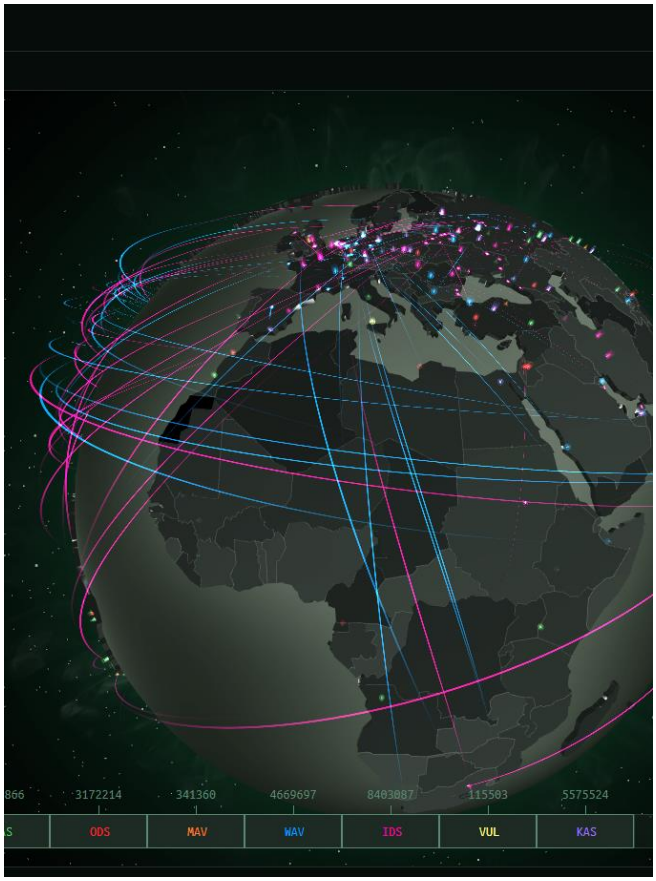
EAK
EVANGELISCHE ARBEITSGEMEINSCHAFT
FÜR KRIEGSDIENSTVERWEIGERUNG
UND FRIEDEN

PROTESTANT ASSOCIATION
FOR CONSCIENTIOUS OBJECTION AND PEACE



Cyberbedrohungen weltweit: Momentaufnahme
https://cybermap.kaspersky.com/de

CYBERWAR VERSTEHEN- CYBERPEACE MITGESTALTEN

Materialsammlung mit Unterrichtsentwurf und Elementen in Leichter Sprache

Maike Rolf

Zur Autorin:

Maike Rolf ist Friedens- und Konfliktforscherin und Mediatorin und arbeitet als Friedensreferentin in der Bundesgeschäftsstelle der Evangelischen Arbeitsgemeinschaft für KDV und Frieden.

Impressum:

Herausgeberin

EAK
EVANGELISCHE ARBEITSGEMEINSCHAFT
FÜR KRIEGSDIENSTVERWEIGERUNG
UND FRIEDEN

PROTESTANT ASSOCIATION
FOR CONSCIENTIOUS OBJECTION AND PEACE

Evangelische Arbeitsgemeinschaft für KDV und Frieden (EAK), Endenicher Str. 41, 53115 Bonn

office@eak-online.de; www.eak-online.de

Autorin: Maike Rolf

Beratung: Detlev Besier (Pfarrer für Frieden und Umwelt der Evangelischen Kirche in der Pfalz), Julika Koch (Referat Friedensbildung der Evangelisch-Lutherischen Kirche in Norddeutschland)

Bonn, 2021.

Einige Tage vor Veröffentlichung dieser Publikation ist im April 2021 die EKD-Denkschrift „Freiheit digital – Die Zehn Gebote in Zeiten des digitalen Wandels“ erschienen. Autorin ist die Kammer der EKD für soziale Ordnung.

Die Denkschrift ist deswegen leider nicht in dieser Publikation berücksichtigt.

Das Kapitel 2.6 der Denkschrift mit dem Titel „Digitalisierte Gewalt unterbrechen“ bezieht sich ausdrücklich auf das Thema Cyberwar.

Link zum pdf: https://www.ekd.de/ekd_de/ds_doc/denkschrift_freiheit_digital_EVA_2021.pdf

Link zum Internetformat der Denkschrift:

https://www.ekd-digital.de/

Inhalt

Vorwort des Friedensbeauftragten des Rates der EKD

Renke Brahms,

Friedensbeauftragter des Rates der EKD sowie theologischer Direktor und Geschäftsführer der Evangelischen Wittenbergstiftung

An digitale Vernetzung im Alltag haben wir uns längst gewöhnt. Sie bietet eine Reihe von Vorteilen und macht uns gleichzeitig auch angreifbar. Darauf muss Politik antworten und ihrer Schutzfunktion nachkommen. Allerdings darf dabei nicht eine militärische Sicherheitslogik zum Paradigma werden, sondern eine entsprechende Verteidigung im Cyberraum muss menschliche Sicherheit im Sinne eines Zivilschutzes in den Fokus rücken.

Die Kundgebung der Synode der Evangelischen Kirche in Deutschland (EKD) „Kirche auf dem Weg der Gerechtigkeit und des Friedens“ aus dem November 2019 ist von einem zentralen Leitgedanken geprägt: Ausgerichtet am Leitbild des gerechten Friedens wird angesichts neuer und sich verschärfender Konflikte am unbedingten Vorrang des Zivilen und dem Weg der Gewaltfreiheit festgehalten. Ziel ist es, militärische Gewalt und kriegerische Mittel Schritt für Schritt zu überwinden und den eindeutigen Schwerpunkt auf die Prävention zu legen.

Vor diesem Hintergrund kommt die Synode der EKD im Hinblick auf Fragen des Cyberraums folgerichtig zu dem Beschluss:

- „Wir sprechen uns dafür aus, bei der Cyber-Abwehr vor allem zivile Strukturen und defensive Maßnahmen zu stärken.
- Wir sehen die Notwendigkeit, zur Vermeidung bzw. Regelung von Konflikten im Cyberraum auf der Grundlage ethischer Kriterien ein völkerrechtlich verbindliches Cyberrecht zu entwickeln und einzuführen. Die Bundesregierung sollte sich im Rahmen der UN dafür einsetzen.“ (Evangelische Kirche in Deutschland, 2019)

In den Auseinandersetzungen mit dem Themenkomplex „Cyberwar“ wurde auch auf der EKD-Synode deutlich, dass innerhalb der Kirche noch vergleichsweise wenig fachliche Expertise und inhaltliche Profilierung vorhanden ist. Dabei werden in diesen Themen sowohl grundlegende friedensethische als auch Fragen der Friedensbildung berührt.

Umso bedeutsamer in diesem Zusammenhang ist die Arbeit der Evangelischen Arbeitsgemeinschaft für Kriegsdienstverweigerung und Frieden (EAK), welche dieses Dossier „*Cyberwar verstehen- Cyberpeace mitgestalten*“ vorgelegt hat. In Anlehnung an eine Begriffsprägung durch den Verein „Forum InformatikerInnen für Frieden und zivilgesellschaftliche Verantwortung“ wird als Gegenentwurf zum Cyberwar der Begriff des Cyberpeace genutzt und inhaltlich gefüllt.

Das Dossier will Wissen vermitteln, Bewusstsein schaffen und zum Nachdenken über ethische Problematiken und Gewissensfragen anregen. Es zeigt eindrücklich wie sich die Bearbeitung von friedensethischen Herausforderungen mit friedenspädagogischen Anregungen verbinden lassen. Dies geschieht in Form eines konkreten Unterrichtsentwurfs für die Arbeit mit Schüler*innen, Konfirmand*innen oder Studierenden. Das Dossier wird des Weiteren bereichert durch Textbausteine in Leichter Sprache, die flexibel in Unterrichtsformate integriert werden können.

Mit dem Dossier ist die Hoffnung einer vertieften Auseinandersetzung mit der Thematik innerhalb der Kirche verbunden. Die Autorin Maike Rolf (Friedensreferentin der EAK in Bonn) liefert mit dieser Publikation einen wichtigen Anstoß.

Einleitung

Die USA und Israel manipulierten mithilfe von Großbritannien durch die Schadsoftware Stuxnet die iranische Atomanlage in Natanz 2009 und 2010 (vgl. Roodsari, 2020). Mehr als 1000 Zentrifugen wurden unbrauchbar gemacht (vgl. Sanger, 2012, zitiert nach Schörnig in Werkner et al., 2019; S. 54). Das iranische Atomwaffenprogramm wurde auf diesem Weg sabotiert und verlangsamt. Stuxnet wurde als „erste digitale, zielgerichtete Cyberwaffe“ (Neuneck, 2017; S.809, zitiert nach Werkner in Werkner et al, 2019; S.8) anerkannt. Der Iran reagierte mit einer Drohgebärde, indem er die Geldautomaten der drei großen amerikanischen Banken USA-weit abschaltete. (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. 2018; 17:36). Der Angriff war Auslöser für die verstärkte Entwicklung der iranischen Cyberkapazitäten. Mittlerweile gibt es mehrere "Advanced Persistent Threats" (APT) – Hackergruppen, hinter denen teilweise angesichts durchdachter Strategien und Ressourcen die Verbindung mit dem Iran vermutet wird. Neben diesen Gruppen gibt es auch Cyberkriminelle, die entlang der Interessen ihrer Regierung patriotisch handeln wollen oder finanziell motiviert sind. Heute ist der Iran mit einem gut entwickelten digitalen Waffenarsenal und professionellen Hackern ausgestattet (vgl. Roodsari, 2020): So folgte beispielsweise im Jahr 2012 ein Cyberangriff auf das Energieunternehmen Saudi- Arabiens, Saudi- Aramco; die komplette IT- Infrastruktur, sprich zehntausend Computer, wurden durch den Angriff funktionslos gemacht. Des Weiteren verschaffte der Iran sich durch Cyberangriffe einen Zugang zu wissenschaftlichen Erkenntnissen aus den USA, zu Themen wie Atomwaffen. Nach der Tötung eines iranischen Generals durch einen US-Drohnenangriff, kündigte der Iran einen schweren Gegenangriff an (vgl. Roodsari, 2020).

Es muss jedoch differenziert werden, denn es gibt auch diverse Angriffe, die zwar nicht als Krieg eingestuft werden, aber dennoch zahlreiche Gefahren für persönliche und politische Sicherheit darstellen. Dabei kann es sich beispielsweise um Wahlbeeinflussung, Spionage, Sabotage, möglicherweise in Kombination mit Erpressung aus politischen oder wirtschaftlichen Motiven handeln. Häufig ermöglichen Sicherheitslücken in Software solche Angriffe. Durchgeführt werden sie von Geheimdiensten, Armeen oder unabhängigen oder assoziierten Hacker*innen oder -gruppen. Ziel können Daten, Objekte und Menschen sein.

Das Dossier **Cyberwar verstehen, Cyberpeace mitgestalten** will Wissen vermitteln, Bewusstsein schaffen und zum Nachdenken anregen über ethische Problematiken und Gewissensfragen; sowie Impulse für Handlungsoptionen geben. Daraus resultierend können friedensbewegte Menschen sich dem Thema nähern, um in der Folge sprachfähig zu werden und den Cyberpeace

mitzugestalten. Das Thema besitzt herausragende Bedeutung für die evangelische Friedensarbeit, denn aufgrund der Aktualität ist es wichtig, dass die Friedensarbeit sich gut damit auskennt, sprech- und handlungsfähig ist. Dieses Dossier bietet Zugang zum Thema Cyberwar und vermittelt Wissen in Fachsprache und Leichter Sprache (siehe Kapitel „pädagogische Anregungen“) für eine breite Zielgruppe- als Ergänzung zur wissenschaftlichen Literatur. Auch ist es einer der Themenschwerpunkte, die die EKD-Synode 2019 als besonders wichtig eingestuft hat. Dieses Dossier ist konzipiert für die Arbeit mit Schüler*innen, Konfirmand*innen, Studierenden und verschiedenen Generationen friedensbewegter Menschen. Inhaltlich liegt der Fokus auf verständlichen, Überblick verschaffenden Informationen, die vielen Menschen als niedrigschwelliger Einstieg dienen können. Hinweise auf weiterführende Literatur finden sich im Text sowie im Literaturverzeichnis.

