Was ist Cyberwar?

Jonathan Simsch

Eine Arbeit erstellt im Rahmen von

Inhaltsverzeichnis

Einleitung

Das Internet als landesgrenzenübergreifendes Kommunikations- und Distributionsnetz bietet mit seinen Kanälen das Potential, Informationen von (fast) jedem beliebigen Punkt der Erde zu jedem anderen Punkt der Erde zu übertragen. Durch die jahrzehntelange Entwicklung computerbasierter Medien, sind mit einem Internetanschluss mittlerweile sowohl Schriften, Bilder, Videos und viele weitere Informationsträger rund um die Uhr verfügbar und verteilbar. Die Natur des Internets bietet also eine nahezu unendliche Anzahl an Möglichkeiten. Jedoch unterliegt das Internet wie alle Technologien und Erfindungen der Menschheit dem Stigma des möglichen Missbrauchs.

So vielseitig die Nutzungen im guten Sinne sind, so vielseitig sind auch die Wege, seinem Gegenüber Schaden zuzufügen. Jeder, der einen Computer mit Internetanschluss besitzt, ist oder wird über kurz oder lang mit sogenannter Malware in Kontakt kommen. Die Hauptvertreter dieser Programmgruppe sind Viren und Trojaner, die den angegriffenen Computer und seinen Benutzer schädigen können.

Jedoch sind nicht die Angriffe auf Privatnutzer des Internets das größte Problem. Ein Thema, welches den Regierungen der Welt seit der Verbreitung des World Wide Web Kopfschmerzen bereitet ist der Cyberwar. Was der Cyberwar ist, welche Interessengruppen dahinter stecken und welche Auswirkungen ein Krieg mit Mitteln der Kommunikationstechnologie haben kann, zeigt diese Arbeit auf. Sie beleuchtet die physischen und psychologischen Bedrohungen, die ein virtueller Konflikt hervorbringen kann und gibt eine Aussicht auf das, was die Gefahr eines Cyberwar in Zukunft für uns bedeuten kann.

Im ersten Kapitel wird eine Wortbedeutung gesucht, die einer weiterführenden Klassifizierung und Einstufung von computergestützen Kriegshandlungen als Basis dienen kann. Anhand von Beispielen aus der Anfangszeit dieser,

wird ein erster Eindruck von der Bandbreite des Themas gegeben. Kapitel zwei führt die Mittel, mit denen ein Cyberwar bestritten wird, weiter aus. Die Mittel und Wege eines Cyberwar sind eine wichtige Verständnisbasis, um die Klassifizierungen, die in Kapitel drei folgen, nachvollziehen zu können. Auch die Einschätzung durch Staaten und Staatenbündnisse, die durch Institutionen wie Verteidigungsministerien und Ausschüssen vertreten sind, finden hier Erwähnung. Kapitel vier beinhaltet eine analysierte Auflistung von Auswirkungen, die aus einer solchen Kriegshandlung entstehen können. Die Gefahr einer physischen oder auch psychischen Wechselwirkung wird an dieser Stelle noch einmal ausführlicher herausgestellt. Das Fazit bildet das fünfte Kapitel und bietet eine Zusammenfassung, auf deren Basis der darauf folgende Ausblick beruht.

1 Ursprung des Cyberwar

In diesem Kapitel wird der Frage nachgegangen, woher die Basis für einen Angriff über Computer gegen computergestützte Systeme kommt. Wieso die Computertechnik solche Möglichkeiten bereithält und welche geschichtlichen Ereignisse mit solchen Übergriffen in Verbindung zu bringen sind soll an dieser Stelle genauer betrachtet werden.

1.1 Wortbedeutung

Das Wort Cyberwar, oder auch Cyberkrieg, ist ein Zusammenschluss der beiden Wörter „Cyberspace“ und „Krieg“. Das Kofferwort verbindet also die Definition einer kriegerischen Auseinandersetzung mit der Umschreibung des virtuellen Raumes, den das Internet darstellt. Cyberwar steht demnach vor allem für die Verstrickung der Kommunikationstechnologie mit der unmittelbaren Bedrohung physischer Angriffe, die auf einer Stufe mit Waffengewalt zu stellen sind.

1.2 Historie der Cyberattacken

Die erste dokumentierte Begebenheit, die die Eigenschaften eines schädlichen Prozesses auf eine Art Computer beschreibt, ist der Artikel „Theory and Organization of Complicated Automata“ von John von Neumann aus dem Jahre 1948.[1] Er beleuchtet in seinem Artikel die Möglichkeit, dass sich ein Fehler

1 von Neumann, John: Design of computers, Theory of Automata and numerical Analysis, 1912-1957

innerhalb einer logischen Prozesskette verselbstständigen und reproduzieren kann. Die Theorie eine Computervirus ist also älter als 70 Jahre.

