Verfassungs- und völkerrechtliche Fragen im militärischen Cyber- und Informationsraum unter besonderer Berücksichtigung des Parlamentsvorbehalts, der Zurechenbarkeit von Cyberangriffen sowie einer möglichen Anpassung nationaler und internationaler Normen

Deutscher Bundestag
Verteidigungsausschuss

Ausschussdrucksache
19(12)950
11.12.2020 - 19/3517
5410

Stellungnahme zur öffentlichen Anhörung im Verteidigungsausschuss am 14. Dezember 2020

PD Dr. Dr. habil. Robert Koch

Robert.Koch@UniBw.de

Vorbemerkung

Die vorliegende Stellungnahme ist keine offizielle Position des Bundesministeriums der Verteidigung, sondern die Sichtweise des Autors vor dem Hintergrund seiner wissenschaftlichen und fachlichen Expertise. Der Autor ist kein Jurist oder Völkerrechtler, sondern promovierter und habilitierter Informatiker mit fachlichem Schwerpunkt IT- und Cybersicherheit. Entsprechend werden nicht alle Fragestellungen des Fragenkatalogs adressiert, sondern es erfolgt insbesondere eine technische Analyse und Bewertung.

Ausgangslage

Chancen und Risiken des Cyber- und Informationsraums Staat, Wirtschaft und Gesellschaft stehen in einer weiter zunehmend digitalisierten und vernetzten Welt wachsenden Herausforderungen im Cyber- und Informationsraum gegenüber. Während die Digitalisierung zahlreiche Chancen bietet, generiert sie aufgrund der dahinterliegenden Daten, Werte und Einflussmöglichkeiten in Verbindung mit den charakteristischen Eigenschaften des Cyber- und Informationsraums wie einer hohen Wirkasymmetrie, herausfordernder Attribuierung und globaler Konnektionsfähigkeit in Nahe-Echtzeit ein lukratives Ziel für Angreifer, von Script Kiddies über Hacktivisten und private Organisationen, der Organisierten Kriminalität (OK), bis hin zu staatlichen Akteuren. Das Spektrum der Angriffe kann dabei von einem Defacement von öffentlichen Webauftritten, einer Diensteverhinderung, bspw. durch eine Systemüberlastung mittels einer DDoS-Attacke[1] oder der erpresserischen Verschlüsselung von Systemen, der Exfiltration oder Manipulation von Daten bis hin zur physikalischen Zerstörung von Infrastruktur gehen.

Notwendigkeit und Grenzen von resilienten Systemen Die zunehmende Professionalisierung von Cyberangriffen und die steigende Anzahl von Akteuren erfordern daher die Sicherstellung der staatlichen Handlungsfähigkeit. Um die Risiken im Cyber- und Informationsraum auf ein tragbares Maß zu reduzieren, ist insbesondere eine effektive Zusammenarbeit im gesamtstaatlichen Ansatz und eine leistungsfähige, gesamtstaatliche Cyber-Sicherheitsarchitektur sowie die Erhöhung der Systemresilienz insbesondere auch im Bereich der Kritischen Infrastrukturen (KRITIS) erforderlich. Da hochwertige Angriffsvektoren jedoch insbesondere auch bei hochsicheren und eigentlich resilient konzipierten System vorhanden sein können, ist durch defensive Maßnahmen alleine kein ausreichendes Sicherheitsniveau zu generieren. Das Vorhalten offensiver Fähigkeiten ist daher zwingend zur Gewährleistung der Cybersicherheit als auch der militärischen Handlungsfähigkeit.