Definitionen

Bei Cyberwar handelt es sich um eine kriegerische Auseinandersetzung zwischen Staaten im virtuellen Raum, die mit Mitteln der Informationstechnologie geführt wird. Ein Cyberkrieg hat zum Ziel, Ländern, Institutionen oder der Gesellschaft auf elektronischem Weg Schaden zuzufügen und wichtige Infrastrukturen zu stören (Luber, 2017). Der virtuelle Raum umfasst alle auf Datenebene vernetzten IT Informationstechnik- Systeme im globalen Maßstab. Grundlegendes Transportnetz ist das Internet, welches durch Datennetze ausgebaut werden kann (Bundesministerium der Verteidigung, 2020). Angreifer*innen haben meist einen kriminellen, extremistischen/ terroristischen, militärischen oder nachrichtendienstlichen Hintergrund (BMI, 2016; S.7).

Doch was ist Krieg, losgelöst von seinen konventionellen Ausprägungen? Vorschlag einer Definition: „Zustand, in dem die Furcht vor Tod, Armut oder einem anderen Unglück den ganzen Tag über am Herzen des Menschen [nagt], der aus Sorge über die Zukunft zu weit blickt, und er hat vor seiner Angst nur im Schlaf Ruhe.“ (Wussow, 2020; , S. 10).

Es gibt verschiedene enger und weiter ausgeführte Definitionen des Cyberwars. Immer handelt es sich um die „Zustandsbeschreibung eines Krieges mit Cybermitteln“ (vgl. Werkner in Werkner et al., 2019; S. 4). Das Tallinn Manual on the International Law Applicable to Cyber Warfare ist eine Studie über die Anwendbarkeit des Völkerrechts hinsichtlich Cyberkonflikte und Cyberkrieg (ebd.). Es bietet einen von der NATO aufgesetzten internationalen Orientierungsrahmen bezüglich Legitimität und Illegitimität digitaler Operationen (vgl. Matthiessen, 2018). Ein Cyberangriff (im Sinne eines Cyberwars) wird darin folgendermaßen definiert: „a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage

or destruction to objects" (Werkner, 2019; S.4). Bisher wurde noch kein Vorfall international offiziell als Cyberkrieg definiert (vgl. ebd.; S. 23). Sehr wahrscheinlich ist, dass kombinierte Formen von Operationen stattfinden, sowohl im physischen Raum als auch Cyberraum und somit Cyberkrieg nicht auf Cyberspace eingeschränkt ist (vgl. ebd.; S. 24f.). Für militärische Operationen gilt übrigens, dass sie heute grundsätzlich über eine Cyberdimension verfügen und die verschiedenen Dimensionen ineinandergreifen. So werden z.B. Drohnenangriffe durch die Ortung von Zielpersonen vorbereitet.

Infokasten: Abgrenzung zu autonomen und automatisierten Waffen

Militärische Operationen verfügen heute immer über eine Cyberdimension und die verschiedenen Dimensionen greifen ineinander: Waffen und Strategien im konventionellen sowie im virtuellen Raum, teilweise auch automatisiert (Ethik und Militär, 01/2019; S. 51).

An dieser Stelle wird die Abgrenzung zu automatisierten und autonomen Waffensystemen notwendig. Diese ermöglichen eine kriegerische Auseinandersetzung im konventionellen Raum mit Mitteln der Informationstechnik (sowie teilweise im virtuellen Raum). Automatisierte Waffensysteme sind u.a. (bewaffnete) Drohnen, die ferngesteuert werden, aber eigenständig starten, landen und vorgegebene Strecken abfliegen können. Der Übergang, insbesondere von hochgradig automatisierten, hin zu autonomen Waffensystemen, ist fließend. Letztere können Tätigkeiten selbst und ohne menschliche Kontrolle ausführen, im Falle von künstlicher Intelligenz kann ein System sich innerhalb des ihm von der Programmierung zugewiesenen Bereichs sogar neue, nicht programmierte „Fähigkeiten" aneignen und danach handeln (Bundeszentrale für politische Bildung, 2016; Killer Roboter stoppen!, 2015). Nach Auffassung von Human Rights Watch sowie der International Human Rights Clinic verstoßen autonome Waffensysteme gegen das Völkerrecht (Human Rights Watch; International Human Rights Clinic, 2018).

Grundvoraussetzung für Angriffe im Cyberraum sind vorhandene Sicherheitslücken in der IT-Infrastruktur. Es geschieht sehr häufig, dass sie ausgenutzt werden, häufig mit eigens dafür programmierter Schadsoftware. In Bedrohungsszenarien kann das Wissen um die Kompetenz Anderer Verhandlungen beeinflussen, so wie bisher der Faktor Truppenstärke. Das meistbesprochene Szenario ist das am wenigsten wahrscheinliche: der aktive Cyberkrieg mittels Angriffen im virtuellen Raum sowie mit konventionellen Waffen, Toten und Verletzten (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 2018; 21:08).

Jedoch wird der Begriff „Cyberwar“ auch kritisch gesehen. Es braucht sprachliche Differenzierung, um in der Debatte präzise zu sein und umfassendes Verständnis zu vermitteln, anstatt diffuse Ängste zu schüren. Zudem darf Kriegsrhetorik kein Alltagszustand sein, denn zahllose Angriffe im Cyberraum bleiben unterhalb der Schwelle zur Gewalt (Schörnig in Werkner et al., 2019; S. 39f.).

Zum Beispiel Cyber Network Attacks: „werden Daten eines Computernetzwerkes mithilfe von Malware umfunktioniert oder gelöscht, liegt eine Computer Network Attack vor, die regelmäßig netzwerkexterne Zwangswirkungen aufweist.“ (Schmahl in Rogg, 2020; S. 91). Sabotageakte verletzen das Interventionsverbot. Das Gewaltverbot wird erst verletzt, wenn es sich um Operationen handelt, die eine signifikante zerstörerische Wirkung nach sich ziehen. Vorbeugende Selbstverteidigung im Cyberraum ist in den allermeisten Fällen de facto völkerrechtswidrig. Denn wenn bevorstehende Angriffe bekannt sind, können Sie abgewehrt werden; abstrakte Bedrohungslagen gelten wiederum nicht als ausreichende Legitimation (ebd.; S. 91ff.).

Zum Beispiel Cyber Network Exploitation: zwischenstaatliche Spionage wird nach Urteilen des Internationalen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte nicht als Verletzung des völkerrechtlichen Interventionsverbots eingestuft, sofern die Daten nicht verändert werden (Schmahl in Rogg, 2020; S. 90f).

Als Gegenentwurf zum Cyberwar wird hier der Begriff des Cyberpeace genutzt: „Frieden im Cyberspace in sehr allgemeinem Sinn: Die friedliche Anwendung des Cyberspace zum Nutzen der Menschheit und der Umwelt. Dies schließt den Verzicht auf alle Aktivitäten des Cyberkriegs ein, bedeutet aber auch die Nutzung der gesamten Kommunikationsinfrastruktur für internationale Verständigung.“ (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung).

Den Zielzustand der IT- Sicherheit definiert das Bundesamt für Sicherheit in der Informationstechnik (2017) als „einen Zustand, indem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind“ (Werkner et al., 2019; S.19).

Zahlreiche Begriffsdefinitionen aus dem digitalen Sicherheitsbereich können unter den folgenden Links nachgeschlagen werden:

- https://www.hiscox.de/blog/cyber-glossar/
- https://kurzelinks.de/x86v
- https://www.digitalacademy.de/glossar/cybersecurity
- https://kurzelinks.de/lryi

Bedrohungen & Angriffe

Operationen im Cyber- und Informationsraum sind zunehmend Bestandteil kriegerischer Auseinandersetzungen. Bedrohungen im Cyber- und Informationsraum umfassen Diebstähle und Missbrauch persönlicher Daten sowie Wirtschaftsspionage. Die Schädigung kritischer Infrastrukturen kann gravierende Folgen für die Zivilbevölkerung bis hin zur Störung der Regierungskommunikation und militärischer Führungskommunikation haben (vgl. Die Bundesregierung, 2016; S. 37).

Sowohl persönliche, gesellschaftliche, wirtschaftliche und politische Schäden können durch Cyberangriffe verursacht werden. Durch die Ausspähung oder Sabotage von staatlichen Institutionen können Verwaltung, Streitkräfte und Sicherheitsbehörden beeinflusst werden und sie können Auswirkungen auf die öffentliche Sicherheit und Ordnung haben. Cyberangriffe auf Energieversorgungsnetze können weite Teile des öffentlichen und privaten Lebens außer Funktion setzen. Gezielte Angriffe und Manipulationen auf Bankeninfrastrukturen oder Börsenkurse können für den Finanz- und Wirtschaftsmarkt in Deutschland und der Welt weitreichende Folgen haben. Ebenso Manipulationen beim automatisierten und vernetzten Fahren, in der IT- gestützten Verkehrslenkung oder bei IT- Anwendungen im Gesundheitswesen können schwerwiegende Folgen für Bürger*innen haben. Die gezielte Verbreitung von Falschmeldungen kann zu Desinformation und Manipulation der öffentlichen Meinung führen und eine langfristige Gefahr für die freiheitliche Gesellschaft und Demokratie darstellen. Die Bedrohungslage durch Cyberattacken/ -kriege im Bereich des Staates, der Wirtschaft und der Gesellschaft in Deutschland wird zunehmend als gravierend eingestuft (Bundesministerium des Innern, 2016; S.7).

Cyberangriffe bestehen meist aus einer Kombination verschiedener Methoden. Das Ausnutzen von Programmierfehlern und Schwachstellen in einer Software, sogenannte Exploits, ist eine häufig angewandte Methode (vgl. Matthiessen, 2018). Im Rahmen eines lokalen Exploit wird auf dem Zielgerät eine Schadsoftware, beispielsweise ein Trojaner, installiert. Das Schadprogramm kann als Anhang an E-Mails angeheftet werden, sodass es sich nach dem Öffnen durch Zielpersonen installiert (in diesem Fall spricht man von Spear Phishing) (vgl. Siller, 2013, zitiert nach Flögel, 2014; S.5). Es gibt verschiedene Formen von Exploits, unter anderem das Nutzen einer völlig unbekannten Lücke (Zero-Day-Lücken). Hier werden ggf. Quellcodes einer Software oder eines Betriebssystems benötigt. Auch der Computerwurm gehört zur Malware, ist allerdings deutlich aggressiver hinsichtlich des Eindringens in Systeme (vgl. ebd.). Ein weiteres Tool ist die (Distrupted) Denial of Service Attacke (DDos); auch Cyberangriffe, die mit Proxies (Zombies) oder

Botnets eines Zombie-Computers ausgeführt werden sind sogenannte DDos (vgl. Werkner et al., 2019; S.24). Für diesen Angriff werden mehr als tausend Privatcomputer benutzt, um auf einem bestimmten Dienst oder einer bestimmten Website Anfragen zu senden. Dies führt zu einer Kapazitätsüberlastung der Server und zum zeitweisen Ausfall des Webdienstes. (vgl. Flögel, 2014; S.5).