Dass so etwas von Dritten gewollt initiiert sein könnte findet jedoch bei Neumann noch keine Erwähnung. Dieses Beispiel findet sich vielmehr unter dem Namen „Brain.a“. Brain.a ist eine Datei, die als Brain-Virus bekannt wurde und die Aufgabe wahrnahm, den Inhaltsverzeichnissen von schwarzkopierter Software den Namen „Brain“ zu geben. Die Kopien wurden von den Autoren des Virus verkauft und sollten, durch ihre geänderte Dateistruktur, die Kunden an die Verkäufer binden. Namentlich zwei junge pakistanische Computerenthusiasten, Basit & Amjad, Gründer von Brain Computer Services. Das, nach eigenen Angaben für Werbezwecke gedachte, Virus enthielt den Namen der beiden Programmierer und ihre Adresse. Es verbreitete sich zusehends auf der ganzen Welt und die überraschten Brüder sahen sich einer internationalen Protestwelle gegenüber, die sie zwang, ihren Telefonanschluss zu kündigen.[2]

Ein Virus allein macht aber noch keinen Cyberwar. Ein Vorfall, der dem Begriff Cyberwar ein wenig näher kommt, ist die Explosion der Tscheljabinsk-Pipeline in der Sowjetunion im Jahre 1982. Die Steuerungstechnologie der Pipeline stammte aus den USA, die ihre Software für die Verdichtungsstation der Pipeline nur unter großem Widerstand zur Verfügung stellte. Diese Unfreiwilligkeit führte zur Implementierung eines Schutzprogramms in die Software, die dem Nutzer acht Monate Zeit gab, die rechtmäßige Erwerbung mit einer Codeeingabe zu bestätigen. Sollte dies innerhalb der Frist nicht geschehen, würde das Programm selbstständig und unbemerkt die Steuerung der Pipeline dahingehend verändern, dass der Pipelinedruck die Grenzbelastung um ein Vielfaches übersteigt. Wie die Geschichte zeigt, ist genau dies geschehen. Die Folge war eine drei Kilotonnen starke Explosion. Vergleichbar also mit einem Fünftel der Kraft einer Atombombe.[3]

Im Rahmen des kalten Krieges wurde so eine softwarebasierte Möglichkeit genutzt, dem Gegner eine strategisch wichtige Institution zu zerstören. Jedoch wirkt dieser Vorfall noch eher wie eine Trotzreaktion seitens der USA. Als erste, als Cyberwar einzustufende Begebenheit, wird deshalb von einigen Experten der Jugoslawienkrieg 1999 genannt. Im Laufe des Konflikts bekamen

2 Vgl. Hypponen, Mikko: Fighting viruses, defending the net, 2011, [Hyp11]
3 Vgl. Kloiber, Manfred; Welchering, Peter: Militärs suchen Strategien gegen Cyberattacken, 2011, [Klo11]

Computerexperten des Geheimdienstes CIA den Auftrag, die Konten des jugoslawischen Parteichefs Slobodan Milošević zu löschen.[4]

Der Kosovokrieg hält noch weitere Beispiele bereit, wie den angeblichen Angriff der serbischen Hackergruppierung „Schwarze Hand“ auf einen Computer der Navy. Die Löschung der darauf vorhandenen Daten wurde nie bestätigt. Die Indizien sprechen jedoch dafür, dass der Rechner für einen gewissen Zeitraum blockiert wurde.[5]

In den Jahren 1998 bis 2000 wurden die USA erneut Opfer einer breit angelegten Reihe von Cyberattacken. Die unter dem Namen Moonlight Maze bekanntgewordene Angriffswelle zielte unter anderem auf Rechnereinheiten des Pentagon, der NASA und Computer des amerikanischen Energieministeriums. Neben dem digitalen Einbruch auf diese wurden während des Angriffs zahlreiche Datensätze gestohlen.[6]

Auch beim sogenannten Hainan-Zwischenfall sind die USA als Opfer in Cyberattacken involviert. Nach dem Zusammenstoß eines amerikanischen mit einem chinesischen Kampfjets wurden die Würmer Code Red und Code Red II auf zahlreichen amerikanischen Computern gefunden. Label wie „hacked by Chinese“ und die zeitliche Nähe lassen die Vermutung zu, das dieser Hackerangriff mit der Jetkollision in Verbindung steht.[7]

Im Laufe der letzten Jahre kam es immer wieder zu gegenseitigen Cyberattacken zwischen den großen Industrienationen wie die USA, China und Russland, um nur einige zu nennen. Da die Informationen, die im Rahmen dieser Angriffe geklaut wurden sowohl militärischer als auch wirtschaftlicher Natur sind und die Angreifer meist unerkannt bleiben, lassen sich über den Verbleib der kopierten Daten nur Vermutungen anstellen.

Ein Cyberwar kann also viele verschiedene Formen annehmen. Möchte man ihn verstehen, reicht es deshalb nicht, sich einzelne geschichtliche Ereignisse herauszusuchen. Es gilt vielmehr zu begreifen, dass die Kommunikationstechnologie auf Grund verschiedener Eigenschaften, ebenso wie ein Panzer oder

4 Vgl. Bendrath, Ralf: Der Kosovo-Krieg im Cyberspace, 1999, [Ben99]
5 ebd.
6 Prof. Dr. Dr. Saalbach, Klaus-Peter: Cyberwar Grundlagen und Geschichte, S.20, 2012, [PDDS12]
7 a.a.O., S.21

ein Gewehr, als Waffe angesehen werden kann. Ein Panzer kann gleichermaßen ein fahrbares Geschütz, sowie ein kraftvolles Transportgerät sein. Ein Gewehr kann Menschen einschüchtern oder töten. Genauso wahrscheinlich ist ein Einsatz als Jagdwaffe, die die tägliche Nahrungsbeschaffung sichert. Um einen vollständigen Eindruck des Begriffes Cyberwar zu bekommen ist es daher nötig, sich die Mittel, die für einen solchen eingesetzt werden, näher anzuschauen.