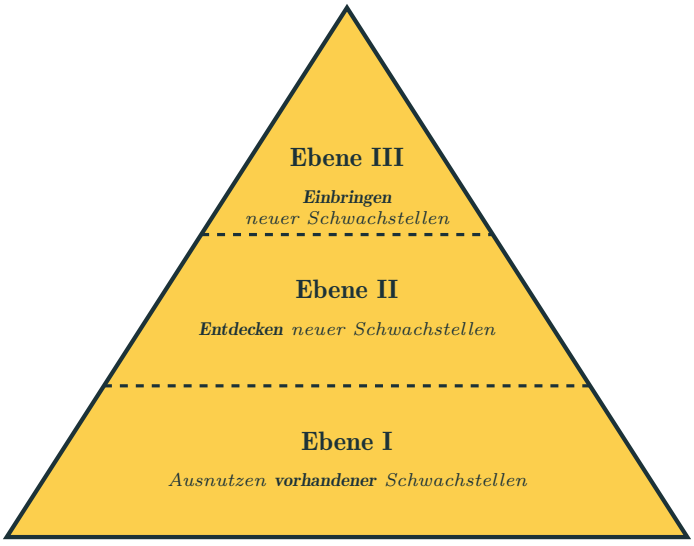
[1] Distributed Denial of Service

Was sind die Möglichkeiten und Grenzen von Cyberoperationen?

Für eine Diskussion der Möglichkeiten und Grenzen von Cyberoperationen kann die Fragestellung, welche Effekte auf welcher Basis generiert werden können, als Ausgangspunkt genutzt werden. Effekte können insbesondere in den Kategorien „Diensteverhinderung“ und „Daten“ generiert werden. Diensteverhinderung kann sowohl temporärer als auch permanenter Natur sein und direkt auf verschiedenen Ebenen, von Applikationen bis zur Hardware, oder indirekt bspw. durch die Störung von Kommunikationskanälen, erfolgen. Bzgl. Daten können insbesondere Aufklärung, Manipulation oder Zerstörung avisiert werden.

Herausforderungen der Cybersicherheit Um entsprechende Effekte zu erzielen, stehen eine Vielzahl von potentiellen Vektoren zur Verfügung; die weitverbreitete Ausnutzung von Schwachstellen in Software stellt hierbei nur einen kleinen Teilbereich dar. Vielmehr ist es daher erforderlich, eine holistische Betrachtung der Angriffsvektoren vorzunehmen; hier spiegelt sich insbesondere auch der Unterschied zwischen IT-Sicherheit und Cybersicherheit wider: Während IT-Sicherheit den „Zustand [beschreibt], in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind“[2], wird bei Cybersicherheit das Aktionsfeld der Informationssicherheit auf den gesamten Cyberraum ausgeweitet[3]. Cybersicherheit überschreitet daher insbesondere die Grenzen der eigenen Firma und beinhaltet Aspekte wie Stromversorgung, Telekommunikation und Versorgungsketten, welche regelmäßig *nicht* unter eigener Kontrolle stehen.

Um die unterschiedlichen Fähigkeiten und Möglichkeiten verschiedener Interessensgruppen, staatlicher als auch nichtstaatlicher Organisationen und Institutionen sowie von Streitkräften verstehen und einordnen zu können, bietet sich die Nutzung eines Bedrohungsmodells mit drei grundsätzlichen Ebenen an[4]:



Dreistufiges Bedrohungsmodell zu Schwachstellen im Cyberraum.

[2] Vgl. Definition „IT-Sicherheit“ im Glossar der Cyber-Sicherheit des BSI.
[3] Vgl. Definition „Cyber-Sicherheit“, ebd.
[4] Vgl. DSB Task Force Report, „Resilient Military Systems and the Advanced Cyber Threat“, 2012.

Ausnutzen vorhandener Schwachstellen In der unteren Ebene werden Bedrohungen eingeordnet, welche bereits öffentlich bekannte Schwachstellen ausnutzen. Solche finden sich bspw. in der CVE-Datenbank der MITRE Corporation[5], während andere Datenbanken wie bspw. die Exploit Database von Offensive Security[6] öffentlich verfügbare Exploits und fehlerhafte Programme sammeln und archivieren. Aufgrund der öffentlichen Verfügbarkeit der Informationen sollte gegen Angriffe dieser Ebene prinzipiell ein guter Schutz etablierbar sein. In der Praxis stößt dies aber aus einer Vielzahl von Gründen immer wieder an Grenzen. Ursachen können mangelhafte oder gar ausbleibende Bereitstellungen von Patches für fehlerhafte Produkte durch die betroffenen Unternehmen bis hin zur per se fehlenden Möglichkeit des Patchens eines Systems sein. Letzteres kann bspw. durch nicht ausreichende Systemressourcen bedingt sein, zum Beispiel bei IoT-Geräten[7], durch das Supportende eines Produkts oder gar, weil die entsprechende Herstellerfirma nicht mehr existiert. Gerade IT-Systeme in KRITIS und Steuerungsanlagen können hiervon betroffen sein, da dort regelmäßig eine besonders lange Nutzungsdauer vorliegt.