Die Anfälligkeit von Software- Systemen liegt zum einen daran, dass in der Software- Entwicklung zunächst die Priorität darauf liegt, dass das System überhaupt funktioniert, denn aufgrund der Komplexität sind Fehler beim Programmieren wahrscheinlich. Zum anderen sind Softwareentwickler*innen häufig nicht ausreichend im sicheren Programmieren ausgebildet. Sicherheitsrisiken sind somit u.a. die Folge von Unwissenheit und Fahrlässigkeit der Softwareentwickler*innen. Diese „Fehler, Versäumnisse und Gedankenlosigkeit, die beim Programmieren Sicherheitslücken entstehen lassen, bilden die technische Grundlage für Cyberwaffen“ (Matthiesen, 2018). Auch Fernwartungszugänge, teils von den Herstellern erstellt, sind Schwachstellen, die bei Hackerangriffen genutzt werden können. Zugänge werden teilweise sogar bewusst für z.B. Geheimdienste offengehalten (ebd.). Durch die unsichere IT- Struktur und die (nicht) freiwillige Kooperation mit Geheimdiensten kommt es zu einem Vertrauensverlust in der IT-Sicherheit (z.B. CISCO USA). Cyberangriffe auf Industrieanlagensteuerung (Industrial Control System - ICS), sogenannte SCADA- Systeme (Supervisory Control and Data Acquisition System) oder DCS (Distributed Control Systems) sind sehr komplex und schwieriger, als das Hacken von Systemen, die ausschließlich mit COTS Produkten (Commercial Off-The-Shelf, seriengefertigte Soft- und Hardware) gesteuert werden (vgl. Flögel, 2014; S.6). Selbst bei Nicht-Verbindung mit einem Netzwerk oder einer Internet-Verbindung, d.h. wenn eine „air gap“ vorhanden ist, können SCADA-Systeme teils über Funk- und Wireless-Verbindungen erreicht werden (vgl. Flögel, 2014; S.6). Mit diesen Verbindungen lässt sich Schadsoftware (beispielsweise Stuxnet) in Industrieanlagen einschleusen (vgl. ebd.).

In den letzten Jahren wurden bereits zahlreiche Cyber Attacks und Exploitations verzeichnet, die von politischer Relevanz sind. Beispielsweise wurden im Jahr 2007 Internetseiten sowohl von estländischen Banken und Behörden als auch von Polizei und Regierung mit Denial of Service-Attacken angegriffen. Mehrere Millionen Rechner in 75 Ländern wurden in das Bot-Netz (Gruppe automatisierter Schadprogramme) mit einbezogen (vgl. Werkner et al., 2019; S.52). Der internationale Austausch, beispielsweise im Handel- oder Bankverkehr wurde lahmgelegt und sogar Notrufnummern blockiert (vgl. ebd.). 2014 richtete vermutlich Nordkorea Cyberangriffe auf Sony. 2015 war das interne Kommunikationssystem des Deutschen Bundestages und 2016 die

Energieversorgung in der Ukraine Angriffsziel von Cyberangriffen (vgl. ebd.; S.8). Weitere relevante Cybervorfälle aus den Jahren 2007 bis 2019, die vermutlich oder gesichert auf den staatlich-militärischen Einsatz von Malware zurückzuführen sind oder im Kontext der Debatte über eine Militarisierung des Cyberspace eine wichtige Rolle spielen, können abgerufen werden unter: https://cyber-peace.org/cyberpeace-cyberwar/relevante-cybervorfalle/ .

Kein bewaffneter Angriff oder gar Cyberwar, aber vielleicht eine umso größere Herausforderung für die demokratische Grundordnung sind vielfältige und zahlreiche Aktionen unterhalb der Schwelle eines bewaffneten Angriffs. Sie können große Auswirkungen haben und erfordern einen strategischen Umgang. Ein Beispiel dafür sind Social Bots, also Computerprogramme, die darauf programmiert sind, automatisierte Aufgaben durchzuführen. Menschliche Identitäten können so mit Fake-Accounts in sozialen Netzwerken erstellt werden. Für die Programmierung eines Social Bot benötigt es nur eine kostenfreie Software (Bundeszentrale für politische Bildung, 2017). Belegt ist eine Anwendung von Social Bots auf Twitter in Situationen der Ukraine-Krise, der Brexit-Kampagne sowie im zurückliegenden US-Präsidentschaftswahlkampf (vgl. Schünemann, 2019). Mithilfe von Social Bots können auf sozialen Onlineplattformen wie Facebook extreme Meinungen und Hassbotschaften verbreitet, kommentiert und häufig geliked werden. Dies kann den Eindruck bei vielen Menschen erwecken, dass diese Meinung richtig ist und zum erneuten Teilen appellieren. Manipulierte, akkumulierte Beiträge können auf diesem Weg einen großen Umfang und Einfluss erreichen (vgl. Bundeszentrale für politische Bildung, 2017), beispielsweise, was die öffentliche Meinung und demokratische Debatte angeht (vgl. Schünemann, 2019). Gleichzeitig wird daran gezweifelt, dass Menschen nur wegen Social Bots politisch beeinflussbar sind und ihre Meinung ändern. Der Chaos Computer Club ist der Meinung, dass Social Bots im Bereich der Politik und im Einfluss auf Wahlen überbewertet werden. „Bots könnten vorhandene Tendenzen lediglich verstärken – und Verstärkung sei grundlegend für das algorithmische System des Internets“ (Bundeszentrale für politische Bildung, 2017).

Im Rahmen der Digitalisierung entstehen neue Wege der (politischen) Kommunikation, und damit auch neue Herausforderungen und Risiken. Auch die Forschung ist diesbezüglich noch in den Anfängen. Bei politischen Gegenmaßnahmen muss die Vorsicht darin bestehen, dass keine negativen Folgen für die Meinungsfreiheit und Demokratie eintreten (vgl. Schünemann, 2019). Beispielsweise ist es bedenklich, „[…] Restriktionen von als politisch destabilisierend wahrgenommenen Informationen im Cyberspace zu legitimieren, da hiermit erhebliche Gefahren für die Meinungs- und Informationsfreiheit im Cyberspace verbunden sein dürften“ (Werkner et al., 2019; S. 76).

Cyberangriffe und Exploitations können auf den ersten Blick attraktiv sein. Denn aus Proportionalitätsüberlegungen heraus, ähnlich wie in der Debatte um bewaffnete Drohnen, erscheinen Angriffe als nahezu risikolos und locken mit geringen eigenen Verlusten. Zunächst bleiben Cyberangriffe auf digitale Systeme beschränkt und erzielen physische Wirkungen in der realen Welt erst als sekundäre Effekte. Dabei wird das Risiko einer Eskalationsspirale, die sich sowohl im Cyber- als auch im konventionellen Raum ausprägen kann, leider oft ausgeklammert (Werkner et al., 2019; S. 40).

Den*die Angreifer*in ausfindig zu machen, ist allerdings meist schwierig. Es gibt Zurechnungs- und Beweisprobleme, denn im Cyberraum werden kaum Spuren hinterlassen, der informatorische Gehalt bei Cyberangriffen ist manipulierbar und bei den „Werkzeugen“ handelt es sich überwiegend um „handelsübliche Alltagstechnologien“ (z.B. PCs, USB-Sticks oder Standardprogramme). Hinzu kommt, dass große Teile von Wissen und Technologie in dem Bereich der Dual-Use-Problematik unterliegen, also sowohl für Schutz und Aufklärung, als auch für Angriffe genutzt werden können (vgl. ebd.; S.7).

Die Bedrohungen und auch die realen Angriffe sind vielfältig, und auch sehr vielschichtig. Es ist wichtig, sie zu verstehen, um daraus Positionen und Strategien entwickeln zu können. Im abschließenden Kapitel wird eine Auswahl von Handlungsansätzen und Forderungen skizziert.

Handlungsansätze

Eine essenzielle rechtliche Basis konnte durch die Entscheidung, dass das Völkerrecht auch im Cyberraum gilt, gelegt werden (vgl. Vereinte Nationen, 2013 & 2015). Im Detail jedoch besteht häufig noch Unklarheit über die Auslegung der bestehenden Völkerrechtsnormen.

In Deutschland hat das Bundesministerium des Innern (BMI) 2016 eine Cyber-Sicherheitsstrategie entworfen. Für die zivile Sicherheit ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig (Bundesministerium des Innern, 2016). Das Auswärtige Amt soll für internationale Rechtsnormen sorgen, um Cyberangriffe und Eskalationsspiralen zu verhindern (Bundesministerium des Innern, 2016; S.14). Das Verteidigungsministerium (BMVg) und die Bundeswehr sind zuständig für die Verteidigungsaspekte. In der Bundeswehr gilt der Cyberraum als eigene Dimension neben Land, Luft und See; die Kompetenzen liegen im Organisationsbereich CIR (Cyber- und Informationsraum). Laut Weißbuch von 2016 hat die Bundeswehr die Aufgabe, offensiv und defensiv im Cyberraum zu agieren (vgl. die Bundesregierung, 2016; S.93). Denn laut BMVg reicht Defensive nicht aus, auch Offensive sei für die Abschreckung von Cyberangriffen

notwendig. (Koch, 2021). Um offensiv vorzugehen, beispielsweise um Daten in fremden Netzen zu verändern oder Netze zu beeinflussen, braucht die Bundeswehr ein Mandat des Bundestages, ebenso wie bei konventionellen militärischen Einsätzen (Hänel, 2020; 02:55). Aus rein zeittechnischen Gründen ist der Prozess der Mandatserteilung in den meisten Fällen jedoch nicht möglich, so dass die parlamentarische Kontrolle damit de facto entfällt (Widdig, 2016).

Friedensforscher*innen resümieren, dass Cybersicherheit eine starke Prävention, Defensive und Resilienz brauche. Auf die Bindung von Ressourcen zur Entwicklung von Gegenangriffen sollte hingegen verzichtet werden (vgl. Kreuzer in Werkner, 2019; S.82). Westliche Staaten sollten „der Versuchung scheinbar opferloser Konflikte widerstehen und sich besser darauf konzentrieren, die Sicherheit und Verteidigung zu verstärken und mögliche Verwundbarkeiten zu reduzieren“ (Schörnig in Werkner, 2019; S. 56). Möglichkeiten zur Minimierung von Risiko- und Bedrohungsschwachstellen liegen unter anderem in Firewalls und der Nutzung von IT-Strukturen von vertrauenswürdigen Hersteller*innen. Wichtig ist auch gute Disaster Recovery, um die Wiederherstellung von Daten und Infrastruktur sicherzustellen. Auch „Honeypots“ seien hilfreich, um potentielle Angreifer*innen abzulenken und ihre Vorgehensweise zu verstehen (vgl. ebd.; S.57). Auf Bundesebene sei auch eine unabhängige Prüfstelle für ein IT-Sicherheitszertifikat empfehlenswert (vgl. ebd. S. 131), welche in den Leitlinien des BSI auch vorhanden ist (Bundesministerium des Innern, 2016).

Zivilgesellschaftliche Fachverbände wie das Forum Informatiker*innen für den Frieden fordern die Entwicklung einer Digitalen Genfer Konvention, gemäß derer kritische Infrastruktur (d.h. für die Zivilbevölkerung lebenswichtig, z.B. Strom-, Wasser- und Gesundheitsversorgung) nicht angegriffen werden darf. Staaten sollen sich zu einer rein defensiven Sicherheitsstrategie verpflichten, also keine Offensivwaffen für den Cyberwar zu entwickeln oder gar einzusetzen, auch nicht aus präventiven Überlegungen heraus. Demokratische Transparenz der militärischen Aktivitäten muss gesichert sein. Wirtschaftliche Interessen wie ein Verstoß gegen Intellectual Properties sind kein legitimer Kriegsgrund. Staatliche Stellen, Unternehmen und Bürger*innen müssen zur Offenlegung von Schwachstellen verpflichtet werden. Onlineprotestformen dürfen nicht kriminalisiert werden (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 2017). Das Hackertoolverbot in der Bundesrepublik Deutschland, das Hacker*innen kriminalisiert, die ohne vertraglich festgelegten Auftrag nach Sicherheitslücken in IT-Infrastruktur suchen, soll geändert werden. Aktuell führe das dazu, dass deutsche Software weniger geprüft wird und Sicherheitslücken seltener repariert werden (Wilde et al.). Auf internationaler Ebene arbeitet die NGO CyberPeace Institute Geneva auf verschiedenen Ebenen

an diesen Themen. Der Fokus liegt auf der Unterstützung und dem Schutz von vulnerablen Bevölkerungsgruppen. Das Institut unterstützt Opfer von Cyberangriffen, analysiert Angriffe und Sicherheitslücken, setzt sich für internationale Regulierungen ein und untersucht neue Herausforderungen des globalen Cyberraums (https://cyberpeaceinstitute.org).