2 Mittel des Cyberwar

Der Frage, welche Mittel für kriegerische Handlungen über Kommunikationsnetze zur Verfügung stehen, wird in diesem Kapitel nachgegangen. als Grundlage für weitere Ausführungen soll zunächst ein kurzer Abriss über die Struktur des Internets gegeben werden.

2.1 Die Struktur des Internets

Die Kommunikationstechnologie, somit das Internet, jeder Computer und auch jedes andere elektronische Kommunikationsgerät basieren auf dem einfachen Zusammenschluss von Sender und Empfänger. Ein Computer kann eine Datei versenden, die an einem anderen Computer wiederum ankommt. Hinter dieser einfachen Leistung steht ein ganzes Netz von Programmen, weiteren rechnenden und verwaltenden Maschinen und eine kaum zu überblickende Anzahl an Wegen, die der elektronische Informationsträger gehen könnte. Der Cyberspace ist also eine Vernetzung unzähliger Anfangs- und Endpunkte, verbunden durch Kabel, Funk und Glasfaser.

Meist ist ein solcher Anfangs- oder Endpunkt durch einen im Haushalt gebräuchlichen PC gegeben. Dies ist jedoch nicht immer der Fall. Rechner werden in der modernen Welt mittlerweile für fast alle automatisierten Prozesse eingesetzt. Sei es ein zu steuernder Aufzug, eine Waschmaschine oder ein Garagentor. Sind diese Steuerungsrechner an das Internet angeschlossen, bilden sie automatisch einen Teil des Systems. Ein System, in dem jeder mit jedem kommunizieren kann, wenn man die richtigen Wege kennt.

Kommunikation bedeutet in der Computersprache jedoch in den seltensten Fällen das technische Äquivalent eines Gespräches von Angesicht zu Angesicht. Wenn an dieser Stelle des weiteren von Kommunikation gesprochen wird, so ist der Datenaustausch im weitesten Sinne gemeint.

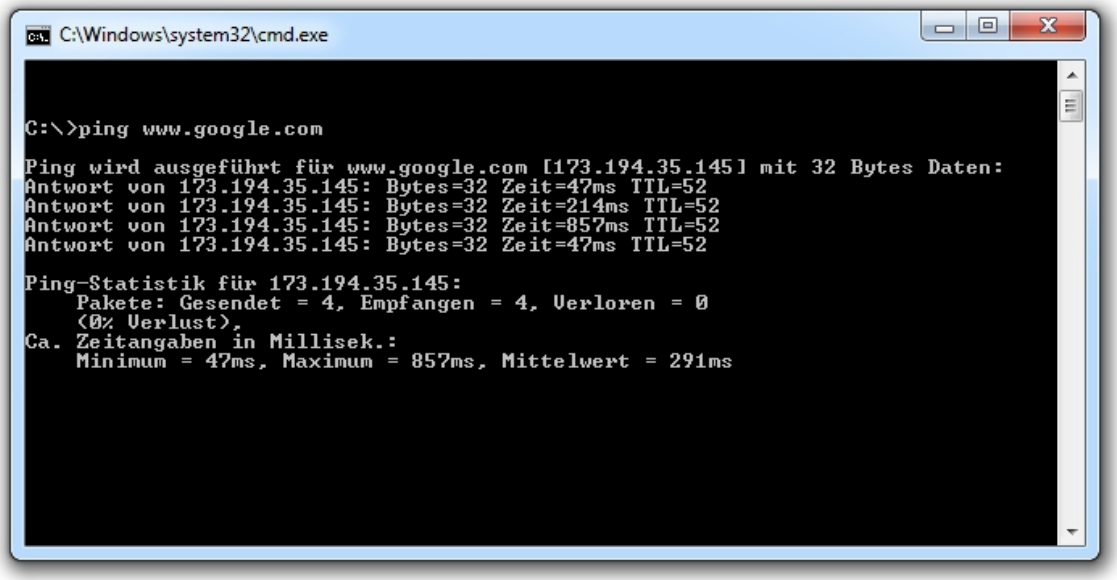

Abbildung 2.1: Ping an www.google.com[8]

Damit Computer kommunizieren können, wird zuerst ein Ping versendet, mit dem die Verbindung geprüft werden kann. Ein Ping ist ein kleines Datenpaket, welches zwischen Rechnern einmal hin und wieder zurückgeschickt wird. Ist die Übertragung des Pings geglückt, ist eine Verbindung vorhanden.

8 Simsch, Jonathan, 2012

2.2 Wiederkehrende Angriffsmuster

Wie sehen nun Methoden aus, mit denen ein Angriff vonstatten geht? Um diese Frage zu beantworten folgen an dieser Stelle einige Erläuterung zu den stets wiederkehrenden Angriffsmustern von Cyberattacken.[9]

2.2.1 Denial-Of-Service

Lediglich für die Überprüfung der Verbindung gedacht, ist der Ping das erste und kleinste Mittel, eine Cyberattacke auszuführen. Wie in der Abbildung 2.1 zu sehen ist, dauert der Vorgang nur wenige Millisekunden. Eine Massenanfrage von vielen hunderten von Rechnern auf einmal auf eine einzige Adresse jedoch, kann den angefragten Rechner bereits so sehr beschäftigen, dass er die vielen Anfragen nicht mehr bearbeiten kann. Das kann einen Systemabsturz zur Folge haben oder zur Unerreichbarkeit des Gerätes führen. Was im ersten Moment wenig verheerend erscheint, kann durch die Wahl des richtigen Zieles in eine Katastrophe münden.

