lassen sich durch die vereinte Rechnerleistung komplizierte Codes knacken, was wiederum ein Eindringen in auch gut geschützte Netzwerke ermöglicht. Botnetze selbst werden dabei durchaus auch vermietet oder verkauft (vgl. Etwa Bowden 2012: 43).

Um ein Botnetz zu errichten muss der Angreifer zunächst in fremde Rechner eindringen, diese übernehmen und ggf. das System der Sicherheitsupdates ausschalten. Der Erstzugriff ließe sich häufig durch entsprechende Sicherheitsvorkehrungen vermeiden, doch durch Unwissenheit, Ignoranz oder bewusste Vorbehalte gegenüber Softwareherstellern klaffen eklatante Sicherheitslücken im gesamten Internet (vgl. Bowden 2012: 21, 67-76). Lange schon warnen Experten „vor der geradezu aberwitzigen Fragilität des Internet [...]. Sie waren es gewohnt, dass man ihre Mahnungen ignorierte“, schreibt der Journalist Mark Bowden (2012: 126), der sich intensiv mit der Thematik befasst, und gelangt noch 2012 zu dem Schluss, dass es „zu den besonderen Eigenarten der modernen Zeit [gehört], dass die Industrieländer sich zwar mehr und mehr in allen Bereichen auf Computernetzwerke verlassen, bislang aber vergleichsweise wenig über deren Schutz nachgedacht haben“ (ibid. 128).

eklatante Sicherheitslücken

7. Wie reagieren? Entnetzung und Erhöhung der gesellschaftlichen Resilienz

Wie soll auf diese Herausforderungen reagiert werden? Auf Ebene von Militär und Staatsschutz lassen sich erste Anstrengungen erkennen. Die Bundesregierung hat eine Cyber-Strategie entworfen, das Bundesamt für Sicherheit in der Informationstechnik (BSI) ins Leben gerufen und das Nationale Cyber Abwehrzentrum (NCAZ) geründet, das beim BSI angesiedelt ist und im April 2011 seine Arbeit aufgenommen hat. Beim NCAZ handelt es sich um eine der Kommunikation zwischen den mit der nationalen Sicherheit betrauten Behörden dienende Einrichtung, jedoch keine eigenständige Behörde. Somit bleiben die Zuständigkeiten der zahlreichen Einzelbehörden – und damit die institutionelle Zersplitterung in der Cyberabwehr – weitgehend gewahrt. Auch in anderen Ländern, etwa den USA, die sich schon etwas länger auf die Abwehr der Bedrohungen aus dem Cyberspace eingestellt haben, hinkt man hinterher. Staaten wie Russland und China hingegen haben schon lange den systematischen Aufbau von Cyberkapazitäten betrieben. So bildete Moskau bereits im Kalten Krieg Informatiker aus, die Wege zur Kompensation der ballistischen Kapazitäten der USA finden sollten. Heute ist es vor allem die Naschni, eine ultra-nationalistische, Putins Kreml treu ergebene Jugendorganisation, die Russland den Nachwuchs an Cyberkriegern liefert. Auch war die Naschni selbst maßgeblich an den Cyberangriffen auf Estland beteiligt, was den Vorteil hatte, dass eine direkte Zurechenbarkeit der Attacken zum russischen Staat unmöglich war. Auch China ist mit Cyberkapazitäten sehr weit vorangeschritten. Seit etwa drei Jahrzehnten verfolgt das Land deren systematischen Aufbau über spezielle Schulen und Hochschulen. Auch Beijing sah in dieser Strategie den einzigen Weg, die Überlegenheit potenzieller künftiger Gegner zu kompensieren. Diese Strategie erwies sich bislang als sehr erfolg-

Nationales Cyber Abwehrzentrum (NCAZ)

institutionelle Zersplitterung

Anti-GPS-Einheit

reich, wie das Beispiel der Anti-GPS-Einheit aufzeigt. Seit deren Existenz bekannt ist, ist der Einsatz der VII. US-Flotte im Südpazifik bei einem etwaigen Konflikt mit China fraglich geworden, wie aus vertraulicher Quelle am Rande einer Konferenz zur Cybersicherheit im Frühjahr 2012 berichtet wurde. Tatsächlich geht man davon aus, dass die Anti-GPS-Einheit in der Lage wäre, die Schiffe, Flugzeuge und Flugkörper zu hacken und die Überwachungssysteme zu manipulieren. Allein dieser Umstand zeigt nochmals dramatisch auf, wie ernst die Bedrohung aus dem Cyberspace zu nehmen ist, und wie eng der abstrakte Cyberspace und die fühlbare Wirklichkeit zusammenhängen.

Dieses Bewusstsein gilt es sowohl bei den politischen Entscheidern als auch in der breiten Bevölkerung zu stärken. Denn wie im Kontext der Botnets dargelegt, fängt die nationale Sicherheit tatsächlich schon beim ungeschützten Rechner im eigenen Wohnzimmer an. Doch das alleine reicht nicht. Gerade bei Unternehmen und Behörden muss ein ganzheitliches Bild der Sicherheit im Bereich der Informationstechnologie etabliert werden.