Auch im digitalen Raum gilt es, Militarisierung und Aufrüstung entgegen zu wirken, um Eskalationsspiralen zu vermeiden. Dafür muss das entsprechende Wissen vermittelt werden. Die Autorin lädt Sie ein, diese Themen in Ihre Schulklassen, Konfigruppen und Gruppen des politischen Engagements einzubringen. Im Anhang finden Sie dazu einen Unterrichtsentwurf und Textbausteine auch in einfacher Sprache. Außerdem lädt die Autorin Sie ein, bei Interesse den Literaturverweisen nachzugehen und sich tiefer einzulesen. Lassen Sie uns den Cyberpeace mitgestalten!

Pädagogische Anregungen

In diesem Kapitel werden beispielhaft einige Bausteine für Bildungsarbeit in Schulen und nicht-formellen Kontexten wie Konfirmand*innenarbeit, Politgruppentreffen oder Workshops mit Einladung zur weiteren Verwendung eingebracht. Dank der Anregung von Lehrer*innen findet sich in diesem Kapitel nicht nur ein Unterrichtsentwurf, sondern auch Texte in Leichter Sprache, die flexibel in diverse Unterrichtsformate integriert werden können.

Unterrichtsentwurf für digitalen Unterricht & Präsenzunterricht

Phase	Inhalt	Methode	Medium
Einstieg (10 Minuten)	Arte – Stories of Conflict: Cyberwar, Krieg 2.0, Sendung vom 18.09.2020, https://www.youtube.com/watch?v=O4JIw2WQK_g (zul. abger. am 04.04.21) *Alternativ:* Odysso - Wissen im SWR: Hackbacks bei der Bundeswehr?, Sendung vom 28.02.2020, https://www.youtube.com/watch?v=4_LQ2GLHMoE (zul. abger. am 04.04.21)	Videoanalyse	Video
Vertiefung I (50 Minuten)	Textanalyse in Fachsprache und Leichter Sprache: (siehe folgendes Unterkapitel „Textbausteine in Leichter Sprache“). Aufteilung der Schüler*innen oder Teilnehmenden in Gruppen, jede Gruppe übernimmt eine Rolle (Wissenschaft, Zivilgesellschaft, Hacker, Regierung, Bundeswehr, Kirche) für die spätere Diskussion. **Aufgaben:** Welche Position vertritt meine Rolle?	Textanalyse und Diskussion	Texte

	Welche Ziele, Wünsche und Argumente hat meine Rolle? Was kann passieren im Cyberwar und wie sollen wir damit umgehen, z.B. gesetzlich, was darf die Bundeswehr, die Hacker usw.? Notiert euch mindestens 5 Argumente.		
Vertiefung II (15 Minuten)	Fishbowl- oder Podiumsdiskussion: Eine Person pro Gruppe (Rolle), wahlweise Wechsel zwischen den Gruppen(Rollen)mitgliedern. Digital: Alle mit Kamera an zurück im Plenum. Dann: wer diskutiert, Kamera an, melden durch Meldefunktion, der Chat kann auch gerne integriert werden. Moderation durch Lehrer*in/ Trainer*in: Alle positionieren sich und diskutieren z.B. über die folgenden Fragen: • Soll der Bundestag weiterhin über jeden Offensivangriff abstimmen? Erfordert Cyberwar Geheimhaltung statt parlamentarischer Kontrolle? Darf die Bundeswehr Hackbacks durchführen? • Sollte die digitale Verteidigungsstrategie offensiv oder defensiv sein? • Ist das Hackertoolverbot sinnvoll? • Wie können wir die Resilienz stärken? • Welche Beschränkungen (Gesetze), Kompetenzen und rechtlichen Klärungen brauchen wir?	Diskussion (Fishbowl oder Podium) (weitere Methoden z.B. bei bpb: https://www.bpb.de/shop/lernen/thema-im-unterricht/36913/methoden-kiste).	
Auswertung (15 Minuten)	Haben sich Meinungen durch die Debatte verändert? Was nehmt ihr mit? Wie würdet ihr mit dem Thema umgehen?	Gruppen-diskussion	

Textbausteine in Leichter Sprache

*60% der Deutschen verstehen keine Fachsprache, 5% können nur mittels Leichter Sprache erreicht werden (Netzwerk Inklusion, 2020). In der Entwicklung des vorliegenden Dossiers wurde deutlich, dass die bislang als Grundlage für Friedensbildung vorliegenden Informationen zum Thema Cyberwar abstrakt und schwer verständlich sind, beispielsweise die Publikation: Werkner; Schörnig: Cyberwar- die Digitalisierung der Kriegsführung. Springer, 2019. Auch in der Friedensarbeit gibt es Wissenslücken: Viele Personen haben noch keinen Zugang zum Wissen über „neue Kriegsführung" gefunden. Fundiertes Wissen über Friedensthemen muss so vielen Menschen wie möglich zugänglich gemacht werden. Deswegen geht es der EAK als Herausgeberin in diesem Dossier darum, die Mechanismen der Kriegsführung im virtuellen Raum so zu vermitteln, dass jede*r sie verstehen kann.*

Einige der erläuterten Grundlagen zum Thema Cyberwar werden im Folgenden beispielhaft als Bausteine in Leichter und Fachsprache angeboten. Anhand dessen soll verdeutlicht werden,

welche Wirkung Texte in verschiedenen Verständlichkeitsstufen haben. Es werden beispielhaft einige Fachinhalte in Fachsprache und Leichter Sprache erklärt und nebeneinandergestellt.

*Um insgesamt möglichst viele Menschen zu erreichen, ist es wichtig, Informationen in verständlicher Sprache zur Verfügung zu stellen. Darum haben Initiativen wie Inclusion Europe und das Netzwerk für Leichte Sprache die Leichte Sprache als Instrument zur Vermeidung von Ausgrenzung entwickelt. Mittlerweile gibt es dafür einen Leitfaden, feste Kriterien, zahlreiche Online-Angebote sowie Testleser*innen, die testen, ob ein Text tatsächlich verständlich geschrieben wurde. Das Leseniveau liegt bei A1. Grundsätze sind beispielsweise leser*innenfreundliches Layout (linksbündig, große Schrift), Nebensätze vermeiden, Verben statt Substantive, Fachbegriffe unmittelbar erklären, lange Wörter mittels Bindestrich trennen, Aktiv statt Passiv, kein Konjunktiv oder Genitiv, nicht gendern, Beispiele geben. Neben der Leichten Sprache gibt es auch die vereinfachte Standardsprache, auch Einfache Sprache genannt; hier liegt das Sprachniveau bei A2/B1, es gibt jedoch bisher kein Regelwerk dafür. Sie macht einen normalsprachlichen Eindruck, vermeidet aber komplizierte Sprachelemente. Laut Netzwerk Inklusion können 60% der Deutschen Texte nicht verstehen, die komplexer als die vereinfachte Standardsprache sind. In Ansätzen gibt es mittlerweile Lexika für verständliche Sprache (www.hurraki.de; www.bpb.de/nachschlagen/lexika/lexikon-in-einfacher-sprache) und einen Leitfaden für Leichte Sprache (Bundesministerium für Arbeit und Soziales; Netzwerk Leichte Sprache, 2014). Auch gibt es Konzepte für sprachsensiblen Unterricht. Kernelement ist, inhaltliche und sprachliche Lernziele gemeinsam zu betrachten. In der Umsetzung gilt es, zwischen Darstellungsformen zu wechseln und Sprachhilfen anzubieten.*

Dieses Kapitel fokussiert sich auf Beispiele für Leichte Sprache und Fachsprache. Es soll anregen, ganzheitlich sprachsensible Lernsituationen zu schaffen. Die folgenden Textbausteine zeigen eine von vielen Möglichkeiten, Wissensvermittlung sprachsensibel zu gestalten.

Grundlagen zur Einführung in das Thema

Fachsprache	Leichte Sprache
Der Begriff Cyberwar beschreibt eine kriegerische Auseinandersetzung zwischen Staaten im virtuellen Raum, die mit Mitteln der Informationstechnologie geführt wird. Ein Cyberkrieg hat zum Ziel, Ländern, Institutionen oder der Gesellschaft auf elektronischem Weg Schaden zuzufügen und wichtige Infrastrukturen zu stören. Dabei werden häufig drei Szenarien thematisiert:	Cyber-War ist Englisch und bedeutet Krieg im Internet. Das Ziel von Cyber-War ist: auf elektronischem Weg Ländern Schaden zufügen. Digitale Technologie wird immer wichtiger in unserem Leben. Diese digitale Technologie wird angegriffen, damit sie nicht mehr funktioniert. Davor haben viele Menschen Angst. Die Technologien sind neu. Darum wissen viele Menschen nicht, was passieren kann. Es gibt 3 Gefahren:
1. unsichere Infrastruktur: Sicherheitslücken in Software und punktuelles Ausnutzen derer geschieht sehr häufig. Sicherheitslücken sind die Munition für den Cyberwar.	1. Software sagt dem Computer, was er machen muss, wenn ein Mensch eine Taste drückt. Ein anderes Wort ist: Computer-Programm. Oder: App. Software hat eine virtuelle Mauer, um sich vor Angriffen zu schützen. Manchmal gibt es Löcher in der Mauer. Diese Löcher heißen Sicherheits-Lücken.

	Manche Menschen suchen die Sicherheitslücken. Diese Menschen heißen Hacker. Manche Hacker wollen etwas kaputt machen oder Informationen klauen. Oft arbeiten sie im Auftrag von einem Land oder sind Kriminelle. Das passiert sehr oft. Diese Sicherheits-Lücken machen Angriffe und Cyber-War möglich. Das nennt man: un-sichere Infra-Struktur.
2. komplette Infiltration: Systeme sind gehackt und infiltriert. Dies wird teilweise als Verhandlungsmasse genutzt, denn die Bedrohung ist zu wissen, dass „die Anderen" dies technisch machen könnten.	2. Hacker können durch die Sicherheits-Lücken in einer Software die ganze Software kaputt machen oder alle Informationen klauen. Zum Beispiel: persönliche Konto-Daten. Oder Geheimnisse aus der Regierung. Oder die Strom-Versorgung in einem Krankenhaus. Das nennt man: komplette Infiltration. Das passiert selten. Aber es ist eine große Bedrohung. Denn wir wissen: das ist möglich. Manchmal droht ein Land einem anderen Land damit. Um seinen Willen zu bekommen.
3. aktiver Cyberkrieg: konkrete Angriffe im virtuellen Raum sowie mit konventionellen Waffen, Tote und Verletzte. De facto das meistbesprochene, aber am wenigsten relevante Szenario.	3. Elektronische Angriffe, Tote und Verletzte. Zum Beispiel: ein Land macht über das Internet die Strom-Versorgung in Deutschland kaputt. Dann funktioniert nichts mehr. Chaos entsteht. Die Krankenhäuser können nicht mehr richtig arbeiten. Deutschland wirft Bomben auf das andere Land, damit sie aufhören. Das nennt man: aktiver Cyber-Krieg. Viele Menschen reden darüber. Aber das passiert wahrscheinlich nicht.
Die meisten Cyberangriffe lösen nicht das Selbstverteidigungsrecht aus, z.B. Spionage oder Wahlmanipulation. Denn Daten gelten rechtlich nicht als Objekte, so dass hier keine Gewaltanwendung vorliegt- mit Ausnahme von Angriffen auf die kritische Infrastruktur, wenn sie großen Schaden auslösen. (Widdig, 2016) Wenn Cyberangriffe ein gewisses Ausmaß an Gewalt und ihrer Wirkung haben, dann wird das völkerrechtliche Gewaltverbot verletzt. Dieses Ausmaß muss dem einer Anwendung konventioneller Waffen gleichen, etwa weil Menschen verletzt oder getötet oder erhebliche Sachgüter zerstört wurden. (Deutscher Bundestag, 2018, S. 3).	Viele Angriffe im Internet sind klein und machen wenig kaputt. Zum Beispiel: Spionage oder Be-Einflussung von Wahlen. Manchmal machen Angriffe sehr viel kaputt. Auch im Internet. Zum Beispiel: viele Menschen sind verletzt. Oder tot. Oder wichtige Sachen sind kaputt. Das ist verboten. Viele Staaten haben das zusammen gesagt. Dann darf der Staat sich wehren. Die Bundes-Wehr macht oft Angriffe. Aber der Bundes-Tag, also das Parlament, muss erst ja sagen. Das Problem ist: die Bundes-Wehr muss die Angriffe schnell machen. Sie kann den Bundes-Tag nicht fragen.

