Cyberwar zwischen Fiktion und Realität – technologische Möglichkeiten

Christian Reuter, Thea Riebe, Larissa Aldehoff, Marc-André Kaufhold und Thomas Reinhold

1 Einleitung

Im Dezember 2017 wurde eine Invasion des deutschen Regierungsnetzwerks entdeckt; dieses vernetzt Bundesministerien und Behörden (vgl. Reinhold 2018a). Die Angreifer nutzten das Intranet der Hochschule des Bundes für öffentliche Verwaltung und der Bundesakademie für öffentliche Verwaltung als Einfallstor. Dieses ist der am wenigsten gesicherte Teil des Systems, da externe Teilnehmerinnen und Teilnehmer auch außerhalb der Einrichtung darauf zugreifen müssen, beispielsweise für Fortbildungen des Auswärtigen Amtes. Wahrscheinlich sollte der erste Eingriff dazu dienen, das Netzwerk weiter zu durchdringen. Um sich Bewegungsfreiheit im Intranet zu verschaffen, wurden systematisch Administratorrechte in Anspruch genommen. Bisher konnte nicht geklärt werden, ob sich Teile der genutzten Schadsoftware weiterhin im System befinden (vgl. Mascolo et al. 2018).[1]

1 Der Beitrag basiert auf Reuter et al. (2019).

I.-J. Werkner und N. Schörnig (Hrsg.), *Cyberwar – die Digitalisierung der Kriegsführung*, Gerechter Frieden,
https://doi.org/10.1007/978-3-658-27713-0_2

Dieser Vorfall ist ein gutes Beispiel für die zunehmende Relevanz von Informationstechnik für Frieden und Sicherheit (vgl. Reuter 2019). Die Innovationen naturwissenschaftlicher und technischer Forschung wurden schon immer für militärische Zwecke genutzt und haben so die Kriegsführung stark beeinflusst. Diese Erkenntnis trifft auf Wissenschaftler und Mathematiker wie Archimedes (287-212), Leonardo da Vinci (1452–1519) und Isaac Newton (1643–1727) zu. Die erste planvolle Einbeziehung technischen Wissens in das Militär fand in der Rekrutierung von Ingenieuren nach der Französischen Revolution statt. Im Ersten Weltkrieg wurden dann Chemiker, Mathematiker, Physiker und Ingenieure systematisch in die Produktion von Kriegsmaterial integriert (vgl. Altmann et al. 2010, S. 411f.). Weiterhin wurden während des Ersten Weltkriegs Telefone und Radiokommunikation auf den Schlachtfeldern eingeführt. Seitdem ist die IT mit ihren weitreichenden Entwicklungen in Krisen, Konflikten und Kriegen zunehmend wichtiger geworden (vgl. Bernhardt und Ruhmann 2017, S. 364ff.).

Gewaltsame Konflikte können in verschiedenen Domänen geführt werden. Neben Land, See, Luft und dem Weltraum ist nun der sogenannte Cyberspace eine von ihnen. Deshalb ist die Resilienz von IT-Infrastrukturen von wachsender Bedeutung. Dennoch berücksichtigen Sicherheitsstrategien die spezifischen Charakteristika von IT nur unzureichend:

- Viele der involvierten Akteure (die die Gruppe potenzieller Aggressoren darstellen) sind entweder Individuen oder Teil des Privatsektors.
- Die Zuschreibung (Attribution) von sicherheitsbedrohenden oder offensiven Aktivitäten ist schwierig, da die Identität der Sicherheitsbedrohung nicht bekannt ist.
- Sicherheitsbedenken und internationale Proliferation – das heißt die Verbreitung von militärischen oder militärisch nutzbaren

Technologien innerhalb und zwischen Staaten (vgl. Altmann 2019) – erhöhen das Risiko von Militäreinsätzen als präventives Mittel (vgl. Chivvis und Dion-Schwarz 2017).
- Viele Technologien können auch als Waffe oder Teil eines Waffensystems missbraucht werden. Deshalb ist ihnen das Risiko, zweckentfremdet zu werden, um einer signifikanten Anzahl von Menschen Schaden zuzufügen, inhärent. Die *Dual Use*-Problematik (vgl. Riebe und Reuter 2019) ist insbesondere deshalb von zunehmender Relevanz für die IT, weil die militärische Verwendung von IT-Systemen und Infrastrukturen Phänomene wie den Cyberwar, den Informationskrieg (vgl. Ruhmann und Bernhardt 2019), (terroristische) Propaganda, *Fake News* (vgl. Kaufhold und Reuter 2019), Datenspionage und *Hacking* (vgl. Herrmann 2019) einschließt.

Der Beitrag nimmt diese Herausforderungen und Ansatzmöglichkeiten für Lösungen in den Blick. Grundlegend dafür sind eine genauere Differenzierung der verwendeten Begrifflichkeiten sowie eine Darstellung der dahinterstehenden Konzepte. Darauf aufbauend werden die jeweils unterschiedlichen Formen des schadhaften Wirkens im Cyberspace, ihre Akteure und Motivationen, die sich in der Wahl der entsprechenden technischen Hilfsmittel niederschlagen, analysiert. Der Beitrag beleuchtet dabei auch die wichtigsten technischen Probleme zum Schutz im Cyberspace, die Angreifer bei der Wahl ihrer Taktik und Angriffswerkzeugen entgegenkommen.

2 Von der Informatik zur Cybersicherheit

Seitdem Computer in der Lage sind, Daten auszutauschen, ist die Sicherheit dieser Daten eine Herausforderung. In den letzten Jahren hat die Bedrohung der Datensicherheit aufgrund der Vernetzung und Kollaborativität von Systemen sowie der Einführung von *Cloud Computing* zugenommen. Die folgenden Abschnitte erläutern, was unter Sicherheit im Kontext der Informatik zu verstehen ist, und gehen auf die militärische Perspektive dieser Herausforderungen ein.