2.2.2 Diffamierung

Wer einmal ein soziales Netzwerk mit Hilfe eines Computers besucht hat, mag unter Umständen auf Meinungsäußerungen gestoßen sein, die im gewöhnlichen sozialen Umgang weniger zu finden sind. Beschimpfungen und Gerüchte, die Dritte in einem schlechten Licht erscheinen lassen, sind an der Tagesordnung. Verleumdungen entstehen in der vermeintlichen Anonymität des Internets leichter als beispielsweise in der Presse oder in Kreisen mit bekannten Gesichtern. Nun wird sich ein Staat im allgemeinen nicht an einer Beleidigung seitens eines Einzelnen aufhalten. Die gezielte Diffamierung

9 Weitere Übersichten bieten das Bundesamt für Sicherheit in der Informationstechnik in ihren Lageberichten(`https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html`) und die Dokumentation „Cyber-Krieg - Wenn das Web zur Waffe wird“ von N24 (`http://www.n24.de/mediathek/cyber-war-wenn-das-web-zur-waffe-wird_1552737.html`).

bestimmter staatstragender Persönlichkeiten jedoch, hat das Potential sich weiter auszubreiten.

Man stelle sich einen Politiker vor, der bestimmte Interessen vertritt, die einem anderen Staat, einer anderen Partei oder einer ähnlichen Interessengruppe erhebliche Schwierigkeiten bereitet. Die Person kann durchaus im Recht sein und lediglich mit den Mitteln agieren, die ihm durch den Staat zur Verfügung stehen. Mit legalen Mitteln kann ihm sein Gegner also keinen Einhalt gebieten. Hängt man der Person jedoch ein Gerücht an, welches weitere Kreise zieht, wird ihr die Handlungsgrundlage durch unlautere Mittel entzogen. Passiert dies im internationalen Rahmen über das Internet, im Vorfeld oder während eines Krieges, ist auch die Diffamierung als Mittel des Cyberwar anzusehen.

2.2.3 Spam

Als Spam werden eMails angesehen, die meist willkürlich an alle möglichen Postfächer gesendet werden. Der Inhalt dieser Mails besteht meist aus Werbung und dubiosen Angeboten aller Art von angeblichen Privatleuten.

2.2.4 Manipulation von Bestandsdaten

Viele Institutionen und Entscheidungsträger arbeiten vermehrt mit digitalen Informationen. Versicherungen berufen sich auf das gespeicherte Wissen in ihren Datenbanken. Staatliche Einrichtungen arbeiten mit elektronischer Kommunikation über das Internet und halten Webseiten vor, die sie im Internet repräsentieren. Banken führen ihre Kundenkonten schon lange nicht mehr hauptsächlich auf abgezählten Zahlungsmitteln in ihren Tresoren sondern auf Grund von Bits und Bytes, die den Kontostand jedes Einzelnen darstellen. Soll und Haben sind lediglich Zahlen, gespeicherte Informationen in einer Tabelle. Eine Zahl unter vielen anderen.

Die Datenbanken, die durch die Arbeiten solcher Gruppierungen entstehen sind höchst sensibel. Lediglich digital hinterlegt sind diese außerdem höchst angreifbar. Ein Tastendruck und aus dem 12.000 Haben wird ein -12.000 Soll. Selbstverständlich gibt es hier weitreichende Sicherheitsmaßnahmen. Eigens

für die Internetsicherheit zuständige Firmen werden in die Prozesse mit eingebunden und vielfältige technische Raffinessen sollen ein unautorisiertes Ändern oder Entfernen der Daten verhindern. Jedoch ist ein Angriff durch einen Computer über das Internet einer breiteren informierten Masse möglich, als es ein physischer Einbruch in eine solche Institution wäre. Körperlicher Einsatz im Sinne der Kriminalität ist nicht mehr von Nöten und lediglich Computerwissen und eine elektronische Verbindung ersetzen die Gefahr, sein Vorhaben in persona vor Ort umzusetzen.

2.2.5 Manipulation von technischen Abläufen

Wahrscheinlich noch populärer als die Löschung von Miloševićs Konten im Rahmen von Datenmanipulation ist der Virus „Stuxnet“. Das Programm wurde hauptsächlich auf Rechnern des Typs PCS-7 der Firma Siemens gefunden. Der Löwenanteil dieser infizierten PCs steht im Iran, welche für die Steuerung der Anlagen der dortigen Atomindustrie verwendet werden. Nach eingehenden Untersuchungen schien der Virus mit Hilfe eines USB-Stick in eine der Anlagen geschleust worden zu sein, um die Geschwindigkeit der Anreicherungszentrifugen zu verändern und den daran anliegenden Sensoren ein falsches Signal zu überlagern. Dies hätte zur Folge, dass sich die Zentrifugen nach und nach selbst zerstören.[10]

2.2.6 Lauschangriff

So wie Telefonnetze in früheren Agentenfilmen angezapft werden, ist es auch heute noch mit Übertragungswegen der IT-Technologie möglich, Informationen auf ihrem Transportweg abzufangen und auszuwerten. Die Funkstrecken von mobilen Endgeräten sowie Netzwerkkabel und W-LAN-Verbindungen haben jeweils eigene Schwachstellen, die mit den unterschiedlichsten Mitteln geschützt werden müssen. Die breite Bevölkerung ist sich dieser Gefahr jedoch kaum bewusst, sodass es immer wieder zu erfolgreichen Lauschangriffen kommt.