Die erhebliche Alltagsrelevanz dieser Ebene zeigt sich in der Praxis durch Vorfälle wie im Rahmen der Ransomware „WannaCry“, welche im Mai 2017 zahlreiche Systeme weltweit, insbesondere auch im Bereich der KRITIS und von Industrieanlagen, infizierte. Die ausgenutzte Schwachstelle war bereits bekannt und Patche verfügbar, betroffen waren aber insbesondere Systeme, welche vom Hersteller Microsoft nicht mehr unterstützt wurden, bspw. Windows XP und Server 2008[8].

Entdecken neuer Schwachstellen Auf der mittleren Ebene des Bedrohungsmodells finden sich Angriffe, welche auf Basis neu entdeckter und öffentlich noch unbekannter Schwachstellen, sog. Zero-Days (0days) ausgeführt werden. Zum Auffinden von 0day-Schwachstellen ist typischerweise ein entsprechend höherer Ressourcenaufwand erforderlich, insbesondere bzgl. Fachwissen, Systemkenntnis und Programmiererfahrung. Allerdings werden in den letzten Jahren neue Schwachstellen zunehmend durch automatisierte Softwaretests, bspw. Fuzzing, gefunden[9]. Hierbei werden die Fuzzingtechnologien stetig weiterentwickelt und u.a. auch mit Machine Learning Verfahren kombiniert. Beachtet werden muss hierbei, dass Wert und Nutzen einer 0day-Schwachstelle für eine Cyberoperation sehr unterschiedlich sein kann, da die Effekte von einfacher Diensteverhinderung bis hin zu entfernter Codeausführung mit administrativen Rechten[10] reichen können. Dies spiegelt sich bspw. in der Bewertung von Schwachstellen im Common Vulnerability Scoring System (CVSS)[11] wider. Stuxnet[12], der Angriff auf die iranische Urananreicherungsanalage in Natanz, ist von programmiertechnischer Perspektive dieser Ebene zuzurechnen.

[5] Common Vulnerabilities and Exposures, The MITRE Corporation
[6] The Exploit Database
[7] Internet-of-Things
[8] Die Gruppe „The Shadow Brokers“ veröffentlichte die der NSA zugerechnete Schwachstelle ETERNALBLUE am 14. April 2017, die Schadsoftware WannaCry verschlüsselte vom 12. bis 15. Mai 2017 zahlreiche Systeme weltweit. Ein Patch (MS17-010) wurde bereits im März 2017 herausgegeben, allerdings ursprünglich nicht für die von Microsoft nicht mehr unterstützten Betriebssysteme.
[9] Vgl. bspw. Fuzzing ImageIO oder 5 CVEs found with Feedback-based Fuzzing.
[10] Remote Code Execution with Privilege Escalation
[11] Vgl. FIRST CVSS-SIG
[12] Operation „Olympic Games“

Schwachstellen dieser Ebene müssen aber nicht zwangsläufig die Soft- oder Firmware betreffen, sondern können auch in Hardware vorliegen. Die Schwachstellen Spectre[13] und Meltdown[14], welche unbefugt Speicherbereiche in modernen Prozessoren auslesen konnten, sind prominente Beispiele in diesem Bereich.

Einbringen neuer Schwachstellen Bedrohungen der oberen Ebene zeichnen Schwachstellen aus, welche *bewusst* in ein (typischerweise sicherheitsrelevantes) System eingeführt werden. Diese sind so angelegt, dass sie möglichst unauffällig sind und die originale Funktionsweise nicht beeinflussen. Neben einer Abbildung in Software, Firmware oder Hardware, können entsprechende Angriffsvektoren auch in mathematischen Verfahren (Algorithmik oder Zahlen) versteckt werden. Im Falle der Einbringung einer entsprechenden Schwachstelle in Hardware kann eine Aktivierung bzw. Ausnutzung entweder von außen in Form einer Hintertür (Backdoor) erfolgen, oder autark durch die Aktivierung bei bestimmten System- oder Umgebungsparametern[15]. Daraus ergibt sich eine sehr schwierige und ggf. nicht mögliche Detektierbarkeit, bei derzeit in der Praxis sehr eingeschränkten und oftmals nicht zerstörungsfreien Untersuchungsverfahren.