2.1 IT-, Informations- und Cybersicherheit

Den Begriff der Sicherheit gibt es in der Informatik seit langem. Dessen Perspektive hat sich in den vergangenen Jahren unter dem Eindruck des Cyberspace und von Cyberattacken jedoch verändert, stärker differenziert und sich so in der Wahl der Begrifflichkeiten niedergeschlagen. Eine sehr technische, klassische Herangehensweise bietet die Norm ISO/IEC 27001, die IT-Sicherheit definiert als

> „Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; zusätzlich können andere Eigenschaften wie Authentizität, Verantwortlichkeit, Nichtabstreitbarkeit und Zuverlässigkeit auch involviert sein" (ISO 27001 2015).

Dabei stellten die Autorinnen und Autoren vor allem die Sicherheit der „technischen Information" (heute würde man von Daten sprechen) und die einzelnen, in aller Regel nicht miteinander verbundenen IT-Systeme, auf denen diese Daten verarbeitet werden, in den Vordergrund. Entsprechend wurde hier von Informationssicherheit gesprochen; ein Begriff, der sich mit dem Aufkommen des Internets zum knapperen Begriff der IT-Sicherheit gewandelt

hat. Mit der zunehmenden Kommerzialisierung des Internets, neuer Dienste, mobiler internetfähiger Geräte sowie der damit einhergehenden massiven Vernetzung und dem konstanten Datenaustausch wurde der Begriff des Cyberspace als Beschreibung der Gesamtheit dieser Geräte und deren Interaktionen geprägt. Mit dieser Entwicklung wurde jedoch auch deutlich, dass technische Sicherheit in einem größeren Maßstab gedacht werden muss, der die Verwundbarkeiten aufgrund der Vernetzung von IT-Geräten sowie deren technischen wechselseitigen Abhängigkeiten in den Fokus nimmt. Der dafür geprägte Begriff der Cybersicherheit wird dementsprechend zunehmend synonym zu dem Begriff der Informationssicherheit verwendet. Jedoch ist zu konstatieren:

> „Cybersicherheit geht über die Grenzen der traditionellen Informationssicherheit hinaus und umfasst nicht nur die Absicherung von Informationsressourcen, sondern auch die anderer Güter sowie der Person selbst. Die Informationssicherheit bezieht sich, was die menschliche Komponente anbelangt, meist lediglich auf die Rolle(n) von Menschen im Sicherheitsprozess" (von Solms und van Niekerk 2013, Übersetzung d. Verf.).

Nach dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bezieht sich Cybersicherheit auf alle Aspekte der Sicherheit in Informations- und Kommunikationstechnologien (*Information and Communication Technologies*, ICT). Dabei wird

> „das Aktionsfeld der klassischen IT-Sicherheit […] auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein" (BSI 2017).

Als IT-Sicherheit definiert das Bundesamt für Sicherheit in der Informationstechnik (2017):

> „einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind".

IT-Sicherheit ist also ein Zustand, „in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind" (BSI 2017). Der jährliche Lagebericht über IT-Sicherheit in Deutschland analysiert anhand detaillierter Beispiele die aktuelle Lage der IT-Sicherheit, Gründe für Cyberangriffe sowie angewendete Mittel und Methoden (vgl. BSI 2016). Er führt Schwachpunkte in den Bereichen *Cloud Computing*, Software und Hardware, Kryptographie, mobile Kommunikation, Standardisierung und Internetinfrastruktur auf und erläutert Gründe sowie kontextuelle Faktoren. Folgend findet sich eine Übersicht über die vom Bundesamt für Sicherheit in der Informationstechnik aufgeführten Mittel und Methoden von Cyberangriffen (vgl. BSI 2ß16) sowie potenzieller Schutzmechanismen (vgl. Herrmann 2019).

Gegenüber IT- und Cybersicherheit stellt Informationssicherheit ein umfassenderes Konzept dar, dass das Schützen von Informationen, die auf Papier oder Computern gespeichert sind, einschließt (vgl. BSI 2013). Laut ISO 27001 (2015) impliziert es Sicherheitskontrollen, insbesondere auf administrativer, logischer und physischer Ebene.

Die Entdeckung der Stuxnet-Software und der seit 2013 anhaltende NSA-Skandal zeigen die Signifikanz möglicher Invasionen durch staatliche Organisationen auf: Diese haben das Potenzial, nicht nur die Privatsphäre, sonders die gesamte IT-Infrastruktur zu bedrohen (ausführlicher hierzu Hollick und Katzenbeisser 2019).

Tab. 1 Überblick über gängige Mittel und Methoden von Cyberangriffen sowie Schutzmechanismen

Mittel und Methoden von Cyberangriffen	Schutzmechanismen
• Schadsoftware • Ransomware • Social Engineering • Advanced Persistent Threats (APTs) • Spam • Botnetze • Distributed-Denial-of-Service (DDoS) • Drive-by-Exploits und Exploit-Kits • Identitätsdiebstahl • Seitenkanalangriffe	• Anwendungssicherheit (z. B. Antivirus-Software, sichere Programmierung, Sicherheitsdesign, sichere Betriebssysteme) • Angriffserkennung und -prävention • Autorisierung und Zugriffskontrolle • Authentifizierung und Identifikation • Protokollierung • Durchführung von Sicherheitskopien • Netzwerksicherheit (z. B. durch Firewalls) • Sichere Mobile Gateways

Quelle: Eigene Darstellung auf der Basis des BSI (2016).