10 Langner, Ralph: Cracking Stuxnet, A 21st-century cyber weapon, 2001, [Lan11]

2.2.7 Menschliches Versagen/Social Engineering

Social Engineering bedeutet das Ausnutzen personeller Strukturen in einem Betrieb oder einer Institution. Die Infektion eines USB-Sticks eines Mitarbeiters zum Beispiel gehört zu dieser Art des Angriffes.

2.2.8 Drive-By-Exploits

Drive-By-Exploits beschreibt die Infizierung von PCs über das Internet, bei denen keine aktive Beteiligung des Nutzers gegeben sein muss. Der klassische Fall, dass ein Benutzer auf ein Werbebanner in seinem Internetbrowser klickt und sich damit unwissentlich schädliche Software herunterlädt ist nicht mehr gegeben. Mittlerweile reicht es aus, dass die Werbung lediglich im Browser angezeigt wird um die Installation von Schadsoftware zu ermöglichen. Das Opfer wird somit „im Vorbeigehen“ zum ausgesuchten Ziel dieser Attacke.

2.2.9 Botnetze

Botnetze sind Zusammenschlüsse infizierter (Privat-)Rechner, die von Dritten ferngesteuert werden können. Genutzt werden diese Botnetze um beispielsweise Spammails zu verschicken, Denial-of-Service-Attacken durchzuführen oder die Spur einer Cyberattacke durch komplexe Weiterleitungen zu verwischen.

2.2.10 Identitätsdiebstahl und -missbrauch (Trojaner)

Die Verwendung eines Benutzernamens in Verbindung mit einem Passwort ist die gängigste Methode eine Person auf einer bestimmten Internetseite auszuweisen. Diese und weitere sensible Daten sind für einen Dritten in dem Moment von wert, wenn die Daten die Verwaltung von Beständen wie einem Bankkonto, eines Accounts bei einem Versandhaus oder ähnlichem ermöglichen. Ungewollte Auktionsteilnahmen auf einschlägigen Seiten oder Masseneinkäufe bei Versandhäusern sind oft die Folge nach Diebstahl der

persönlichen Daten. Die jeweiligen Schädigungen hängen natürlich davon ab, wofür diese genutzt werden.

3 Klassifizierung von Cyberattacken

Um Angriffen zu entgehen oder entgegen zu wirken, müssen sie zuallererst als solche erkannt werden. Staaten und Regierungszusammenschlüsse wie die USA, die NATO oder die EU haben deshalb ihre eigenen Kategorien für Angriffe aus dem Netz gebildet. 1997 wurde zu diesem Zweck unter Präsident Clinton beispielsweise eine solche Kategorisierung in den USA erstellt. Dieser Artikel[11] teilt die Cyberattacken in fünf grundsätzliche Klassen auf:

Ein Angriff...

- ...auf eine spezifische Datenbank.
- ...auf ein Netzwerk mit dem Ziel, Zugang zu diesem zu erhalten.
- ...mit dem Ziel der Spionage.
- ...mit dem Ziel, bestimmte Teile eines System außer Funktion zu setzen.
- ...auf ein System um diesem durch Fremdeinfluss schaden zuzufügen.

Deutschland reagierte 1991 auf die wachsende Bedrohung mit der Bildung des „Bundesamtes für Sicherheit in der Informationstechnik“ (BSI). Das Bundesamt bringt seitdem jährlich einen Lagebericht heraus, der die unterschiedlichen Gefährdungen der Cybersicherheit auflistet und ihnen eine aktuelle Bedeutung beimisst.

11 Cordesman, Anthony H.: CYBER-THREATS, INFORMATION WARFARE ,AND CRITICAL INFRASTRUCTURE PROTECTION, Defending the U.S. Homeland, 2002, [Cor02]

Auch die NATO, die vor allem ein militärischer Staatenbund ist, setzt sich mit dem Thema der Cybersicherheit auseinander. In einem der strategischen Papiere zum Thema der internationalen Sicherheit heißt es unter Anderem: „...cyber attacks are one of the top three threats facing the Alliance.“[12]

Die Stellung der USA zum Thema Cyberwar oder anders „Informational Operations“, zeigt sich recht deutlich aus dem Bericht „Warfighting in Cyberspace“: „Unsere momentanen und potentiellen Gegenspieler haben eine klare Vorstellung vom militärischen Potential des Cyberspace und der Einflussgröße dieses Mediums.“[13] Es ist nicht weiter überraschend, dass die Ziele, die das US-amerikanische Militär für diese Bedrohung bereithält, von offensiver Natur ist: „Das ultimative strategische Ziel [...] ist es, die Handlungsfreiheit den vereinigten Staaten im Cyberspace zu sichern und sie dem Feind zu verwehren.“[14]

In den strategischen Papieren der Staaten und -bündnisse werden die Probleme in Handlungsbedürfnisse aufgeteilt, die aus den potentiellen gefahren resultieren. Die US-amerikanischen Kategorien hierzu unterscheiden sich heutzutage nicht groß von denen von 2002: „...im Sinne von militärischen Operationen, sind die Netzwerk Operationen in Computer-Netzwerk-Angriffe, Computer-Netzwerk-Verteidigung und damit einhergehende Datenbeschaffungsmaßnahmen unterteilt.“[15]