Aufgrund der hohen Komplexität und internationalen Verzweigung der Versorgungsketten mit einer Vielzahl von beteiligten Akteuren in unterschiedlichsten Ländern[16], gerade auch bei IT-Produkten, steigt das Risiko entsprechender Manipulationen in allen Bereichen, von der Design- bis zur Auslieferungsphase, erheblich an. Weiterhin ergibt sich, insbesondere bei geeigneter Ausführung im Rahmen von Hardwaremanipulationen, ein hoher Grad an Abstreitbarkeit[17]. Beispiele hierfür sind die Diskussion aus dem Jahre 2012 um das Vorhandensein einer Hardware-Hintertür in einem auch in verschiedenen militärischen Anwendungen eingesetzten Mikrochip[18] oder der Bloomberg Businessweek-Artikel „The Big Hack“[19]. Auch wenn es stark umstritten ist, ob eine wie im Bloomberg-Artikel dargestellte Manipulation tatsächlich stattgefunden hat, ist die technische Realisierbarkeit gegeben[20]. Auch im Bereich der Algorithmik liegen öffentlich bekannte Beispiele hochwertiger Manipulationen vor[21].

Im Rahmen der Snowden-Dokumente[22] wurden weiterhin die sog. „Interdiction Operations“ der NSA bekannt, bei denen bspw. Hardwareimplantate zur Bereitstellung von mit konventionellen Sicherheitslösungen nicht detektierbaren, persistenten Hintertüren während des Versandwegs eingebracht wurden[23]. Beachtet werden muss, dass die Hürde für Angreifer zur Durchführung entsprechender Manipulationen stetig sinkt, bspw. sind bereits Kurse zur Herstellung von Hardware-Implantaten verfügbar[24], die einem versierten Hacker das notwendige Wissen als auch die praktischen Fähigkeiten vermitteln.

[13] CVE 2017-5753, CVE 2017-5715
[14] CVE 2017-5754
[15] Auch als „Killswitch“ bezeichnet.
[16] Vgl. bspw. John Adams und Paulette Kurzer, „Remaking American Security: Supply Chain Vulnerabilities and National Security Risks Across the US Defense Industrial Base“, Alliance for American Manufacturing, 2013.
[17] Vgl. das Konzept der glaubhaften Abstreitbarkeit (Plausible Deniability).
[18] Actel/Microsemi ProASIC3 FPGA, vgl. Sergei Skorobogatov und Christopher Woods, „Breakthrough Silicon Scanning Discovers Backdoor in Military Chip“, LNCS Volume 7428, Springer, 2012.
[19] Vgl. The Big Hack How China Used a Tiny Chip to Infiltrate U.S. Companies
[20] Vgl. bspw. Analyse durch die Security Group des Computer Laboratory der University of Cambridge.
[21] Vgl. bspw. die Beeinflussung und Standardisierung der Dual-EC durch die NSA. Daniel J. Bernstein, „Dual EC: A Standardized Back Door, Springer LNCS Volume 9100, 2016.
[22] Vgl. bspw. Spiegel Netzwelt, Die NSA rüstet zum Cyber-Feldzug.
[23] Vgl. bspw. GODSURGE-Tool und FLUXBABBITT Hardware-Implant für DELL Power Edge 1950 und 2950 Server, welches über das JTAG Debugging-Interface auf das Zielsystem zugreift.
[24] Vgl. bspw. SecuringHardware.com

In der Praxis kann die Detektion entsprechend hochwertiger Angriffe auf bspw. Versorgungsketten äußerst komplex und nahezu unmöglich sein; insbesondere ist regelmäßig keine, auch nur annähernd lückenlose Kontrolle möglich. Entsprechend greift die SWP-Studie „Militärische Cyber-Operationen“[25] durch die Fokussierung auf 0day-Schwachstellen deutlich zu kurz.