2.2 Militärische Vorkehrungen für den Cyberspace

Im Lichte dieser Entwicklung überrascht es nicht, dass mehr und mehr Verteidigungsministerien den Cyberspace – neben Land, Luft, See und Weltall – als eine eigene Domäne etablieren. So haben mittlerweile alle NATO-Mitgliedstaaten, darunter auch Deutschland (vgl. BMVg 2016), den Cyberspace als eine militärische Domäne anerkannt; damit können sie Cyberoperationen als Angriff einstufen oder selbst in Aktion treten (vgl. NATO 2016). Als Herausforderung erweist sich jedoch die Abstimmung und

Koordinierung von Fähigkeiten, Materialien und Zuständigkeiten bei der gemeinsamen Abwehr von Bedrohungen aus dem Cyberspace sowohl zwischen den Staaten als auch auf nationaler Ebene, wie dies in den jährlichen *Locked Shields*-Übungen deutlich wird (vgl. Backhaus und Wanninger 2018).

Dabei bezeichnet Cyberspace die

> „Umgebung, die durch physische und nicht-physische Komponenten gebildet, und durch die Nutzung von Computern sowie dem elektromagnetischen Spektrum zum Speichern, Modifizieren, und Austauschen von Daten unter Nutzung von Computernetzwerken, charakterisiert wird" (Schmitt 2013, Übersetzung d. Verf.).

Ähnlich definiert das Bundesministerium des Innern Cyberspace als den

> „virtuellen Raum aller IT-Systeme, die global auf Datenebene verknüpft sind. Die Basis des Cyberspace ist das Internet als universelle und öffentlich zugängliche Verbindung und transparentes Netzwerk, das durch beliebig viele zusätzliche Datennetzwerke ergänzt und erweitert werden kann. IT-Systeme in einem isolierten virtuellen Raum sind nicht Teil des Cyberspace" (BMI 2011).

Da es im Cyberspace keine nationalen Grenzen gibt, sind innere und äußere Sicherheit kaum voneinander trennbar. Zu dieser Komplexität trägt zusätzlich bei, dass die darin tätigen Akteure sehr verschiedene Fähigkeiten, Intentionen und Ressourcen einbringen. Hinsichtlich der benötigten Ressourcen lässt sich kaum zwischen defensiven und offensiven Mitteln unterscheiden. Diesem Dilemma unterliegen auch Ansätze des Aufbaus rein ziviler Verteidigungsmechanismen. Zudem bleiben Bedrohungen nicht notwendigerweise auf den Cyberspace begrenzt, da Auseinandersetzungen auch vom Cyberspace auf andere Domänen und dort in bewaffnete Konflikte übergehen können. Des Weiteren exis-

tieren sogenannte *Overlay*-Netze, die oberhalb der existierenden Infrastruktur als logisches Netz zu verorten sind. Solche Netze können *Darknets* sein, auf die mit spezifischer Software, mit Konfigurationen oder speziellen Autorisierungen zugegriffen werden kann. Der Zugriff auf diese Netzwerke erfolgt in aller Regel über Anonymisierungsnetzwerke wie beispielsweise TOR (vgl. Mansfield-Devine 2009; Denker et al. 2019), die Nutzerinteraktionen und deren Zuordenbarkeit verschleiern.

3 Technologische Möglichkeiten des Cyberwar

Ähnlich wie der Begriff der Cybersicherheit umfasst der Begriff des Cyberwar sehr viele unterschiedliche Aspekte, die durch ihre jeweils verschiedenen Angriffsformen, Angriffspunkte, Akteure und Motivationen gekennzeichnet sind. Die jeweilige Konstellation entscheidet dabei maßgeblich über die Art des ausgewählten Angriffswerkzeuges. Im Folgenden werden die Charakteristika und exemplarisch einige technische Möglichkeiten dargestellt.

3.1 Cyberkrieg und Cyberangriffe

Das Konzept des Cyberkrieges ist umstritten. Bisher hat es keinen Vorfall gegeben, der international offiziell als Cyberkrieg charakterisiert worden ist. Nichtsdestotrotz muss betont werden, dass Cyberattacken im Rahmen zwischenstaatlicher Konflikte zunehmen. Das betrifft nicht nur Individuen und Unternehmen, sondern auch Regierungen und öffentliche Verwaltungseinrichtungen. Die folgenden Ausführungen beziehen sich auf die letzten beiden Institutionen.

Heute ist die üblichste Form von Cyberangriffen der Versuch, illegal in Computer einzudringen, um Daten zu manipulieren oder zu stehlen (vgl. Neuneck 2017). Die meisten Cyberangriffe, die mit *Proxies* (Zombies) oder *Botnets* eines Zombie-Computers ausgeführt werden, sind *Distributed Denial of Service*-Angriffe (DDoS). Diese können die virtuelle – und insbesondere im Falle einer engen Verbindung die physische – Infrastruktur wie etwa Banken, das Gesundheitssystem oder die Stromversorgung beeinträchtigen (vgl. Gandhi et al. 2011), indem sie IT-Systeme mit unzähligen, gleichzeitig ausgelösten regulären Anfragen überlasten. Ein berühmtes Beispiel hierfür ist die DDoS-Attacke auf Estland im Jahr 2007, bei der die Webseiten des estnischen Parlaments, des Präsidenten und der Regierung sowie der beiden größten estnischen Banken und Nachrichtenportale nicht zugänglich waren (vgl. Hansen und Nissenbaum 2009). Die Angreifer konnten nie identifiziert werden (vgl. Gandhi et al. 2011).