Die bereits über zehn Jahre alte Einschätzung in Cordesmans Buch ist also trotz der sich schnell ändernden Welt der Informationstechnologie so gut wie aktuell geblieben. Im Allgemeinen kristallisieren sich den Institutionen zufolge diese stets wiederkehrenden Probleme heraus:

12 Working with the private sector to deter cyber attacks, 2011, [NAT11]

13 Originaltext: „Our current and potential adversaries clearly understand the military potential of cyberspace and the expansive power of the medium.“, Alexander, Keith B.: Warfighting in Cyberspace, S.59, 2007, [Ale07]

14 Originaltext: „The ultimate strategic objective of these operations is to ensure U.S. freedom of action in cyberspace and to deny the enemy the same.“, ebd.

15 Originaltext: „...for the purpose of military operations, computer network operations are divided into computer network attack, computer network defense, and related computer network exploitation enabling operations“, Joint Publication 3–13, Information Operations, February 13, 2006, URL: www.dtic.mil/doctrine/jel/new$_p$*ubs*/*jp*3$_1$3.*pdf*

- Die Gefährdung der Datensicherheit (Verlust und Manipulation)
- Die potentielle Gefahr des Zugriffs Dritter auf Netzwerkstrukuren (Schädigung)
- Fremder Einfluss auf Handlungsspielräume (Beschränkung)
- Distribution von Fehlinformation (Diffamierung, Störung der internen Kommunikation, Spaltung)

Diese recht allgemein gehaltene Auflistung kann durch den Aufbau der Computertechnik und ihrer klassischen Daten- und Netzwerkstruktur auf die meisten Cyberttacken angewendet werden. Zusätzlich gilt jedoch zu unterscheiden, von wem der Angriff erfolgte, und wem er galt. Viele Cyberattacken sind nicht nur schlecht zurück zu verfolgen, sondern können, wenn der schädliche Programmcode allgemeingültig gehalten wird, sogar nicht einmal einem konkreten Opfer zugeschrieben werden. Wenn in einer großen Industrienation beispielsweise durch eine Cyberattacke der Strom ausfällt, kann man deshalb nicht ohne Weiteres die Absicht dahinter erkennen.

Jedoch lassen sich auch hier bestimmte Angriffsrichtungen im Vorfeld abstecken. Abbildung 3.1 zeigt, wie komplex die Hintergründe für eine Cyberattacke, allein durch die Vielzahl potentieller Beteiligter, sein können. (Der Umstand, dass Wirtschaftsunternehmen eine Cyberattacke initiieren, wurde hier außer Acht gelassen. Auch wenn dies theoretisch passieren kann, ist ein Präzedenzfall nicht bekannt.)

Wie im Vorfeld beschrieben, ist jeder Computerbesitzer ein denkbarer Teilnehmer dieses Schemas. Auf welcher Seite dieser steht ist lediglich vom technischen Wissen und der Bereitschaft abhängig, dieses zu nutzen.

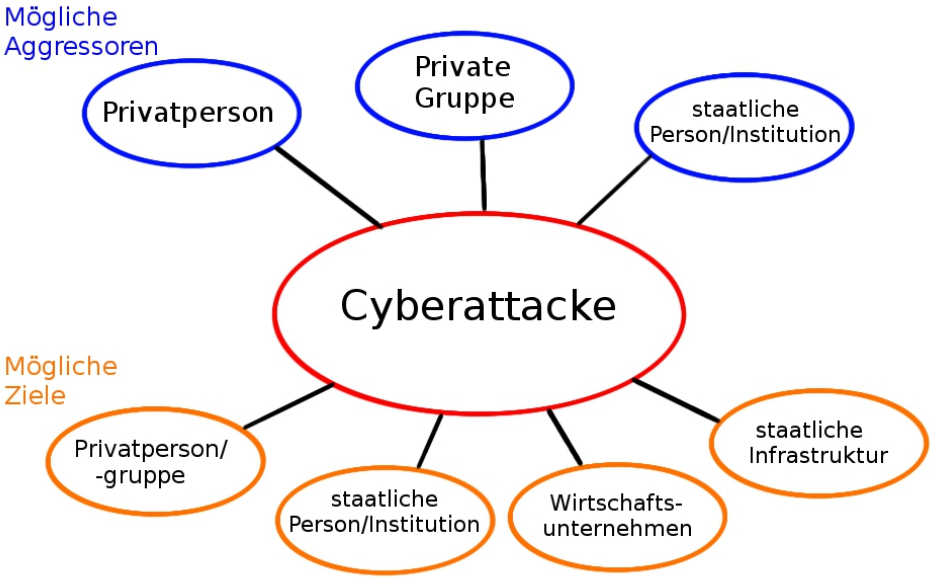

Abbildung 3.1: Typische Aggressor/Opfer-Beziehung von Cyberattacken [16]

Die vier grundlegenden Angriffsarten und die Aggressor-Opfer-Beziehungen bilden die Basis für eine schier endlose Zahl möglicher Auswirkungen. Welche dies sind und wie im allgemeinen dagegen vorgegangen wird, wird in Kapitel 4 näher betrachtet.