Die Nutzung unbekannter 0day-Schwachstellen ist, im Gegensatz zur Folgerung der Studie, lediglich im mittleren Bedrohungsniveau einzuordnen, während die „Königsdisziplin“ die *bewusste Einbringung* von Schwachstellen darstellt. Auch ist der Rahmen möglicher Akteure weiter zu spannen. So ist die Suche nach 0days durch die bereits erwähnten Fuzzingtechnologien zunehmend einfach, weiterhin ist der Erwerb von 0day-Exploits für alle verbreiteten Zielsysteme und Effektebenen durch Firmen wie bspw. ZERODIUM[26] sehr leicht möglich, auch ohne eigene Kapazitäten für die Suche zu haben. Dass auch kleine Nationen 0day-Exploits im staatlichen Rahmen nutzen, hat bspw. die Entdeckung von mehreren durch den usbekischen Geheimdienst genutzten 0days unterstrichen[27].
Auch wenn es bisher, zumindest öffentlich bekannt, noch zu keinem „Cyber-9/11“ gekommen ist, darf die diesbzgl. vorhandene Gefährdung nicht unterschätzt werden[28]. Ein Blick auf bekannt gewordene Sicherheitsvorfälle zeigt[29], wie insbesondere auch gegen KRITIS zunehmend Cyberangriffe zu registrieren sind. Bekannt geworden sind u.a. Angriffe gegen Stromnetze, Wasserversorgungen und Verkehrsleitsysteme. Insbesondere gilt es zu beachten, dass entsprechende Aktionen oftmals nicht darauf angelegt sind, direkt Effekte zu generieren, sondern vielmehr die Vorbereitung für einen späteren Zugriff sind[30].

Was sind die Besonderheiten, Vor- und Nachteile von Cyberwirkmitteln?

Um eine Analyse der Möglichkeiten, Vor- und Nachteile von Cyberwirkmitteln zu eröffnen, ist insbesondere eine geeignete Terminologie erforderlich. Während oftmals von „Cyberwaffen“ gesprochen wird, ist die Nutzung dieser Begrifflichkeit nicht zielführend. Vielmehr gilt es, eine grundlegende Unterscheidung zwischen *Schadsoftware* und *Cyberwirkmitteln* vorzunehmen, um die Charakteristika und Einsatzmöglichkeiten zu beleuchten. Cyberwirkmittel sind, im Gegensatz zu Schadsoftware, regelmäßig auf konkrete Ziele zugeschnitten und präzise. Weiterhin sind Cyberwirkmittel in der Regel nicht letal und reversibel.

Vorteile von Cyberwirkmitteln Cyberwirkmittel können auf konkrete Ziele, bspw. eine militärisch relevante Komponente in einem Stromnetz, zugeschnitten werden. Dabei können im Unterschied zu anderen Wirkmöglichkeiten insbesondere temporäre, reversible Effekte generiert werden, was bei einer Erbringung in einer anderen Dimension, bspw. bei einer Zielbekämpfung mit Luft-Boden-Raketen, typischerweise nicht möglich ist. Der Wurm Stuxnet hat demonstriert, dass ein zielgerichteter Angriff auf ein spezifisches System möglich ist. Auch wenn im Verlauf der Operation eine weitere Verbreitung des Wurms in

[25] Matthias Schulze, Militärische Cyber-Operationen. Nutzen, Limitierungen und Lehren für Deutschland, SWP-Studie 2020/S, 2020.
[26] Vgl. ZERODIUM
[27] Vgl. l+f: Die freigiebige Zero-Day-Spender-Box
[28] Vgl. bspw. Thomas M. Chen, „Cyberterrorism after Stuxnet“, Strategic Studies Institute U.S. Army War College, 2014.
[29] Vgl. bspw. Center for Strategic and International Studies (CSIS), Significant Cyber Incidents.
[30] „Preparation of the Battlefield“, vgl. bspw. Robert Koch und Mario Golling, „The Cyber Decade: Cyber Defence at a X-ing Point“, 10th International Conference on Cyber Conflict (CyCon), IEEE, 2018.