Außerhalb des Verteidigungsfalles dürfen offensive Cyber-Maßnahmen nur mit Bundestagsmandat durchgeführt werden. Allerdings werden die Meisten bereits beendet sein, bevor das Parlament überhaupt befragt werden kann. (Widdig, 2016)	

Bereits Aufklärungsaktionen im Cyberraum können das Verbot friedensstörender Handlungen (Artikel 26, Absatz 1 Grundgesetz) brechen, weil dabei häufig Manipulationen an den fremden IT-Systemen vorgenommen werden. Die Zunahme von solchen (nachrichtendienstlichen und militärischen) Aktivitäten erhöht das Eskalationspotenzial, obwohl sie sich unterhalb der Schwelle offener militärischer Konflikte befinden. Fehlende internationale Vereinbarungen über Begrenzungen solcher Aktivitäten in IT-Systemen steigern das Risiko von Fehlinterpretationen und damit auch Fehlreaktionen. Aktuell werden vor allem militärische Offensiv-Maßnahmen für den Cyberraum entwickelt. Weil IT-Fachkräfte und technisches Wissen knappe Ressourcen sind, wird dadurch der Aufbau einer gemeinsamen zivilen IT-Sicherheit in Deutschland vernachlässigt (Reinhold, 2020; S. 2). Auch der wissenschaftliche Dienst des Bundestags kommt zu der Einschätzung, dass Abschreckung durch Angriffe ineffektiv sei und ein Risiko für Gegenangriffe mit den eigenen Waffen berge (Meister; Biselli, 2019).	Die deutsche Armee, also die Bundes-Wehr, sucht über das Internet nach geheimen Informationen in anderen Staaten. Das passiert immer öfter. Oft verändern sie dabei etwas in den Programmen von dem anderen Staat. Aber eigentlich sagt das Grund-Gesetz: niemand darf den Frieden zwischen Staaten kaputt machen. Auch nicht im Internet. Vielleicht ist der andere Staat dann wütend und macht etwas bei dem Anderen kaputt. Und ihr Streit wird immer größer. Das nennt man: Eskalation. Vielleicht gibt es sogar Krieg. Viele Länder auf der Welt haben gesagt: wir wollen keinen Krieg. Die Länder sollen auch sagen: wir wollen keinen Krieg im Internet. Wir wollen Vertrauen haben zu anderen Staaten. Darum wollen wir nur Technologien bauen für Verteidigung. Nicht für Angriffe. Leider bauen heute viele Staaten Technologien für Angriffe. Das ist der Regierung wichtig. Es gibt wenige Menschen die das bauen können. Darum werden wenig Technologien für Verteidigung gebaut.

Vertiefung: Problematiken im Themenfeld, Beispiel dual-use-Problematik

Fachsprache	Leichte Sprache
Dual Use-Technologien sind doppelverwendungsfähige Technologien oder Produkte, die für zivile und militärische Zwecke genutzt werden können. Im Fall der europäischen Firma FinFisher wurden Produkte von deutschen Sicherheitsbehörden gekauft, aber während des arabischen Frühlings auch an das autoritäre Regime in Bahrain exportiert, um dort gegen Oppositionelle vorzugehen. Als Versuch, damit	Digitale Technologie wird immer wichtiger in unserem Leben. Oft kann die gleiche Technologie für militärische und nicht-militärische Zwecke benutzt werden. Das sind Dual-Use-Technologien. Zum Beispiel: Die Firma FinFisher verkauft Software an Deutschland. Die Software kann manchmal Terroristen über das Internet

umzugehen, gibt es die Dual-Use-Verordnung der EU, seit 2015 wird darin auch Überwachungstechnologie erfasst. Solche Exporte werden jedoch meistens genehmigt. Friedensorganisationen fordern daher strenge Prüfungen anhand von moralischen Gesichtspunkten (Human Rights Watch 2020). Ein weiterer Versuch, mit umzugehen ist das Hackertoolverbot in der BRD. Seit 2008 ist es strafbar, Sicherheitslücken durch Testprogramme ausfindig zu machen, weil diese Programme auch für das Eindringen in fremde Systeme genutzt werden können. Dadurch ist es allerdings auch illegal, Sicherheitslücken durch Tests zu suchen um sie zu reparieren (Wilde et al.).	finden. Die Firma FinFisher verkauft die gleiche Software auch an andere Länder. In dem Land Bahrain bestraft die Regierung Menschen, die eine andere Meinung haben. Dafür hat die Regierung die Software von FinFisher gekauft. Dann wird die Software benutzt, um Menschen zu bestrafen. Eigentlich hatte die Software einen guten Zweck. Darum prüft der Zoll jedes Mal, ob eine Dual-Use-Technologie an andere Länder verkauft werden darf oder nicht. Leider entscheidet der Zoll oft falsch. Dann kann die Technologie trotzdem für schlechte Dinge benutzt werden. Friedens-Organisationen fordern: der Zoll muss die Exporte strenger prüfen. Ein Export darf nur erlaubt werden, wenn er keine Menschen-Rechte gefährdet. Wenn der Export trotzdem erlaubt wird, nur damit Deutschland mehr Geld verdient, dann ist das schlecht.

Fishbowl- oder Podiumsdiskussion: Akteur*innen und ihre Positionen

	Fachsprache	Leichte Sprache
Resilienz und Vertrauen sind effektiver als offensive Fähigkeiten:		
Zivilgesellschaft (Stiftung neue Verantwortung)	Sie haben keine empirischen Belege dafür, dass Abschreckung (Androhung der Vergeltung) im Cyberraum wirken kann. Sie haben aber empirische Belege dafür, dass Abschreckung durch eigene Sicherheits- und Resilienzmaßnahmen wirken kann, weil Angreifer*innen es schwer haben und angegriffene Systeme schnell wiederhergestellt werden können (Odysso, 2020; 4:10-4:36) Der Cyberraum wird untrennbar für zivile und militärische Aktivitäten genutzt, darum müssen in der Cyberverteidigungspolitik alle relevanten Politikbereiche einbezogen werden. Die Bundesregierung muss eine konkrete Strategie entwickeln, die Richtlinien im Weißbuch präzisieren (der aktuelle Leitfaden für die deutsche Sicherheitspolitik). Das Weißbuch betont die defensive Cyberabwehr,	Angriffe im Internet sollen anderen Staaten Angst machen. Damit sie uns nicht angreifen. Wir haben gesehen: das klappt nicht. Es gibt die andere Möglichkeit: verteidigen. Dafür müssen viele Menschen aufpassen: dass es kein Loch in der Schutz-Mauer gibt. Sie müssen die Mauer reparieren. Dann können Angreifer nicht durch die Mauer kommen. Das Internet wird für Militär genutzt und für das normale Leben genutzt. Darum müssen verschiedene Ministerien zusammen entscheiden, was sie als nächstes machen. Die Regierung muss konkret alles aufschreiben. Die Regierung muss dann das tun was sie aufschreibt. Das hilft: damit die Staaten sich vertrauen. Damit ein Streit nicht eskaliert, also immer größer wird. Deutschland soll mit der Europäischen Union reden.

	während in der Praxis v.a. die Offensive gefördert wird. Solche Inkohärenzen darf es nicht geben, denn wir brauchen Vertrauen und anerkannte Verhaltensnormen im Cyberraum, um Eskalation und Konflikte zu verringern. Gemeinsam mit der EU soll eine Cybersicherheitsstrategie entwickelt werden (Schuetze, 2021; S. 1ff).	
Pflicht zur Offenlegung und Legalität von Protest:		
Hacker (Forum Informatiker *innen für den Frieden)	Forderung nach einer Digitalen Genfer Konvention, gemäß derer kritische Infrastruktur (=für die Zivilbevölkerung lebenswichtig, z.B. Strom-, Wasser-, Gesundheitsversorgung etc.) nicht angegriffen werden darf. Staaten sollen sich zu einer rein defensiven Sicherheitsstrategie verpflichten. Wirtschaftliche Interessen wie ein Verstoß gegen Intellectual Properties sind kein legitimer Kriegsgrund. Staatliche Stellen, Unternehmen und Bürger*innen müssen zur Offenlegung von Schwachstellen verpflichtet werden. Onlineprotestformen dürfen nicht kriminalisiert werden (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 2017). Hacker suchen häufig nach Sicherheitslücken in IT-Infrastruktur. Das ist in Deutschland strafbar, wenn es keinen Auftrag von dem entsprechenden Unternehmen gibt. Das Hackertoolverbot führt dazu, dass deutsche Software weniger geprüft wird und Sicherheitslücken seltener repariert werden. Hacker*innen fordern, dass dieses Verbot geändert wird (Wilde et al.).	Hacker fordern: - die Staaten müssen Regeln machen für den Krieg im Internet. Es soll drin stehen: lebens-wichtige Sachen dürfen nicht angegriffen werden. Das nennt man: kritische Infra-Struktur. Zum Beispiel: Kranken-Häuser. - Staaten dürfen im Internet nur Abwehr planen und machen. Keine Angriffe. - man darf keinen Krieg um Geld führen - Manchmal finden Geheim-Dienste Löcher in der Sicherheits-Mauer. Manchmal verraten sie das nicht. Weil: durch die Löcher können sie spionieren. Hacker fordern: der Finder muss Löcher immer verraten. Damit sie repariert werden können. - Protestieren kann man auf der Straße und auch im Internet. Das muss immer erlaubt sein, auch im Internet. - Hacker suchen Sicherheits-Löcher. In Deutschland müssen sie aufpassen. Oft verstoßen sie dabei gegen das Gesetz. Darum arbeiten Hacker im Ausland. Die Wirkung: deutsche Programme werden weniger geprüft und repariert. Sie sind weniger sicher. Hacker fordern: das Gesetz muss geändert werden.
Ressortübergreifend und Verfassungskonform:		
Regierung u. parlamen-tarische Kontrolle	Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. (Deutscher Bundestag, 2018, S. 3). Weißbuch 2016: Das Bundesministerium des Innern, für Bau	Die deutsche Armee, also die Bundes-Wehr, muss das Parlament, also den Bundes-Tag, um Erlaubnis fragen: dürfen wir einen anderen Staat angreifen? Die Bundes-Wehr muss auch fragen, wenn sie einen Angriff im Internet machen will.