Cyberangriffe können auch Teil von physischen Militäroperationen sein. Solche Angriffe schließen das Schädigen von militärischen Informationssystemen eines Gegners ein. Dies umfasst auch Informationssysteme in Waffen, ist aber nicht auf diese beschränkt. Ein Beispiel dafür, dass solche Operationen bereits durchgeführt wurden, ist das gemeinsame Programm der USA und Israels, Stuxnet, das verwendet wurde, um iranische Urananreicherungsanlagen zu sabotieren (vgl. Nakashima und Warrick 2012; Sanger 2014). Natürlich sind Urananreicherungsanlagen nicht die einzigen Anlagen, die in einem Krieg von strategischer Relevanz sind. Jede Form von kritischer Infrastruktur (beispielsweise die Wasser-, Strom- oder Gasversorgung) stellt ein potenzielles Ziel von Cyberangriffen dar. Es ist sehr wahrscheinlich, dass solche Angriffe nicht in einem Cyberkrieg stattfinden würden, der auf den Cyberspace begrenzt bleibt, sondern in Form kombinierter Operationen im Rahmen eines Krieges, der sowohl im physischen Raum als auch im Cyberspace

ausgefochten wird. Aufgrund der Abhängigkeiten von derartigen Infrastrukturen bergen Cyberattacken jedoch auch das Risiko unkalkulierbarer oder unbeabsichtigter Neben- und Ketteneffekte. Dieser Effekt wird durch „Monokulturen" wie beispielsweise bei der Verwendung von Netzwerk-Hardware oder dem großflächigen Einsatz gleicher Betriebssysteme in Organisationen zusätzlich verstärkt. Eine unbeabsichtigte Fremd- oder Eigengefährdung ergibt sich auch aus dem sogenannten *Stockpiling* von Sicherheitslücken. Diese Informationen über Schwächen in populären IT-Produkten bilden die Basis für Cyberwaffen: Sie werden zurückgehalten, um Schutzmaßnahmen in fremden Systemen zu umgehen. Im Falle von Stuxnet führte das durch *Stockpiling* erlangte Wissen um Schwachstellen zur Erstellung der Schadsoftware, die für die Zentrifugen-Steuerungssysteme der iranischen Urananreicherungsanlage in Natanz maßgeschneidert wurde. Jedoch proliferierte die Schadsoftware unbeabsichtigt rund um den Globus, besonders in Asien, und infizierte massenhaft Windows-Betriebssysteme. Dabei entfielen ca. 1,5 Prozent der infizierten Computer auf die USA, wo die Schadsoftware mutmaßlich erstellt wurde (vgl. Shearer 2017).

EternalBlue (vgl. Reinhold 2018b) ist ein analoger Fall: Die NSA entdeckte eine Sicherheitslücke in Windows, informierte den Hersteller Microsoft darüber allerdings nicht, sondern entwickelte ein Tool namens EternalBlue, um die Schwachstelle ausnutzen zu können. Dann wurde das Tool jedoch selbst gehackt und öffentlich zur Verfügung gestellt. Die Vorfälle verdeutlichen, dass unter Umständen auch eigene IT-Systeme ungeschützt bleiben, wenn Hersteller aufgrund von Unkenntnis der Sicherheitslücken keine Anpassungen vornehmen.

3.2 Cyberspionage, -sabotage und -subversion

Informationstechnologien bieten eine Bandbreite an Möglichkeiten für militärische und nicht-militärische Überwachung. Spionage ist ein Versuch, das System eines Gegners zu penetrieren, um sensitive oder geschützte Informationen zu gewinnen. Ein solcher Datendiebstahl kann sozial oder technisch sein (vgl. Rid 2012) und einen ökonomischen oder staatlichen Hintergrund haben (vgl. Neuneck 2017). Spionage war immer relevant in Konflikten und Wettbewerben, entwickelt sich aber zu einem zunehmend akuten Thema in der IT, da Geheimdienste für ihre nachrichtlichen Aufgaben wie die Lagebildaufklärung in fremde IT-Systeme eindringen müssen und sie damit gefährden.

Unter Cyberspionage lassen sich Cyberangriffe durch ausländische Sicherheitsdienste fassen, die gegen die Vertraulichkeit von IT-Systemen gerichtet sind (vgl. Schmitt 2013, S. 14f.). Der Begriff kann

> „als jeder Akt verstanden werden, der heimlich oder unter falschen Vorwänden Cyberkapazität nutzt, um (den Versuch zu unternehmen) Informationen zu sammeln mit der Intention, diese einer nicht befugten Partei zukommen zu lassen. Der Akt muss im Territorium einer der Konfliktparteien stattfinden. ‚Heimlich' bezieht sich auf Aktivitäten, die verdeckt oder geheim unternommen werden, wie bei einer Cyberspionageoperation, die entwickelt wurde, um die Identität der involvierten Personen oder die Tatsache, dass sie stattgefunden hat, zu verbergen" (Schmitt 2013, S. 193, Übersetzung d. Verf.).

Empirisch betrachtet fällt die Mehrheit aller politischen Cybersicherheitsvorfälle in die Kategorie Spionage (vgl. Herrmann 2019). Andere offensive Kategorien sind Sabotage und Subversion. Sabotage ist

> „der vorsätzliche Versuch, ein ökonomisches oder militärisches System zu schwächen beziehungsweise zu zerstören. Sabotage ist überwiegend technischer Natur, aber natürlich werden auch soziale Einflussmöglichkeiten genutzt. […] Die in Sabotage genutzten Mittel müssen nicht immer, können aber zur physischen Zerstörung oder offenen Gewaltausübung führen. Wenn Gewalt genutzt wird, stellen Dinge, nicht Menschen, die primären Ziele dar, auch wenn das endgültige Ziel sein kann, die Kosten-Nutzen-Rechnung von Entscheidungsträgern zu verändern. Sabotage ist meist taktischer Natur und hat selten operative oder strategische Effekte. Je höher die technische Entwicklung und die Abhängigkeit einer Gesellschaft, ihrer Regierung und ihres Militärs von ihr ist, desto höher ist das Potenzial für Sabotage, insbesondere für cyberunterstützte Sabotage" (Rid 2012, Übersetzung d. Verf.).