Systemen weltweit erfolgt ist, kam es durch das extakte Zuschneiden von Stuxnet auf das Zielsystem, die iranische Urananreicherungsanlage in Natanz, zu keinem dokumentierten, unbeabsichtigen ähnlichen Effekt. Im Gegenteil, die Verbreitung hat demonstriert, dass weder eine unbeabsichtigte Zerstörung eines Nicht-Ziels durch das Cyberwirkmittel erfolgt ist, ein Kollateralschaden also vermieden werden konnte, weiterhin hatte sich die nach Bekanntwerden der Verbreitung des Wurms in der Presse diskutierte Befürchtung, Cyberterroristen könnten auf Basis des Wurmcodes Angriffe gegen Systeme der KRITIS fahren[31], auch bis jetzt nicht bestätigt. Dies liegt auch an den für die Entwicklung des Cyberwirkmittels erforderlichen Informationen über Zielsysteme wie die Zentrifugensteuerung der Anlage in Natanz, welche typischerweise nicht über den Cyberraum generiert werden können. Dadurch kann aber nicht ausgeschlossen werden, dass es zukünftig nicht zu solchen terroristischen Angriffen kommen kann.

Cyberwirkmittel können Effekte rein auf IT-Systeme beschränkt, aber auch physische Auswirkungen generieren. Auch wenn der tatsächlich genutzte Angriffsvektor im Rahmen der Operation „Outside the Box“[32] der Israelischen Luftwaffe gegen einen im Bau befindlichen, syrischen Reaktor am 5. und 6. September 2007 nicht mit letzter Sicherheit bestimmt werden kann[33], ist Tatsache, dass die syrischen Radaranlagen die israelischen F-15I und F-16I nicht detektieren bzw. darstellen konnten. Wahrscheinlich ist ein Angriff im elektromagnetischen Spektrum, welcher ein falsches Bild der Luftlage in die syrischen Systeme eingespielt hat[34], ggf. auch die Ausnutzung einer Hintertür in den syrischen Radarsystemen[35]. Gerade die Komplexität militärischer Systeme und deren Abhängigkeit von IT eröffnet hier zahlreiche Handlungsoptionen und macht den Schutz eigener System sehr herausfordernd[36]. Der Wurm Stuxnet wiederum hat gezeigt, wie physische Auswirkungen durch Cyberwirkmittel generiert werden können.

Nachteile von Cyberwirkmitteln Nachteil eines Cyberwirkmittels können der Pflegeaufwand sein, wenn bspw. zu nutzende Schwachstellen aktualisiert werden müssen. Dabei muss jedoch berücksichtigt werden, dass auch im konventionellen Vergleich entsprechende Aufwände vorhanden sind. So sind bei seegehenden Einheiten bspw. entsprechend regelmäßig Konservierungsmaßnahmen zur Erhaltung der vollen Funktionsfähigkeit des Materials erforderlich, wie zum Beispiel die Erneuerung des Anstrichs insbesondere auch im Unterwasserbereich. Die Pflege eines Cyberwirkmittels differiert in der Praxis daher nicht zu sehr von den Notwendigkeiten klassischer Systeme, wenn diese auch in anderer, mitunter aber sogar einfacher durchzuführender Form, erbracht werden muss.

Für das Zuschneiden auf ein Ziel ist weiterhin eine entsprechende Aufklärung im Vorfeld erforderlich, was sich somit aber nicht elementar von den klassischen Dimensionen unterscheidet. Für die zielgerichtete Nutzung eines Cyberwirkmittels ist jedoch eine entsprechende Vorbereitungszeit zur Entwicklung und Überprüfung des Wirkmittels erforderlich.

[31] Vgl. bspw. Thomas M. Chen, ebd.
[32] Auch bekannt unter dem Namen „Operation Orchard“. Eine öffentliche Stellungnahme und ein Bekennen zur Durchführung der Operation erfolgte durch die Israelischen Streitkräfte erstmals am 21. März 2018.
[33] Vgl. bspw. Sally Adee, „The Hunt for the Kill Switch, IEEE Spectrum, 2008.
[34] Vgl. bspw. David A. Fulghum et al., „Black Surprises“, Aviation Week and Space Technology.
[35] Vgl. bspw. Spies in the Middle East: Israeli Cyber Operations
[36] Vgl. bspw. Robert Koch und Mario Golling. „Weapons Systems and Cyber Security - A Challenging Union“, 8th International Conference on Cyber Conflict (CyCon), IEEE, 2016.