	und Heimat (BMI) ist dafür zuständig, eine Cybersicherheitsstrategie zu erarbeiten (Bundesministerium des Innern, 2016). Das Verteidigungsministerium (BMVg) und die Bundeswehr sind für die Verteidigungsaspekte zuständig. Die Gesamtverantwortung für die internationale Cybersicherheitspolitik liegt beim Auswärtigen Amt (die Bundesregierung, 2016; S. 38).	Das Internet ist für Alle wichtig: im Krieg und im zivilen Leben. Darum müssen Alle zusammen arbeiten für Sicherheit im Internet. - Das Innen-Ministerium soll überlegen und arbeiten: wie kann sich Deutschland schützen vor Angriffen aus dem Internet? Was machen wir, wenn wir angegriffen werden? - Das Verteidigungs-Ministerium und die Bundes-Wehr sollen eine militärische Strategie entwickeln. - Das Außen-Ministerium soll an der welt-weiten Politik für Sicherheit im Internet arbeiten.
Offensive Abschreckung und Pragmatismus:		
Verteidigungsministerium & Bundeswehr	Wir brauchen eine leistungsfähige, gesamtstaatliche Cyber-Sicherheitsarchitektur für mehr Systemresilienz, v.a. um die kritischen Infrastrukturen zu schützen. Defensive Maßnahmen alleine reichen nicht aus. Offensive Fähigkeiten können zur Gewährleistung der Cybersicherheit beitragen und sind notwendig für den Erhalt der militärischen Handlungsfähigkeit. Ist die parlamentarische Kontrolle noch zeitgemäß? (Koch, 2021).	Wir müssen zusammen-arbeiten. Wir brauchen eine gemein-same Strategie: wie wir Angriffe abwehren. Wie wir mit neuen Situationen umgehen. Und wann wir andere Staaten angreifen. Wir brauchen mehr Geld. Wir müssen die kritische Infra-Struktur, also die lebens-wichtigen Sachen, beschützen. Abwehr reicht nicht. Wir müssen auch angreifen können. Damit andere Länder Angst haben. Damit andere Länder uns nicht angreifen. Und damit wir uns wehren können, wenn uns ein anderes Land angreift.
Cyberrecht im Völkerrecht und Vorrang für Zivil:		
Kirchen (EKD)	EKD-Synodenkundgebung 2019: Militärische Cyberkommandos sind an rechtsstaatliche Verfahren zu binden, ihre Kontrolle ist durch die staatlichen Organe und ihre Verbindung mit nichtmilitärischen Einrichtungen der Aufklärung und Gefahrenabwehr zu sichern und zu stärken. Wir sprechen uns dafür aus, bei der Cyber-Abwehr vor allem zivile Strukturen und defensive Maßnahmen zu stärken. Wir sehen die Notwendigkeit, ein völkerrechtlich verbindendes Cyberrecht zu entwickeln und einzuführen (Evangelische Kirche in Deutschland, 2019, S. 6).	Das Parlament der evangelischen Kirche hat 2019 gesagt: Die Bundeswehr arbeitet im Internet. Dafür muss sie die Gesetze befolgen. Zum Beispiel: sie muss das Parlament, also den Bundestag, fragen. Wir brauchen auch neue Gesetze für die Kontrolle. Wir brauchen auch zivile, also nicht-militärische Experten, die zivil sind, also die nicht bei der Bundes-Wehr sind. Deutschland soll mehr Geld geben für zivile Experten. Und mehr für Abwehr. Deutschland soll weniger Geld geben für die Bundes-Wehr. Und weniger für Angriffe.

		Wir brauchen ein Völker-Recht für das Internet. Das heißt: wir brauchen Regeln für den Krieg im Internet.

Im Anhang finden Sie die beiden Fassungen als Fließtext.

Leichte Sprache zwingt den*die Autor*in, präzise zu formulieren. Sie nimmt der Sprache zahlreiche Facetten und Schönheit, kann aber auch neue Schönheiten eröffnen. Details gehen zum Teil verloren, denn um auch die Textlänge angemessen zu gestalten, müssen zwangsläufig Informationen weggelassen werden. Auch ist es eine Herausforderung, einen Text in verständlicher Sprache zu schreiben: selbst die Beispiele im vorliegenden Dossier können sicher noch einfacher formuliert werden. Weitere Schritte für leichtere Verständlichkeit sind graphische und symbolische Darstellungen als Ergänzung zum Text. Doch es lohnt sich: Bereits der Versuch befähigt eine große Zahl von Kindern und Erwachsenen dazu, eigenständig Informationen einzuholen, sich fortzubilden und damit auch sich eine Meinung zu bilden. Friedensethische Bildung an alle Menschen heranzutragen, ist unerlässlich für Inklusion, gesellschaftlichen Zusammenhalt und eine breite zivilgesellschaftliche Beteiligung an politischen Prozessen. Nur wer von friedensethischen Themen weiß, kann sich für den Frieden einsetzen.

Anregung für weitere Projektarbeiten

Im Anschluss an dieses Dossier könnte beispielsweise ein Lernspiel als Handy-App programmiert werden, anhand dessen sich vor allem junge Menschen mit den friedensethischen und Gewissensfragen beschäftigen können, in dem sie Entscheidungen treffen müssen (was tun, wenn...). Nebenbei könnte punktuell Wissen vermittelt werden. Diese digitale Form ist in Pandemie-Zeit besonders geeignet. Beispiele könnten die folgenden Spiele sein: http://www.lastexitflucht.org/againstallodds/, http://keep-cool-mobil.de/, https://www.getbadnews.de/#intro oder https://kapitalismusgame.bpb.de/. Die vorliegenden Begleitmaterialien können Multiplikator*innen Hintergrundinformationen und pädagogische Bausteine anbieten. Zur besseren Anpassung an die unterschiedlichen Bedürfnisse der Schüler*innen sind die Informationen in den Begleitmaterialien in zwei Schwierigkeitsstufen zur Verfügung gestellt: in Leichter sowie in Fachsprache. Anlässlich der Veröffentlichung der App könnte eine öffentliche (online-)Auftaktveranstaltung organisiert werden: eine Podiumsdiskussion mit Expert*inneneinschätzungen durch Hacker*in, BMI/BMVg, Wissenschaftler*in aus technischer & ethischer Perspektive. Im Falle eines online-Formats würde die Veranstaltung als Livestream angeboten und dauerhaft online zur Verfügung gestellt (Youtube) werden können. Wichtig für ein solches Projekt sind Kooperationspartner*innen, ein*e externe*r Berater*in für digitale Spieleentwicklung sowie eine breit angelegte Öffentlichkeitsarbeit.

Quellenangaben & Literaturhinweise zur Weiterarbeit

Arte (18.09.2020): Stories of Conflict- Cyberwar Krieg 2.0, https://www.youtube.com/watch?v=O4JIw2WQK_g (zul. abger. am 04.04.21)

Biermann, Kai (12.07.2029): Deutschland will zurückhacken. Zeit Online, https://www.zeit.de/digital/internet/2019-07/hackback-cyberwar-datensicherheit-digitaler-angriff-bundesregierung (zul. abger. am 04.04.21)

Bundesministerium der Verteidigung (2020): Entwicklung des Organisationsbereichs der Bundeswehr, https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/entwicklung-des-org-bereich-bei-der-bw (zul. abger. am 04.04.21)

Bundesministerium des Inneren (2016): Cyber-Sicherheitsstrategie für Deutschland, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (zul. abger. am 04.04.21)

Bundesministerium für Arbeit und Soziales; Netzwerk Leichte Sprache (2014): Leichte Sprache. Ein Ratgeber, https://www.bmas.de/SharedDocs/Downloads/DE/Publikationen/a752-ratgeber-leichte-sprache.pdf?__blob=publicationFile&v=1 (zul. abger. am 04.04.21)

Bundeszentrale für politische Bildung (2017): Was sind Social Bots?, https://www.bpb.de/252585/was-sind-social-bots (zul. abger. am 04.04.21)

Bundeszentrale für politische Bildung (2016): Automatisierte und autonome Systeme in der Militär- und Waffentechnik, https://www.bpb.de/apuz/232968/automatisierte-und-autonome-systeme (zul. abger. am 04.04.21)

Bundeszentrale für politische Bildung: einfachPOLITIK: Lexikon, https://www.bpb.de/nachschlagen/lexika/lexikon-in-einfacher-sprache/ (zul. abger. am 04.04.21)

CyberPeace Institute: https://cyberpeaceinstitute.org/

Deutscher Bundestag (2018): Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland, https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf (zul. abger. am 04.04.21)

Die Bundesregierung (2016): Weißbuch, Zur Sicherheitspolitik und zur Zukunft der Bundeswehr, https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf (zul. abger. am 04.04.21)

Ethik und Militär (01/2019): Konfliktzone Cyberspace- Perspektiven für Sicherheit und Frieden. Zebis, Hamburg, http://www.ethikundmilitaer.de/fileadmin/ethik_und_militaer/Ethik-und-Militaer-2019-1.pdf (zul. abger. am 04.04.21)

Evangelische Kirche in Deutschland (2019): Kundgebung der 12. Synode der Evangelischen Kirche in Deutschland auf ihrer 6. Tagung, https://www.ekd.de/ekd_de/ds_doc/Kundgebung-Kirche-auf-dem-Weg-der-Gerechtigkeit-und-des-Friedens.pdf (zul. abger. am 04.04.21)

Evangelische Kirche in Deutschland (2021): Freiheit digital. Die Zehn Gebote in Zeiten des digitalen Wandels. Eine Denkschrift der Evangelischen Kirche in Deutschland, https://www.ekd.de/ekd_de/ds_doc/denkschrift_freiheit_digital_EVA_2021.pdf (zul. abger. am 29.04.21)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (2018): Cyberpeace- nur ein ziviles Internet ist nachhaltig, https://media.ccc.de/v/bub2018-151-cyberpeace_-_nur_ein_ziviles_internet_ist_nachhaltig#t=36 (zul. abger. am 04.04.21)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.: Einige Begriffsdefinitionen, https://cyberpeace.fiff.de/Kampagne/Definitionen/ (zul. abger. am 04.04.21)

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (2017): Forderungen des FIfF zum Cyberpeace, https://www.fiff.de/themen/ruin/ruestung-und-informatik/forderungen-des-fiff-zum-cyberpeace (zul. abger. am 04.04.21)

Flögel, Florian (2014): Cyberwar- Systematisierung und Kategorisierung einer „neuen" Bedrohung, https://www.ispk.uni-kiel.de/de/publikationen/upload-working-paper/KASZ%2035.pdf (zul. abger. am 04.04.21)

Gebauer, Matthias (2016): Bundeswehr- Hacker knackten afghanisches Mobilfunknetz, https://www.spiegel.de/politik/ausland/cyber-einheit-bundeswehr-hackte-afghanisches-mobilfunknetz-a-1113560.html (zul. abger. am 04.04.21)

Gessat, Michael (2012): Allianz gegen Cyber- Attacken, https://www.deutschlandfunk.de/allianz-gegen-cyber-attacken.684.de.html?dram:article_id=207703 (zul. abger. am 04.04.21)

Hänel, Michael (2020): Hackbacks bei der Bundeswehr? https://www.ardmediathek.de/ard/video/Y3JpZDovL3N3ci5kZS9hZXgvbzEyMDUxNDE (zul. abger. am 04.04.21)

Heinemann-Grüder, Andreas; Wiggen, Johannes (2020): Subversion im Cyberraum- Sicherheit, freiheit und Resilienz gegen Angriffe im Netz. Institut für Auslandsbeziehungen, Stuttgart, https://www.bicc.de/uploads/tx_bicctools/subversion-cyberraum_heinemann_wiggen_01.pdf (zul. abger. am 04.04.21)

Hofstetter, Julia-Silvana (2021): Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Agenda Forward, INEF Report 114/2021, Duisburg: Institute for Development and Peace. https://www.uni-due.de/imperia/md/images/inef/ir114_hofstetter-final-web-1.pdf (zul. abger. am 229.04.21)

Human Rights Watch (2020): EU- Export von Überwachungstechnologien verschärfen, https://www.hrw.org/de/news/2020/06/12/eu-export-von-ueberwachungstechnologien-verschaerfen (zul. abger. am 04.04.21)

Human Rights Watch; International Human Rights Clinic (2018): Heed the Call- a Moral and Legal Imperative to Ban Killer Robots, https://www.hrw.org/report/2018/08/21/heed-call/moral-and-legal-imperative-ban-killer-robots (zul. abger. am 04.04.21)

Hurraki Wiki: Wörterbuch für Leichte Sprache, https://hurraki.de/wiki/Hauptseite (zul. abger. am 04.04.21)

Killer Roboter stoppen! (2015): Waffensysteme mit autonomen Fähigkeiten, https://www.killer-roboter-stoppen.de/files/2015/11/autonomewaffensysteme.pdf (zul. abger. am 04.04.21)

Koch, Dr. Robert (2021): Stellungnahme zur öffentlichen Anhörung im Verteidigungsausschuss am 15. März 2021, https://www.bundestag.de/resource/blob/827490/3c014ce226f491f0b39701614415868c/stellungnahme-Robert-Koch_15-03-2021-data.pdf (zul. abger. am 04.04.21)

Kreuzer, Leonhard (2019): Hobbesscher Naturzustand im Cyberspace? Enge Grenzen der Völkerrechtsdurchsetzung bei Cyberangriffen. In: Werkner; Schörnig: Cyberwar- die Digitalisierung der Kriegsführung, Bd. 6, Wiesbaden: Springer.