Cyberspionageoperationen benötigen ein hohes technisches Niveau; komplexe Sabotageoperationen sind noch anspruchsvoller. Sie werden von professionellen Agenten, die von Regierungen oder großen Unternehmen kostenintensiv trainiert wurden, sowie Hackern und Individuen durchgeführt (vgl. Rid 2012). Dem stehen jedoch erheblich höhere Kosten konventioneller Rüstungsprojekte gegenüber. Dieser Umstand lässt eine Cyberoperation, die gezielt unterhalb bewaffneter Konflikte durchgeführt werden kann und keinen Einsatz menschlicher Kräfte mit *boots on the ground* erfordert, in militärischen Planungen als praktikable Alternative erscheinen.

Da IT mit Daten sowie der Qualität von und dem Vertrauen in Informationen arbeitet, stellt Subversion das dritte Ziel dar, das durch das Eindringen in und Manipulieren oder sogar Ausnutzen von Informationssystemen erreicht werden kann (ausführlicher hierzu Kaufhold und Reuter 2019). Unter Subvention verstehen wir

> „den vorsätzlichen Versuch, die Autorität, Integrität und Verfassung einer etablierten Institution oder Ordnung zu untergraben. […] Der Modus Operandi von subversiven Aktivitäten ist das Aushöhlen

> sozialer Bindungen sowie des Glauben und Vertrauens in den Staat und anderer kollektiver Entitäten. Die von Subversion genutzten Mittel schließen nicht immer Gewalt ein. Ein weit verbreitetes Mittel von Subversion ist Propaganda, beispielsweise Pamphlete, Literatur und Film. Das Vehikel von Subversion ist immer, die Loyalität von Individuen und unberührten Beobachtern zu beeinflussen. Menschliche Köpfe sind das Ziel, nicht Maschinen" (Rid 2012, Übersetzung d. Verf.).

Deutlich hervorzuheben ist, dass jeglicher nicht-autorisierter Zugriff oder Zugriffsversuch auf IT-Systeme eine Beeinträchtigung der Schutzziele von IT-Sicherheit, der Vertraulichkeit, Verfügbarkeit und Integrität, darstellt. Dies bedeutet, dass bereits die Überwindung von Sicherheitsmaßnahmen für Spionagezwecke ohne Schadensabsicht den zuverlässigen Betrieb von IT-Systemen gefährden und unkalkulierte Effekte auslösen kann.

Wie Herrmann (2019) ausführt ist es aus rechtlicher Sicht wichtig, Cyberspionage von destruktiven Formen zu unterscheiden. Destruktive Handlungen, die als Cyberangriffe oder Cybersabotage bezeichnet werden, werden typischerweise als Bedrohung oder Anwendung von Gewalt angesehen. Weissbrodt (2013) schlägt einen einfach durchzuführenden Test vor: Wenn eine Operation nur Informationen sammelt, dann ist es Cyberspionage. Wenn sie darüber hinaus agiert, stellt es mehr als Spionage dar und kann als bewaffneter Konflikt bewertet werden.

3.3 Netzwerkzentrierte Kriegsführung

In den 1980er und 1990er Jahren kam, basierend auf den Dynamiken des Ost-West-Konflikts, eine Diskussion über eine Revolution militärischer Angelegenheiten (*Revolution in Military Affairs*) auf. Die USA reagierten auf die größere Armee der Sowjetunion, indem

sie ihre Militärtechnologie verbesserten und dadurch ihre Truppen stärkten (vgl. Franke 2017). Aufbauend auf dieser Tradition etablierten die USA das strategische Konzept der netzwerkzentrierten Kriegsführung (*Network Centric Warfare*, NCW). Das bedeutet die Nutzung von IT zur Modernisierung der Kriegsführung und militärischen Infrastruktur. NCW ist ein operatives Konzept, das auf Informationsüberlegenheit basiert. Sie führt aufgrund der neuen Qualität der Informationsvernetzung von Überwachungs- und Lagebildsystemen, Führungsebenen und Waffen auf dem Schlachtfeld zu einer Erhöhung der Kampfstärke. Das Ziel der Informationsüberlegenheit ist die Dominanz der US-Streitkräfte in allen Bereichen der Kriegsführung, friedenserhaltenden Maßnahmen und Konfliktprävention. Das Konzept wurde bereits in den 1990er Jahren formuliert und setzt auf die Beherrschung des Weltalls als zentrale Komponente des uneingeschränkten Informationsaustausches (vgl. United States Space Command 1997). Die Vorteile einer uneingeschränkten Verfügbarkeit von militärischen Informationen liegt auf der Hand: Ein besserer Überblick und eine höhere Geschwindigkeit der Kommandoprozesse erhöht das organisatorische Tempo und verbessert die Angriffs- und Verteidigungsstärke, sowie die Koordination von Streitkräften (vgl. Lange 2004). NCW hat die Kriegsführung stark verändert und ist der Weg, über den die USA ihre Vormachtstellung zu halten suchen.

3.4 Attribution und Verifikation

Der Vorfall im deutschen Regierungsnetzwerk zeigt, dass die Attribution (Zuordnung) von Verantwortung für solche Vorkommnisse eine große Herausforderung darstellt. Angreifer sind aufgrund der Virtualität dazu in der Lage, ihre Spuren effektiv zu verwischen oder über unzählige zwischengeschaltete Systeme zu agieren. Eine

Rückverfolgung der Spuren ist daher in den meisten Fällen sehr zeitaufwändig und erfordert die Analyse aller verwendeten Systeme. In ähnlicher Weise konnten bei einem Cyberangriff, der 2008 während des Konflikts zwischen Russland und Georgien stattfand, keine spezifischen Angaben über die Angreifer gemacht werden, obwohl später ein *Botnet Provider* gefunden wurde, der teilweise für die Angriffe verantwortlich war (vgl. Gandhi et al. 2011).