Firewall

Denn auch die höchste Firewall nützt nichts, wenn keine Zugangskontrollen zu den Serverräumen stattfinden oder Kabel für vertraulichen Datenfluss leicht zugänglich auf dem Betriebs- oder Behördengelände verlegt sind. Ebenso gilt es, die Beschäftigten zu sensibilisieren, dass auch sie Teil gezielter Maßnahmen durch Gegner werden können, durch die man an Informationen über innere Abläufe von Organisationen, Passwörter oder sonstige wichtige Informationen gelangt.

Entnetzung

Natürlich stellt sich auch die Frage nach einer zumindest teilweisen Entnetzung. Doch gerade angesichts der Bequemlichkeit, welche die Internetbasierung nahezu aller Systeme der Gesellschaft gebracht hat, und auch angesichts der Kostenersparnisse, die das Internet der Wirtschaft ermöglicht, sehen die diesbezüglichen Perspektiven eher schlecht aus, und sind in letzter Konsequenz wohl auch nicht wünschenswert. Dennoch lassen sich in bestimmten Bereichen schon Entnetzungstendenzen erkennen, etwa in Form der amerikanischen *Trusted Internet Connection Initiative*, in deren Rahmen der Internetverkehr zwischen Behördennetzen und öffentlichen Netzen um knapp 99% reduziert werden soll, oder aber in Form des Hochsicherheitsbunkers der Firma *IronMountain* im Hamburger Hafenviertel, wo derzeit etwa 50.000 Magnetbänder mit hochsensiblen Unternehmensdaten liegen. Auch der israelische Wissenschaftler Gabriel Weimann (2006: 193f.) verweist auf zahlreiche Beispiele, wo Daten, die potenziell von Terroristen genutzt werden könnten, wieder vom Netz genommen wurden.

Trusted Internet Connection Initiative

Doch das alles betrifft nur die technisch-organisatorische Seite der Netzsicherheit. Hierauf wies nicht zuletzt Vizeadmiral Michael Rodgers, der Kommandeur der X. US-Flotte, im Mai 2012 auf einer Rede an der US Naval Academy hin. Vielmehr gehe es um die Frage von Führungsstärke. So befänden wir uns derzeit in einer Situation, in der wir uns für künftige Auseinandersetzungen rüsten müssten, auch wenn weder die vollen Kapazitäten derzeit zur Verfügung stünden noch klar sei, wie ein Szenario konkret aussehen könnte. Dabei verwies er auf die historischen Beispiele der Flugzeugträger, die bereits in den 1920ern gebaut wurden, ohne dass man um konkrete Einsatzmöglichkeiten wusste, diese sich aber im Kontext des Zweiten Weltkrieges als unver-

Führungsstärke

zichtbar erwiesen haben. Gleiches treffe auf die Doktrinentwicklung für Landungseinheiten bereits zwei Jahrzehnte vor D-Day zu. Hätte man seinerzeit die Entwicklungen aller Unsicherheiten und Widerstände zum Trotz nicht beherzt vorangetrieben, wäre die nationale Sicherheit nicht erfolgreich zu verteidigen gewesen. Mit dieser Ansicht zeigt er letztlich den Weg auf, der zugleich ein Ausweg aus jener Lage sein könnte, der im Bericht der 2003 von Präsident Clinton eingesetzten *Kommission zum Schutz kritischer Infrastrukturen* zum Ausdruck kam, wo es heißt, dass „[d]ie Geschwindigkeit, in der das Internet unerwartete und versteckte Verwundbarkeiten hervorbringt, [...] unsere Fähigkeit, was diese Verwundbarkeiten sind und wie künftige aussehen könnten, längst überholt [hat]“ (Bowden 2012: 39).

Soviel auch getan und vorbereitet wird, so wenig lässt sich doch völlige Cybersicherheit erreichen – und angesichts der dargelegten Defizite in absehbarer Zeit nicht einmal eine partielle. Daher gilt es, ergänzend zu all den Bemühungen um Sicherheit zugleich auch die Resilienz unserer Gesellschaften zu erhöhen. Diese müssen mental auf die Folgen von Cyberangriffen, ganz gleich von wem sie ausgehen, vorbereitet werden. Hierzu bedarf es eines offenen Diskurses statt der bislang oft erkennbaren Ignoranz oder Geheimniskrämerei. Und nicht zuletzt muss es darum gehen, einen gesellschaftlichen Diskurs um die generelle Bedeutung des Internets für unsere Gesellschaft anzustoßen. Denn auch dieses Verständnis ist von zunehmender Relevanz für unsere nationale Sicherheit. Auch Scriptkiddies werden erwachsen, das Berufsziel Hacker wird gerade in einer Zeit die gleichermaßen an sicheren Beschäftigungsverhältnissen wie stabilen Werten verliert, immer beliebter. Schul- und Hochschulausbildung werden in bestimmten Kreisen zusehends in Frage gestellt, da sich im Internet, in dem man ohnehin gleichsam lebt, sehr bequem viel mehr Geld verdienen lässt. Im Rahmen einer Tagung zur Cybersicherheit in Wiesbaden wurden die Beispiele zahlreicher jugendlicher Hacker genannt, die innerhalb weniger Wochen mit kriminellen Machenschaften im Internet hunderttausende von Dollars oder Euros verdienten. Kreditkartenbetrug und der Diebstahl von beziehungsweise Handel mit Identitäten ist ein höchst lukratives und sehr einfach zu realisierendes Geschäft mit derzeit fast grenzenlosen Perspektiven und einer äußerst geringen Gefahr, entdeckt oder belangt zu werden. Andernorts, speziell in Osteuropa, werden junge Informatiker beziehungsweise Internet-Cracks von Verbrechersyndikaten angeworben, etwa zur industriellen Herstellung von Schadsoftware.