Luber, Stefan & Schmitz, Peter (2017): Was ist Cyberwar?, https://www.security-insider.de/was-ist-cyberwar-a-672813/ (zul. abger. am 04.04.21)

Matthiessen, Philip (2018): CyberWar- Die Gefahr aus dem Netz, https://politik-digital.de/news/cyberwar-rezension-155574/ (zul. abger. am 04.04.21)

Meister, Andre; Biselli, Anna (2019): Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung, https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/ (zul. abger. am 04.04.21)

Netzwerk Inklusion Landkreis Tischenreuth (2020): Verständliche Sprache, https://www.inklusion-tirschenreuth.de/verstaendliche-sprache.html (zul. abger. am 04.04.21)

Odysso Wissen im SWR (28.02.2020): Hackbacks bei der Bundeswehr?, https://www.youtube.com/watch?v=4_LQ2GLHMoE (zul. abger. am 04.04.21)

Reinhold, Thomas (2020): Stellungnahme zur öffentlichen Anhörung am 14.12.2020 im Verteidigungsausschuss des deutschen Bundestages, https://www.bundestag.de/resource/blob/824622/67fc9db4f856a8445355562500d2a134/stellungnahme-Thomas-Reinhold_15-03-2021-data.pdf (zul. abger. am 04.04.21)

Roodsari, Ali Vahid (2020): Wo sich USA und Iran seit Jahren bekriegen, https://www.t-online.de/digital/sicherheit/id_87102062/iran-konflikt-cyberwar-seit-2010-wo-sich-die-usa-und-der-iran-bekriegen.html#utm_source=feeds&utm_medium=upday&utm_campaign=digital (zul. abger. am 04.04.21)

Schuetze, Julia (2021): Sachverständigen Statement, https://www.bundestag.de/resource/blob/824488/ea47db48d30b5aa32acd846b6ded1996/stellungnahme-Julia-Schuetze_15-03-2021-data.pdf (zul. abger. am 04.04.21)

Schünemann, Wolf J. (2018): Internet und Digitalisierung als Gefahren für die Demokratie?, https://demokratie.niedersachsen.de/startseite/themen/digitalisierung/gefahren_fur_demokratie/internet-und-digitalisierung-als-gefahren-fuer-die-demokratie-163532.html (zul. abger. am 04.04.21)

Vereinte Nationen (2013): UN-Dok. A/68/98 vom 24.06. 2013, para 20, https://digitallibrary.un.org/record/753055 (zul. abger. am 04.04.21)

Vereinte Nationen (2015): UN-Dok. A/70/174 vom 22.07.2015, para 28c

Werkner, Ines- Jacqueline & Schörnig, Niklas (2019) [Hrsg.]: Cyberwar- die Digitalisierung der Kriegsführung, Bd. 6, Wiesbaden: Springer.

Widdig, Vincent (2016): Völker- vs. Wehrverfassungsrecht- Neue Grenzen des Parlamentsvorbehalts beim Einsatz der Bundeswehr im Cyber-Raum? In: Junge Wissenschaft im öffentlichen Recht, https://www.juwiss.de/50-2016/ (zul. abger. am 04.04.21)

Wilde et al. Rechtsanwälte: Penetrationstests, https://www.wbs-law.de/it-und-internet-recht/computerkriminalitaet/penetrationstests/ (zul. abger. am 04.04.21)

Wussow, Philipp von (2020): Keine Aussicht auf Cyberfrieden. In: Zur Sache BW 37, 1/2020.

ANHANG: Textbausteine als Fließtexte

Standardsprache

Grundlagen zur Einführung in das Thema

Der Begriff Cyberwar beschreibt eine kriegerische Auseinandersetzung zwischen Staaten im virtuellen Raum, die mit Mitteln der Informationstechnologie geführt wird. Ein Cyberkrieg hat zum Ziel, Ländern, Institutionen oder der Gesellschaft auf elektronischem Weg Schaden zuzufügen und wichtige Infrastrukturen zu stören. Dabei werden häufig drei Szenarien thematisiert:

1. unsichere Infrastruktur: Sicherheitslücken in Software und punktuelles Ausnutzen derer geschieht sehr häufig. Sicherheitslücken sind die Munition für den Cyberwar.
2. komplette Infiltration: Systeme sind gehackt und infiltriert. Dies wird teilweise als Verhandlungsmasse genutzt, denn die Bedrohung ist zu wissen, dass „die Anderen“ dies technisch machen könnten.
3. aktiver Cyberkrieg: konkrete Angriffe im virtuellen Raum sowie mit konventionellen Waffen, Tote und Verletzte. De facto das meistbesprochene, aber am wenigsten relevante Szenario.

Die meisten Cyberangriffe lösen nicht das Selbstverteidigungsrecht aus, z.B. Spionage oder Wahlmanipulation. Denn Daten gelten rechtlich nicht als Objekte, so dass hier keine Gewaltanwendung vorliegt- mit Ausnahme von Angriffen auf die kritische Infrastruktur, wenn sie großen Schaden auslösen (Widdig, 2016). Wenn Cyberangriffe ein gewisses Ausmaß an Gewalt und ihrer Wirkung haben, dann wird das völkerrechtliche Gewaltverbot verletzt. Dieses Ausmaß muss dem einer Anwendung konventioneller Waffen gleichen, etwa weil Menschen verletzt oder getötet oder erhebliche Sachgüter zerstört wurden (Deutscher Bundestag, 2018, S. 3). Außerhalb des Verteidigungsfalles dürfen offensive Cyber-Maßnahmen nur mit Bundestagsmandat durchgeführt werden. Allerdings werden die Meisten bereits beendet sein, bevor das Parlament überhaupt befragt werden kann (Widdig, 2016).

Bereits Aufklärungsaktionen im Cyberraum können das Verbot friedensstörender Handlungen (Artikel 26, Absatz 1 Grundgesetz) brechen, weil dabei häufig Manipulationen an den fremden IT-Systemen vorgenommen werden. Die Zunahme von solchen (nachrichtendienstlichen und militärischen) Aktivitäten erhöht das Eskalationspotenzial, obwohl sie sich unterhalb der Schwelle offener militärischer Konflikte befinden. Fehlende internationale Vereinbarungen über Begrenzungen solcher Aktivitäten in IT-Systemen steigern das Risiko von Fehlinterpretationen und damit auch Fehlreaktionen.

Aktuell werden vor allem militärische Offensiv-Maßnahmen für den Cyberraum entwickelt. Weil IT-Fachkräfte und technisches Wissen knappe Ressourcen sind, wird dadurch der Aufbau einer gemeinsamen zivilen IT-Sicherheit in Deutschland vernachlässigt (Reinhold, 2020; S. 2). Auch der wissenschaftliche Dienst des Bundestags kommt zu der Einschätzung, dass Abschreckung durch Angriffe ineffektiv sei und ein Risiko für Gegenangriffe mit den eigenen Waffen berge (Meister; Biselli, 2019).

Vertiefung: Problematiken im Themenfeld, Beispiel dual-use-Problematik

Dual Use-Technologien sind doppelverwendungsfähige Technologien oder Produkte, die für zivile und militärische Zwecke genutzt werden können. Im Fall der europäischen Firma FinFisher wurden Produkte von deutschen Sicherheitsbehörden gekauft, aber während des arabischen Frühlings auch an das autoritäre Regime in Bahrain exportiert, um dort gegen Oppositionelle vorzugehen. Als Versuch, damit umzugehen, gibt es die Dual-Use-Verordnung der EU, seit 2015 wird darin auch Überwachungstechnologie erfasst. Solche Exporte werden jedoch meistens genehmigt.

Friedensorganisationen fordern daher strenge Prüfungen anhand von moralischen Gesichtspunkten (Human Rights Watch 2020).

Ein weiterer Versuch, mit umzugehen ist das Hackertoolverbot in der BRD. Seit 2008 ist es strafbar, Sicherheitslücken durch Testprogramme ausfindig zu machen, weil diese Programme auch für das Eindringen in fremde Systeme genutzt werden können. Dadurch ist es allerdings auch illegal, Sicherheitslücken durch Tests zu suchen um sie zu reparieren (Wilde et al.).

Fishbowl- oder Podiumsdiskussion: Akteur*innen und ihre Positionen

Zivilgesellschaft (Stiftung Neue Verantwortung): Resilienz und Vertrauen sind effektiver als offensive Fähigkeiten.

Sie haben keine empirischen Belege dafür, dass Abschreckung (Androhung der Vergeltung) im Cyberraum wirken kann. Sie haben aber empirische Belege dafür, dass Abschreckung durch eigene Sicherheits- und Resilienzmaßnahmen wirken kann, weil Angreifer*innen es schwer haben und angegriffene Systeme schnell wiederhergestellt werden können (Odysso, 2020; 4:10-4:36). Der Cyberraum wird untrennbar für zivile und militärische Aktivitäten genutzt, darum müssen in der Cyberverteidigungspolitik alle relevanten Politikbereiche einbezogen werden. Die Bundesregierung muss eine konkrete Strategie entwickeln, die Richtlinien im Weißbuch präzisieren (der aktuelle Leitfaden für die deutsche Sicherheitspolitik). Das Weißbuch betont die defensive Cyberabwehr, während in der Praxis v.a. die Offensive gefördert wird. Solche Inkohärenzen darf es nicht geben, denn wir brauchen Vertrauen und anerkannte Verhaltensnormen im Cyberraum, um Eskalation und Konflikte zu verringern. Gemeinsam mit der EU soll eine Cybersicherheitsstrategie entwickelt werden (Schuetze, 2021; S. 1ff).

*Hacker*innen (Forum Informatiker*innen für Frieden und zivilgesellschaftliche Verantwortung): Pflicht zur Offenlegung und Legalität von Protest.*

Forderung nach einer Digitalen Genfer Konvention, gemäß derer kritische Infrastruktur (=für die Zivilbevölkerung lebenswichtig, z.B. Strom-, Wasser-, Gesundheitsversorgung etc.) nicht angegriffen werden darf. Staaten sollen sich zu einer rein defensiven Sicherheitsstrategie verpflichten. Wirtschaftliche Interessen wie ein Verstoß gegen Intellectual Properties sind kein legitimer Kriegsgrund. Staatliche Stellen, Unternehmen und Bürger*innen müssen zur Offenlegung von Schwachstellen verpflichtet werden. Onlineprotestformen dürfen nicht kriminalisiert werden (Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, 2017).

Hacker suchen häufig nach Sicherheitslücken in IT-Infrastruktur. Das ist in Deutschland strafbar, wenn es keinen Auftrag von dem entsprechenden Unternehmen gibt. Das Hackertoolverbot führt dazu, dass deutsche Software weniger geprüft wird und Sicherheitslücken seltener repariert werden. Hacker*innen fordern, dass dieses Verbot geändert wird (Wilde et al.).