16 Simsch, Jonathan, 2012

4 Auswirkungen und Gegenmaßnahmen

Die Auswirkungen eines Cyberkrieges lassen sich bei genauerer Betrachtung durchaus mit denen eines real geführten Konfliktes vergleichen. Strategien der Kriegsführung sind teilweise deckungsgleich und lediglich eine Fortführung realer Kriegshandlungen mit anderen Mitteln. Eine physische Bedrohung, durch Zeilen digitalen Programmcodes, erscheint auf den ersten Blick absurd. Die in Kapitel 2 angesprochene Manipulation von technischen Daten ist hierzu aber durchaus in der Lage. Die Änderung von Fahrstuhlsteuerungssoftware oder das Eingreifen in die Regelung von Wasserschleusen sind nur zwei von zahllosen Beispielen.

Konzepte wie das „Smart Grid“, welches die technisch/organisatorische Verbindung von Stromerzeugern und -verbrauchern steuern soll sind dankbare Ziele. Der Trend für die Automatisierung macht vor keinem Gebiet halt, wodurch bereits viele Bereiche im privaten, wirtschaftlichen und politischen Raum stark vom digitalen Informationsfluss abhängig sind. Zusätzlich wird der Zugang zu privaten Daten durch das vermehrte speichern auf externen, nicht eigenen, Rechnern(sog. Clouds), noch einfacher als ohnehin schon.

Psychische Gefahren lauern hingegen eher in der Manipulation von Inhalten. Diffamierung oder politisch motivierte Propaganda können, gezielt auf einzelne Personen gerichtet, für psychischen Schaden sorgen. Psychologische Kriegsführung funktioniert durch die Computertechnologie schneller und zielgerichteter. Propagandamaßnahmen bekommen unter Umständen sogar einen persönlichen Rahmen, da die Daten der Opfer unter Umständen schon von Dritten ausgelesen wurden und nun für Ihre Zwecke verwendet werden.

Die reale Gefahr eines Angriffes aus dem Netz hat heutzutage das Potential, ähnlich Bedrohlich zu wirken, wie das Lagern einer Atombombe. Die

Blockierung lebenswichtiger Infrastrukturen wie der Stromversorgung, der Wasserversorgung oder gar der computergesteuerten Verkehrsführung ist durch die globale Vernetzung mittlerweile denkbar. In Filmen wie „Stirb langsam 4.0“ wird ein mehrstufiger Angriff auf eben jene Strukturen durchgeführt, der ganze Amerikanische Großstädte binnen Stunden ins Chaos stürzt. Was in diesem Maße noch als Fiktion abgetan werden kann, spiegelt in bestimmten Grenzen jedoch ein reales Risiko wieder.

Durch die Anonymität der globalen Vernetzung ist es selbst gut ausgebildeten Computerexperten oft nicht möglich, die Quelle eines Angriffes zurück zu verfolgen. Die Schädigungen kommen oft unvorhergesehen und die Aggressoren bleiben, durch zwischengeschaltete Rechner und Botnetze, im Hintergrund. Da die Angriffe oft durch Sicherheitslücken möglich werden, die von Programmiererseite noch gar nicht festgestellt wurden, ist es fast unmöglich sie hervorzusehen. Personal, das ungeschult ist kann durch Personal Engineering unwissend Programme in das anzugreifende System einschleusen und somit einen Zugang für Dritte schaffen. Die eigentlich vertrauenswürdige Person wird so zu einem schlecht zu tilgenden Sicherheitsproblem. Dem entgegenzuwirken ist oft mühsam und nur durch besondere Schulungen zu bewältigen. Der „National Cyber Security Awareness Month“ der enisa[17] ist ein Versuch, die Bevölkerung auf solche Sicherheitsrisiken aufmerksam zu machen. Im Ernstfall sind solche Aktionen jedoch kaum von Wert, wenn es darum geht sensible Daten in Regierungen und Firmen zu schützen. Um vor Cyberattacken gefeit zu sein bedarf es also einer Vielzahl von Maßnahmen, die in alle möglichen Richtungen wirken.

Die vielfältige Verwundbarkeit und der Umstand, dass die Personen hinter den Attacken kaum zu erfassen sind stellt politische Führungen und die Wirtschaft vor ein höchst brisantes Dilemma: Wie sieht eine umfassende Verteidigung aus?

Betrachtet man die Frage auf Staatsebene bleiben im Grunde nur zwei Möglichkeiten. Erstens könnte ein Staat die nötige Infrastruktur, in Form von hochgezüchteter IT-Technik im großen Umfang errichten, um sich im Ernstfall zu verteidigen. Passivität führt allerdings dazu, Angriffe voraussagen zu müssen und bereits passende Gegenmaßnahmen parat zu haben. Wie oben

17 Die enisa ist die „European Network and Information Security Agency“ und ist von der EU für den Austausch und die Verbesserung der Informationssicherheit ins Leben gerufen worden. (`www.enisa.europa.eu/`)

beschrieben ist dieser Ansatz aber kaum umzusetzen. Abschreckungen durch Bestrafung ist in diesem Zusammenhang auch kein etabliertes Mittel, da begründete Schuldzuweisungen oft nicht möglich sind.

Mit der Anforderung, möglichst nicht verwundbar gegenüber Angriffen auf dem Netz zu sein, bleibt einem Staat im Prinzip nur noch die zweite Möglichkeit: Ein präventiver Erstschlag. Hier stellt sich jedoch die Frage, wen man riskieren kann anzugreifen, ohne selbst Schaden zu erleiden und welchen Nutzen man daraus ziehen kann. Des weiteren ist in vielen Fällen unklar, ob eine solche Maßnahme gerechtfertigt ist.