Ein Grund für den Mangel an Rechenschaftspflicht bei Cyberangriffen ist die Schwierigkeit, eine Täterin oder einen Täter mit hoher Tatwahrscheinlichkeit öffentlich überzeugend zu identifizieren. Cyberattacken werden in aller Regel über fremdgesteuerte IT-Systeme Dritter durchgeführt. Über vielschichtige Pfade und zwischengeschaltete Systeme sind sie verborgen oder ihr Ursprung bleibt durch andere Maßnahmen verschleiert. Eine glaubwürdige Cyberattribution

> „benötigt spezifische Beweise, die an bestimmte Vorfälle gebunden sind, deren Stärke überprüft, bewertet und durch unabhängige Experten bestätigt werden kann" (Davis et al. 2017, Übersetzung d. Verf.)

Der Prozess ist sehr komplex, vielschichtig und zeitaufwändig, weshalb er spezialisierte und robuste Kapazitäten sowie in vielen Fällen internationale Kooperation erfordert. Aber selbst unter solchen optimalen Umständen sind die Ergebnisse häufig nicht glaubhaft. Zusätzlich zu einer komplexen Analyse von technischen Daten ist ein Verständnis von potenziellen politischen und ökonomischen Motivationen des Angriffs notwendig sowie – wenn möglich – eine Analyse der relevanten *Open Source Intelligence* (vgl. Davis et al. 2017), also der Auswertung öffentlich verfügbarer Datenquellen.

Es gibt eine zunehmende Zahl von Regierungsorganisationen, Unternehmen und Forschungsorganisationen, die in der Lage sind, Cyberangriffe zuzuordnen. Aber diese Akteure nutzen

keine standardisierte Methodologie und unterliegen nationalen Interessen. Dies verringert die Glaubwürdigkeit und öffentliche Überzeugungskraft der Attribution. Um einen transparenten Prozess der Attribution und vertrauensbildende Mechanismen zu etablieren, haben globale Softwareunternehmen wie Microsoft Forschungsprojekte finanziert, die sich für die Einführung einer unabhängigen Institution im Rahmen der Vereinten Nationen für Attribution einsetzen und internationale Normen in Form von „digitalen Genfer Konventionen" fordern (vgl. Davis et al. 2017; Saalbach 2019).

Ein solches Abkommen könnte zu einer Regulation der internationalen Beziehungen bezüglich der Cybersicherheit beziehungsweise der Kontrolle militärischer Cyberkapazitäten führen. Ein Prozess zur Verifikation als möglicher Teil eines solchen Vertrages könnte beispielsweise Inspektionen ermöglichen, die für alle Parteien sicherstellen, dass die Vertragsbedingungen sowie vereinbarte Restriktionen und Begrenzungen technischer Kapazitäten eingehalten werden. Eine solche Verifikation würde einen dreistufigen Prozess umfassen, der sich aus einem Monitoring von Aktionen, die für die Erfüllung von Vertragsverpflichtungen von Relevanz sind, der Analyse von Beweismaterial, das auf eine Nichteinhaltung hinweisen könnte, sowie der Feststellung, ob ein Fall von Nichteinhaltung vorliegt, zusammensetzen könnte (vgl. Caughley 2016). Verifikation ist einerseits für die Durchsetzung internationaler Verträge notwendig, andererseits aber auch Teil eines vertrauensbildenden Prozesses zwischen feindlichen Staaten (vgl. Reinhold und Reuter 2019), um unkontrollierte Rüstungswettläufe zu verhindern.

3.5 Cyberabwehr

Das Tallinn Manual definiert aktive Cyberabwehr als eine

> „proaktive Maßnahme zur Feststellung oder Erlangung von Informationen über eine Cyberintrusion [ein Eindringen in den Cyberraum, Anm. d. Verf.], einen Cyberangriff oder eine bevorstehende Cyberoperation beziehungsweise zur Ermittlung der Herkunft einer Operation, die das Beginnen einer präemptiven, präventiven oder Gegenoperation beinhaltet, die gegen die Quelle gerichtet ist" (Schmitt 2013, S. 257, Übersetzung d. Verf.).

Vorbereitungen für einen präemptiven Angriff oder die Drohung, einen durchzuführen, wird auch als Cyberabschreckung verstanden. Das Konzept des präemptiven Angriffs ist jedoch ein recht neues und darüber hinaus hoch umstritten. Denn in Abgrenzung zum im internationalen Recht etablierten Begriff des präventiven Krieges zum Zweck der Selbstverteidigung im Falle eines unmittelbar bevorstehenden Angriffs weitet das Konzept des präemptiven Krieges diese Unmittelbarkeit aus und lässt ihre Grenzen verschwimmen. So soll auch diffuseren Bedrohungen wie dem Terrorismus völkerrechtlich legitimiert mit militärischen Mitteln entgegengetreten werden können. Eine Vielzahl von Völkerrechtlerinnen und Völkerrechtlern hält diese Auslegung jedoch für rechtswidrig und weist das Konzept, dessen Erfinder vornehmlich im Justizministerium der Bush-Administration beheimatet waren, zurück (vgl. Wissenschaftliche Dienste des Deutschen Bundestages 2007). Darüber hinaus ist auch eine passive Cyberabwehr möglich. Sie beinhaltet

> „Maßnahmen zur Feststellung und Minimierung einer Cyberintrusion und der Folgen eines Cyberangriffs, die nicht das Beginnen einer präemptiven, präventiven oder Gegenoperation beinhaltet, die gegen die Quelle gerichtet ist. Beispiele für passive Cyberabwehr sind *Firewalls*, *Patches*, Anti-Virus-Software und digitale

forensische Tools“ (Schmitt 2013, S. 261, Übersetzung d. Verf.; vgl. auch Herrmann 2019).