Regierung und parlamentarische Kontrolle: Ressortübergreifend und Verfassungskonform.

Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte. (Deutscher Bundestag, 2018, S. 3).

Weißbuch 2016: Das Bundesministerium des Innern, für Bau und Heimat (BMI) ist dafür zuständig, eine Cybersicherheitsstrategie zu erarbeiten (Bundesministerium des Innern, 2016).

Das Verteidigungsministerium (BMVg) und die Bundeswehr sind für die Verteidigungsaspekte zuständig. Die Gesamtverantwortung für die internationale Cybersicherheitspolitik liegt beim Auswärtigen Amt (die Bundesregierung, 2016; S. 38).

Verteidigungsministerium und Bundeswehr: Offensive Abschreckung und Pragmatismus.

Wir brauchen eine leistungsfähige, gesamtstaatliche Cyber-Sicherheitsarchitektur für mehr Systemresilienz, v.a. um die kritischen Infrastrukturen zu schützen. Defensive Maßnahmen alleine

reichen nicht aus. Offensive Fähigkeiten können zur Gewährleistung der Cybersicherheit beitragen und sind notwendig für den Erhalt der militärischen Handlungsfähigkeit. Ist die parlamentarische Kontrolle noch zeitgemäß? (Koch, 2021).

Kirchen (EKD): Cyberrecht im Völkerrecht und Vorrang für Zivil.

EKD-Synodenkundgebung 2019: Militärische Cyberkommandos sind an rechtsstaatliche Verfahren zu binden, ihre Kontrolle ist durch die staatlichen Organe und ihre Verbindung mit nichtmilitärischen Einrichtungen der Aufklärung und Gefahrenabwehr zu sichern und zu stärken. Wir sprechen uns dafür aus, bei der Cyber-Abwehr vor allem zivile Strukturen und defensive Maßnahmen zu stärken. Wir sehen die Notwendigkeit, ein völkerrechtlich verbindendes Cyberrecht zu entwickeln und einzuführen (Evangelische Kirche in Deutschland, 2019, S. 6).

Leichte Sprache

Grundlagen zur Einführung in das Thema

Cyber-War ist Englisch und bedeutet Krieg im Internet. Das Ziel von Cyber-War ist: auf elektronischem Weg Ländern Schaden zufügen. Digitale Technologie wird immer wichtiger in unserem Leben.

Diese digitale Technologie wird angegriffen, damit sie nicht mehr funktioniert.

Davor haben viele Menschen Angst. Die Technologien sind neu. Darum wissen viele Menschen nicht, was passieren kann.

Es gibt 3 Gefahren:

1. Software sagt dem Computer, was er machen muss, wenn ein Mensch eine Taste drückt. Ein anderes Wort ist: Computer-Programm. Oder: App. Software hat eine virtuelle Mauer, um sich vor Angriffen zu schützen.

   Manchmal gibt es Löcher in der Mauer. Diese Löcher heißen Sicherheits-Lücken.

   Manche Menschen suchen die Sicherheitslücken. Diese Menschen heißen Hacker. Manche Hacker wollen etwas kaputt machen oder Informationen klauen. Oft arbeiten sie im Auftrag von einem Land oder sind Kriminelle. Das passiert sehr oft.

   Diese Sicherheits-Lücken machen Angriffe und Cyber-War möglich.

   Das nennt man: un-sichere Infra-Struktur.

2. Hacker können durch die Sicherheits-Lücken in einer Software die ganze Software kaputt machen

   oder alle Informationen klauen. Zum Beispiel: persönliche Konto-Daten. Oder Geheimnisse aus der Regierung. Oder die Strom-Versorgung in einem Krankenhaus.

   Das nennt man: komplette Infiltration. Das passiert selten.

   Aber es ist eine große Bedrohung. Denn wir wissen: das ist möglich.

   Manchmal droht ein Land einem anderen Land damit. Um seinen Willen zu bekommen.

3. Elektronische Angriffe, Tote und Verletzte. Zum Beispiel: ein Land macht über das Internet die Strom-Versorgung in Deutschland kaputt. Dann funktioniert nichts mehr. Chaos entsteht. Die Krankenhäuser können nicht mehr richtig arbeiten. Deutschland wirft Bomben auf das andere Land, damit sie aufhören.

> Das nennt man: aktiver Cyber-Krieg. Viele Menschen reden darüber. Aber das passiert wahrscheinlich nicht.

Viele Angriffe im Internet sind klein und machen wenig kaputt. Zum Beispiel: Spionage oder Be-Einflussung von Wahlen.

Manchmal machen Angriffe sehr viel kaputt. Auch im Internet. Zum Beispiel: viele Menschen sind verletzt. Oder tot. Oder wichtige Sachen sind kaputt. Das ist verboten. Viele Staaten haben das zusammen gesagt.

Dann darf der Staat sich wehren.

Die Bundes-Wehr macht oft Angriffe. Aber der Bundes-Tag, also das Parlament, muss erst ja sagen.

Das Problem ist: die Bundes-Wehr muss die Angriffe schnell machen. Sie kann den Bundes-Tag nicht fragen.

Die deutsche Armee, also die Bundes-Wehr, sucht über das Internet nach geheimen Informationen in anderen Staaten. Das passiert immer öfter. Oft verändern sie dabei etwas in den Programmen von dem anderen Staat.

Aber eigentlich sagt das Grund-Gesetz: niemand darf den Frieden zwischen Staaten kaputt machen. Auch nicht im Internet.

Vielleicht ist der andere Staat dann wütend und macht etwas bei dem Anderen kaputt. Und ihr Streit wird immer größer. Das nennt man: Eskalation. Vielleicht gibt es sogar Krieg.

Viele Länder auf der Welt haben gesagt: wir wollen keinen Krieg. Die Länder sollen auch sagen: wir wollen keinen Krieg im Internet. Wir wollen Vertrauen haben zu anderen Staaten. Darum wollen wir nur Technologien bauen für Verteidigung. Nicht für Angriffe.

Leider bauen heute viele Staaten Technologien für Angriffe. Das ist der Regierung wichtig. Es gibt wenige Menschen die das bauen können. Darum werden wenig Technologien für Verteidigung gebaut.

Vertiefung: Problematiken im Themenfeld, Beispiel dual-use-Problematik

Digitale Technologie wird immer wichtiger in unserem Leben.

Oft kann die gleiche Technologie für militärische und nicht-militärische Zwecke benutzt werden. Das sind Dual-Use-Technologien.

Zum Beispiel: Die Firma FinFisher verkauft Software an Deutschland. Die Software kann manchmal Terroristen über das Internet finden. Die Firma FinFisher verkauft die gleiche Software auch an andere Länder.

In dem Land Bahrain bestraft die Regierung Menschen, die eine andere Meinung haben. Dafür hat die Regierung die Software von FinFisher gekauft. Dann wird die Software benutzt, um Menschen zu bestrafen. Eigentlich hatte die Software einen guten Zweck.

Darum prüft der Zoll jedes Mal, ob eine Dual-Use-Technologie an andere Länder verkauft werden darf oder nicht.

Leider entscheidet der Zoll oft falsch. Dann kann die Technologie trotzdem für schlechte Dinge benutzt werden. Friedens-Organisationen fordern: der Zoll muss die Exporte strenger prüfen. Ein Export darf nur erlaubt werden, wenn er keine Menschen-Rechte gefährdet. Wenn der Export trotzdem erlaubt wird, nur damit Deutschland mehr Geld verdient, dann ist das schlecht.

Fishbowl- oder Podiumsdiskussion: Akteur*innen und ihre Positionen

Zivilgesellschaft (Stiftung Neue Verantwortung):

Angriffe im Internet sollen anderen Staaten Angst machen. Damit sie uns nicht angreifen. Wir haben gesehen: das klappt nicht. Es gibt die andere Möglichkeit: verteidigen. Dafür müssen viele Menschen aufpassen: dass es kein Loch in der Schutz-Mauer gibt. Sie müssen die Mauer reparieren. Dann können Angreifer nicht durch die Mauer kommen.

Das Internet wird für Militär genutzt und für das normale Leben genutzt. Darum müssen verschiedene Ministerien zusammen entscheiden, was sie als nächstes machen.

Die Regierung muss konkret alles aufschreiben. Die Regierung muss dann das tun was sie aufschreibt. Das hilft: damit die Staaten sich vertrauen. Damit ein Streit nicht eskaliert, also immer größer wird. Deutschland soll mit der Europäischen Union reden.

Hacker:

Hacker fordern:

- die Staaten müssen Regeln machen für den Krieg im Internet. Es soll drin stehen: lebens-wichtige Sachen dürfen nicht angegriffen werden. Das nennt man: kritische Infra-Struktur. Zum Beispiel: Kranken-Häuser.

- Staaten dürfen im Internet nur Abwehr planen und machen. Keine Angriffe.

- man darf keinen Krieg um Geld führen

- Manchmal finden Geheim-Dienste Löcher in der Sicherheits-Mauer. Manchmal verraten sie das nicht. Weil: durch die Löcher können sie spionieren. Hacker fordern: der Finder muss Löcher immer verraten. Damit sie repariert werden können.

- Protestieren kann man auf der Straße und auch im Internet. Das muss immer erlaubt sein, auch im Internet.

- Hacker suchen Sicherheits-Löcher. In Deutschland müssen sie aufpassen. Oft verstoßen sie dabei gegen das Gesetz. Darum arbeiten Hacker im Ausland. Die Wirkung: deutsche Programme werden weniger geprüft und repariert. Sie sind weniger sicher. Hacker fordern: das Gesetz muss geändert werden.

Regierung und Parlament:

Die deutsche Armee, also die Bundes-Wehr, muss das Parlament, also den Bundes-Tag, um Erlaubnis fragen: dürfen wir einen anderen Staat angreifen? Die Bundes-Wehr muss auch fragen, wenn sie einen Angriff im Internet machen will.

Das Internet ist für Alle wichtig: im Krieg und im zivilen Leben. Darum müssen Alle zusammen arbeiten für Sicherheit im Internet.

- Das Innen-Ministerium soll überlegen und arbeiten: wie kann sich Deutschland schützen vor Angriffen aus dem Internet? Was machen wir, wenn wir angegriffen werden?

- Das Verteidigungs-Ministerium und die Bundes-Wehr sollen eine militärische Strategie entwickeln.

- Das Außen-Ministerium soll an der welt-weiten Politik für Sicherheit im Internet arbeiten.

Verteidigungsministerium und Bundeswehr:

Wir müssen zusammen-arbeiten. Wir brauchen eine gemein-same Strategie: wie wir Angriffe abwehren. Wie wir mit neuen Situationen umgehen. Und wann wir andere Staaten angreifen. Wir brauchen mehr Geld.

Wir müssen die kritische Infra-Struktur, also die lebens-wichtigen Sachen, beschützen.

Abwehr reicht nicht. Wir müssen auch angreifen können. Damit andere Länder Angst haben. Damit andere Länder uns nicht angreifen. Und damit wir uns wehren können, wenn uns ein anderes Land angreift.

Kirchen (Evangelische Kirche in Deutschland):

Das Parlament der evangelischen Kirche hat 2019 gesagt:

Die Bundeswehr arbeitet im Internet. Dafür muss sie die Gesetze befolgen. Zum Beispiel: sie muss das Parlament, also den Bundestag, fragen. Wir brauchen auch neue Gesetze für die Kontrolle. Wir brauchen auch zivile, also nicht-militärische Experten, die zivil sind, also die nicht bei der Bundes-Wehr sind. Deutschland soll mehr Geld geben für zivile Experten. Und mehr für Abwehr. Deutschland soll weniger Geld geben für die Bundes-Wehr. Und weniger für Angriffe.

Wir brauchen ein Völker-Recht für das Internet. Das heißt: wir brauchen Regeln für den Krieg im Internet.