Resilienz

Scriptkiddies

Berufsziel Hacker

Innerhalb bestimmter Kreise, denen eine wachsende Zahl Jugendlicher sich zugehörig fühlt, mangelt es eklatant am Unrechtsbewusstsein im Bereich des Internet, wie etwa offene Sympathiebekundungen für Hackergruppen oder Cyberverbrecher wie Anonymous zeigen, die gleichermaßen gegen Unternehmen vorgehen und demokratische wie rechtsstaatliche Grundsätze nicht respektieren. Diese Entwicklung wird durch den Aufstieg der Piratenpartei gleichermaßen reflektiert und gefördert, wie nicht zuletzt der Umgang beziehungsweise die Forderungen in Fragen geistigen Eigentums oder Urheberrechten im Internet zeigen. Auch und gerade diese gesellschaftlichen Herausforderungen gilt es zu lösen, sollen die Bedrohungen aus dem Cyberspace kalkulierbarer und weniger schädlich werden.

Unrechtsbewusstsein

Anonymous

Völkerrecht

WikiLeaks

globales Finanzsystem

Interdependenz der Weltwirtschaft

Wohl noch länger werden die derzeit offenen Probleme wie die Zurechenbarkeit von Cyberangriffen zu konkreten Angreifern uns beschäftigen, da diese sich allzu leicht hinter Servern in unbeteiligten Ländern verstecken können. Auch die Entwicklung des Völkerrechts, wie mit Cyberkrieg und Cyberterrorismus umzugehen ist, hinkt den realen Herausforderungen hinterher. Für Sicherheitsprobleme, die hier nicht behandelt wurden, wie Facebook-Revolutionen und WikiLeaks, gilt es ebenfalls, geeignete Modi Operandi zu finden. Und nicht zuletzt der Bereich, der gerade schon durch die Vielzahl anderer Herausforderungen weltweit Kummer bereitet, das globale Finanzsystem, wird weiterhin im Fokus des Interesses der Cybersicherheit liegen. Denn gerade wenn in einer Gesellschaft kein Vertrauen mehr in die Sicherheit des Banken- und Finanzsystems besteht und es zu Runs auf Kreditinstitute kommt, weil die Menschen um ihr Geld fürchten, können ganze Gesellschaften zusammenbrechen. Das ist es, was diesen Bereich besonders attraktiv für Terroristen macht, die das Chaos wollen. Aus ebendiesem Grund halten sich Staatenlenker indes auf diesem Sektor zurück. So verpflichteten sich die USA 2003 öffentlich dazu, als sich diese Frage im Fall des Irak konkret stellte, sogar dazu, keine Diktatorengelder aus Banken zu entfernen oder Börsen zu manipulieren, um Staaten zu schwächen, obwohl dies technisch kein allzu großes Problem wäre. Aber die Angst vor Folgen für die Stabilität des eigenen Wirtschaftssystems wie auch der globalen kapitalistischen Weltordnung ist zu groß. Und ebendiese Angst scheint es auch zu sein, die China davon abhält, Wall Street zu manipulieren oder gar zum Absturz zu bringen. Denn angesichts der hohen Interdependenz der Weltwirtschaft und insbesondere ihrer herausragenden Akteure USA und China, wären die Folgen auch für den Angreifer unabsehbar. Vor dem Hintergrund der immensen Schulden, welche die USA bei den Chinesen haben, äußerte sich ein chinesischer Diplomat vor nicht allzu langer Zeit einmal dahingehend, dass die USA keine Angst vor chinesischen Hackerangriffen auf die Wall Street haben müssten, weil das meiste dort ohnehin schon China gehöre, und man sich ja nicht selbst schädigen wolle. Aber das ist ein anderes Problem.

Literaturverzeichnis

Mark Bowden (2012): Worm. Der erste digitale Weltkrieg. Berlin. 2012. Bloomsbury Verlag.

Gabriel Weimann (2006): Terror on the Internet. The New Arena, the New Challenges. Washington.

2006. United States Institute of Peace Press.

Dan Verton (2003): Black Ice. The Invisible Threat of Cyber-Terrorism. Emeryville. 2003 McGraw-Hill