Auf diesem Hintergrund sind groß angelegte Errichtungen von IT-Technik, vergleichbar mit dem Bau einer Anreicherungsanlage für Uran. Unter dem Vorwand einer friedlichen Nutzung aufgebaute Strukturen können den Verdacht nähren, Anderes im Sinn zu haben. Gegenseitiges Misstrauen erzeugt politische Spannungen und erschwert diplomatische Bemühungen.

Die gleichzeitige Verwundbarkeit von Politik und Wirtschaft ist ein weiterer Faktor dieser Problematik. Der Cyberwar bleibt nicht auf militärische Strukturen beschränkt. Die Angriffe von chinesischer Seite gegen Google sind nur eine Version von militärisch einzustufenden Angriffen auf wirtschaftliche Einrichtungen.[18] So, wie ein Bomber seine Bomben überwiegend auf Waffenfabriken und Kasernen fallen lassen soll, so ist der Gedanke eines Computerangriffs auf führende IT-Unternehmen analog. Angriffe von staatlicher Seite auf entsprechende Firmen einer anderen Regierung sind deshalb keine Seltenheit mehr. (Um ein Bild der tatsächlichen Situation zu bekommen richtete das BSI Ende 2012 eine Meldestelle für deutsche Unternehmen ein, um Berichte über Cyberangriffe, auf die Industrie, gebündelt zu sammeln[19])

18 Drummond, David: A new approach to China, 2010, [Dru10]

19 Das Meldeformular ist unter `https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/Meldestelle/meldestelle_node.html;jsessionid=F39938FE12E47D104BBA1D550466F821.2_cid243` zu finden

5 Fazit

Die Computertechnologie hat der Menschheit in den letzten Jahrzehnten eine kaum fassbare Bandbreite an Möglichkeiten und technischen Neuerungen gebracht, ohne die wir heute wahrscheinlich anders leben würden. Der ständig mögliche Zugriff auf Informationen, die Verbindung von Menschen und Einrichtungen aller Art weltweit und die Automatisierung, die Aufgaben übernimmt, zu denen der Mensch alleine gar nicht fähig wäre, sind Meilensteine unserer Geschichte. Computer haben die Entwicklung unseres Planeten auf ein Maß beschleunigt, dass sich wohl erst in ein paar Jahrzehnten umfassend abschätzen lässt.

So erfolgreich der Computer ist, so angreifbar scheint er im Hinblick auf die vorangegangene Aspekte auch zu sein. Das Internationale Ausmaß unserer Kommunikationstechnologie eröffnet weniger wohlwollenden Parteien eine neue Angriffsfläche in Form eines jeden Rechners auf der ganzen Welt. Täter und selbst Opfer sind in der unüberschaubaren Wechselwirkung meist kaum auszumachen und es herrscht eine Anonymität, die die Eindämmung dieser Problematik enorm erschwert.

Das Internet, oder der Cyberspace, sind ein schützenswertes Gut, das uns viele Chancen einräumt, die wir ohne sie nicht hätten. Wird dieses Gut durch Angriffe korrumpiert, kann die globale Vernetzung in seiner jetzigen Form auf Dauer kaum existent bleiben. In diesem Falle besteht die Gefahr eines permanenten Verlustes der momentanen digitalen Infrastruktur. Aus diesem Umstand heraus, sind Schutzmaßnahmen unumgänglich, was in Zukunft ständige Konfliktbildung provoziert. Der Computer wird, im Gegensatz zur Atombombe, stets als Waffe benutzt werden, da die Dosierung des Einschlages so gut zu kontrollieren ist. Umso wichtiger ist es, die Verteidigung des Internets voranzutreiben und die Zukunft der fortschrittlichsten unserer Technologien zu gewährleisten.

Literaturverzeichnis

[Ale07] Alexander, Keith B.: *Warfighting in Cyberspace*, 2007.

[Ben99] Bendrath, Ralf: *Der Kosovo-Krieg im Cyberspace*. http://www.iwar.org.uk/iwar/resources/kosovo.htm, 1999.

[Cor02] Cordesman, Anthony H.: *CYBER-THREATS, INFORMATION WARFARE ,AND CRITICAL INFRASTRUCTURE PROTECTION, Defending the U.S. Homeland*. Praeger Publishers, 2002.

[Dru10] Drummond, David: *A new approach to China*. http://googleblog.blogspot.de/2010/01/new-approach-to-china.html, 2010.

[Hyp11] Hypponen, Mikko: *Fighting viruses, defending the net*. http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html, 2011.

[Klo11] Kloiber, Manfred; Welchering, Peter: *Militärs suchen Strategien gegen Cyberattacken*. http://www.faz.net/frankfurter-allgemeine-zeitung/technik-und-motor/manfred-kloiber-und-peter-welchering-militaers-suchen-strategien-gegen-cyberattacken-1596087.html, 2011.

[Lan11] Langner, Ralph: *Cracking Stuxnet, a 21st-century cyber weapon*. http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html, 2011.

[NAT11] NATO: *A new approach to China*. http://www.nato.int/cps/en/natolive/news_80764.htm?selectedLocale=en, 2011.

[PDDS12] Prof. Dr. Dr. Saalbach, Klaus-Peter: *Cyberwar, Grundlagen-Methoden-Bespiele(Version 5.0)*, 2012.