Vorbeugende technische Sicherheits- und Schutzmaßnahmen der Entkopplung kritischer Infrastrukturen, also die strikte Trennung wichtiger IT-Systeme vom Internet, bieten angesichts der Fähigkeiten staatlicher Angreifer kaum Schutz. Dies wurde im Fall von Stuxnet deutlich, bei dem es den Angreifern gelang, industrielle Kontrollsysteme, die nicht ans Internet angeschlossen waren, zu infizieren. Darüber hinaus sind solche Sicherheitskonzepte ebenso wie der Aufbau manuell steuerbarer Notfallsysteme oder die gezielte Trennung von Daten und Software-Steuerungslogik kaum mit den aktuellen Tendenzen der Dezentralisierung, Automatisierung und Optimierung mit Hilfe von IT-Systemen in Einklang zu bringen. Eine Grundvoraussetzung dieser Prozesse ist der massive Einsatz von IT für die Informationsgewinnung, deren Auswertung und die Steuerung von Geräten sowie die umfassende Vernetzung dieser Systeme. All diese Systeme müssten durch entsprechende Schutzmaßnahmen gesichert werden, sorgen in aller Regel aber eher dafür, dass Angreifer über die Vernetzung on peripheren Systemen auch Zugriff auf zentrale Systeme wie Datenbanken oder Steuerungsalgorithmen erhalten.

4 Fazit

Die bestehende Forschung zeigt, dass die Informationstechnologie einen wesentlichen Einfluss auf die Kriegsführung und Militärstrategien hat. Einerseits setzen militärische Kräfte zunehmend auf den Cyberspace, schaffen Kapazitäten für das offensive Wirken in dieser Domäne und stellen sie sogar, wie im Falle der USA, ins Zentrum der zukünftigen Kriegsführung. Andererseits fehlen

jedoch geeignete Antworten für die internationale Regulierung von Cyberkonflikten und die aktuelle Aufrüstungsdynamik. Dieser Umstand ist auch der permanenten Ambiguität geschuldet, die den Cyberspace, seine Akteure und die in ihm ausgeführten Operationen verhüllt: Es gibt weder Trennlinien zwischen innerer und äußerer Sicherheit noch lässt sich klar bestimmen, welche Cyberressourcen defensiven oder offensiven Zwecken zugeordnet werden können.

Weiterhin existieren zahlreiche technische Möglichkeiten, von denen in diesem Beitrag einige exemplarisch genannt wurden. Auch wenn es bislang keinen Cyberkrieg gegeben hat und das Konzept strittig bleibt, steigt die Zahl der Cyberangriffe. Hervorzuheben sind hier die Datenmanipulation sowie das Blockieren oder Beschädigen gegnerischer Systeme mit DDoS-Angriffen und maßgeschneiderter Schadsoftware, die gezielt Sicherheitslücken ausnutzt. Die Wichtigkeit des Cyberspace lassen auch Cyberspionage, -sabotage und -subversion an Bedeutung gewinnen. Spionage in gegnerischen Systemen ist zum integralen Bestandteil von Geheimdienstarbeit geworden und stellt die Mehrzahl der sicherheitsrelevanten Vorfälle im Cyberspace dar.

Die digitale Revolution setzt sich auch mit der netzwerkzentrierten Kriegsführung fort, die ansetzt, die das Potenzial hat, die Kriegsführung dauerhaft zu transformieren. Attribution und Verifikation sind weiterhin mit Problemen behaftet, obwohl sie zur Durchsetzung internationalen Rechts unabdingbar sind. Schließlich steht die Cyberabwehr vor rechtlichen Dilemmata, nicht zuletzt aufgrund fehlender Normen bezüglich Präemption, Prävention und Gegenoperationen. Die Besonderheiten im Cyberspace im Kontext von Frieden und Sicherheit machen eine gesonderte Betrachtung notwendig, um der Komplexität und Ambiguität des Feldes gerecht zu werden.

Literatur

Altmann, Jürgen. 2019. Natural-Science/Technical Peace Research. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 39–60. Wiesbaden: Springer Vieweg.

Altmann, Jürgen, Martin Kalinowski, Ulrike Kronfeld-Goharani, Wolfgang Liebert und Götz Neuneck. 2010. Naturwissenschaft, Krieg und Frieden. In *Friedens- und Konfliktforschung*, hrsg. von Peter Schlotter und Simone Wisotzki, 410–445. Baden-Baden: Nomos.

Backhaus, Michael und Sebastian Wanninger. 2018. *Auf dem digitalen Gefechtsfeld – Locked Shields*. Berlin: BMVg.

Bernhardt, Ute und Ingo Ruhmann. 2017. Informatik. In *Naturwissenschaft – Rüstung – Frieden*, hrsg. von Jürgen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann und Dieter Wöhrle, 337–448. Wiesbaden: Springer VS.

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2013. IT-Grundschutz: Glossar und Begriffsdefinitionen. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. Zugegriffen: 24. Juni 2019.

Bundesamt für Sicherheit und Informationstechnik (BSI). 2016. Die Lage der IT-Sicherheit in Deutschland 2016. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5. Zugegriffen: 24. Juni 2019.

Bundesamt für Sicherheit und Informationstechnik (BSI). 2017. Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html. Zugegriffen: 24. Juni 2019.

Bundesministerium der Verteidigung (BMVg). 2016. *Abschlussbericht Aufbaustab Cyber- und Informationsraum*. Berlin: BMVg.

Bundesministerium des Inneren (BMI). 2011. *Cyber-Sicherheitsstrategie für Deutschland*. Berlin: BMI.

Caughley, Tim. 2016. Nuclear Disarmament Verification: Survey of Verification Mechanisms. http://www.unidir.org/files/publications/pdfs/survey-of-verification-mechanisms-en-657.pdf. Zugegriffen: 24. Juni 2019.

Chivvis, Christopher S. und Cynthia Dion-Schwarz. 2017. Why It's So Hard to Stop a Cyberattack - and Even Harder to Fight Back. https://

www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html. Zugegriffen: 24. Juni 2019.

Davis II, John S., Benjamin Boudreaux, Jonathan William Welburn, Cordaye Ogletree, Geoffrey McGovern und Michael S. Chase. 2017. Stateless Attribution: Toward International Accountability in Cyberspace. https://www.rand.org/pubs/research_reports/RR2081.html. Zugegriffen: 24. Juni 2019.

Denker, Kai, Marcel Schäfer und Martin Steinebach. 2019. Darknets as Tools for Cyber Warfare. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 107–135. Wiesbaden: Springer Vieweg.

Franke, Ulrike Esther. 2017. Die Revolution in Militärischen Angelegenheiten. In *Friedens- und Konfliktforschung*, hrsg. von Tobias Ide, 69–92. Opladen: Verlag Barabara Budrich.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu und Phillip Laplante. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine*, 30 (1): 28–38.

Hansen, Lene und Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53 (4): 1155–1175.

Herrmann, Dominik. 2019. Cyber Espionage and Cyber Defence. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 83–106. Wiesbaden: Springer Vieweg.

Hollick, Matthias und Stefan Katzenbeisser. 2019. Resilient Critical Infrastructures. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 305–318. Wiesbaden: Springer Vieweg.

ISO 27001. 2015. Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014). https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/wannacry-eternalblue/. Zugegriffen: 24. Juni 2019.

Kaufhold, Marc-André und Christian Reuter. 2019. Cultural Violence and Peace in Social Media. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises,*

War, and Peace, hrsg. von Christian Reuter, 361–381. Wiesbaden: Springer Vieweg.
Lange, Sascha. 2004. Netzwerk-basierte Operationsführung: Streitkräfte-Transformation im Informationszeitalter. https://www.ssoar.info/ssoar/handle/document/24349. Zugegriffen: 24. Juni 2019.
Mansfield-Devine, Steve. 2009. Darknets. *Computer Fraud & Security* 2009 (12): 4–6.
Mascolo, Georg, Ronen Steinke und Hakan Tanriverdi. 2018. Die Geschichte eines Cyber-Angriffs. *Süddeutsche Zeitung* vom 30. April 2018.
Nakashima, Ellen und Joby Warrick. 2012. Stuxnet Was Work of U.S. and Israeli Experts, Officials Say. *Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?noredirect=on&utm_term=.18554a394933. Zugegriffen: 24. Juni 2019.
NATO. 2016. *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Zugegriffen: 24. Juni 2019.
Neuneck, Götz. 2017. Krieg Im Internet? Cyberwar in Ethischer Reflexion. In *Handbuch Friedensethik*, hrsg. von Ines-Jacqueline Werkner und Klaus Ebeling, 805–816. Wiesbaden: Springer VS.
Reinhold, Thomas. 2018a. Hack der deutschen Regierungsnetze. Datenbank relevante Cybervorfälle. 2018. https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/hack-der-deutschen-regierungsnetze/. Zugegriffen: 24. Juni 2019.
Reinhold, Thomas. 2018b. WannaCry / EternalBlue. https://cyber-peace.org. Zugegriffen: 24. Juni 2019.
Reinhold, Thomas und Christian Reuter. 2019. Verification in Cyberspace. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 257–275. Wiesbaden: Springer Vieweg.
Reuter, Christian (Hrsg.). 2019. *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Vieweg.
Reuter, Christian, Larissa Aldehoff, Thea Riebe und Marc-André Kaufhold. 2019. IT in Peace, Conflict and Security Research. In *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 11–37. Wiesbaden: Springer Vieweg.

Rid, Thomas. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies* 35 (1): 5–32.

Riebe, Thea und Christian Reuter. 2019. Dual-Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 165–183. Wiesbaden: Springer Vieweg.

Ruhmann, Ingo und Ute Bernhardt. 2019. Information Warfare - From Doctrine to Permanent Conflict. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 63–82. Wiesbaden: Springer Vieweg.

Saalbach, Klaus-Peter. 2019. Attribution of Cyber Attacks. In *Information Technology for Peace and Security - IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*, hrsg. von Christian Reuter, 279–304. Wiesbaden: Springer Vieweg.

Sanger, David E. 2014. Syria War Stirs New U.S. Debate on Cyberattacks. https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html. Zugegriffen: 24. Juni 2019.

Schmitt, Michael. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Shearer, Jarrad. 2017. W32.Stuxnet. https://symantec.com. Zugegriffen: 24. Juni 2019.

Solms, Rossouw von und Johan van Niekerk. 2013. From Information Security to Cyber Security. *Computers and Security* 38: 97–102.

United States Space Command. 1997. Network Centric Warfare: Background and Oversight Issues for Congress. https://apps.dtic.mil/dtic/tr/fulltext/u2/a476256.pdf. Zugegriffen: 24. Juni 2019.

Weissbrodt, David. 2013. Cyber-Conflict, Cyber-Crime, and Cyber-Espionage. *Minnesota Journal of International Law* 22.

Wissenschaftliche Dienste des Deutschen Bundestages. 2007. Zum Konzept der präemptiven Selbstverteidigung. Berlin: Deutscher Bundestag.