Weitere Charakteristika Cyberwirkmittel können ggf. „Einmalwaffen“ darstellen, da mit der Nutzung, insbesondere bei der Generierung physischer Effekte, eine entsprechende Detektionswahrscheinlichkeit verbunden ist, was folglich zu einer Schließung der ausgenutzten Schwachstelle oder zumindest einer entsprechenden Mitigation führen kann. Auch hier besteht jedoch kein elementarer Unterschied zu klassischen Waffensystemen, bspw. stellt der Einsatz eines Flugkörpers eine äquivalente Situation einer „Einmalwaffe“, bezogen auf das jeweilige Einzelexemplar, dar; bzgl. Entwicklung und Pflege kann das Cyberwirkmittel dabei aber ggf. günstiger sein. Vielmehr gilt, dass die tatsächliche Nutzungsdauer des Cyberwirkmittels in der Praxis insbesondere von der Art des ausgelösten Effekts, der regulären Entdeckungswahrscheinlichkeit der Schwachstelle[37] sowie der Geheimhaltungsfähigkeit der Operationsdurchführung abhängig ist. So lief der Cyberangriff mittels des Wurms Stuxnet für mindestens ein Jahr unentdeckt, *obwohl* die generierten Effekte physischer Natur waren[38].

Was sind die Möglichkeiten und Grenzen der Attribuierung und Beweisführung?

Aufgrund seiner Struktur bietet der Cyber- und Informationsraum versierten Angreifern hinreichende Möglichkeiten, ihre Identität zu verschleiern und anonym zu agieren. Eine Attribuierung von Angriffen kann für die Einschätzung der Sicherheitslage von hoher Bedeutung sein. Unterschieden werden kann die faktische Zuordnung, rechtliche Zurechnung sowie die politische Verantwortlichkeit[39]. Die faktische Attribuierung basiert auf einer technischen Analyse des Angriffs mit dem Ziel der Zuordnung zu einem IT-System und darauf aufbauend, weiter zu einem Angreifer. Die rechtliche Attribuierung dient der Feststellung der völkerrechtlichen Verantwortlichkeit eines Staates. Da beide, faktische wie rechtliche Attribuierung in der Praxis regelmäßig längere Zeit in Anspruch nehmen können, dient die politische Attribuierung als Grundlage für Maßnahmen, welche keiner rechtlichen Zurechnung bedürfen[40].

Anonymisierungsnetze Mit Blick auf die technische Analyse bieten sich einem Angreifer zahlreiche Möglichkeiten, die eigene Identität zu verschleiern. Neben dem Legen falscher Spuren bspw. durch Anmerkungen im Programmcode in einer bestimmten Sprache[41], um bspw. im Rahmen einer Analyse von Schadcode abzulenken, können insbesondere technische Verfahren zur Anonymisierung genutzt werden. Bspw. ermöglicht das Tor-Netz[42] eine Anonymisierung der IP-Adresse, so dass eine Rückverfolgung nicht beim eigentlichen Nutzer, sondern bei einem der Ausgangsknoten[43] des Tor-Netzes endet. Solche Ausgangsknoten werden weltweit zur Verfügung gestellt, in Deutschland bspw. durch den Chaos Computer

[37] Vgl. bspw. Lillian Ablon und Andy Bogart, „Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits“, RAND Corporation, 2017.
[38] Dies ist insbesondere darin begründet, dass die angegriffenen Zentrifugen des Typs IR-1 per se erhöhte Ausfallraten hatten und der Anstieg daher zunächst keinen Verdacht erweckt hat. Weiterhin hat Stuxnet zunächst Manipulationen in der Drucksteuerung vorgenommen, um das Anreicherungsprodukt unnutzbar zu machen; erst die spätere Version hat auf die Umdrehungsgeschwindigkeit der Zentrifugen eingewirkt und somit zur physischen Zerstörung geführt; vgl. bspw. Ralph Langner, „Stuxnet und die Folgen“, 2017.
[39] Vgl. bspw. Katharina Ziolkowski, „Attribution von Cyber-Angriffen“, GSZ Zeitschrift für das Gesamte Sicherheitsrecht, 2. Jahrgang, 2/2019.
[40] Vgl. ebd.
[41] Vgl. insb. das „Anti-Forensic Marble Framework“ der CIA zur Verschleierung und Förderung einer Fehlattribuierung.
[42] The Onion Router
[43] Tor Exit Nodes

Club[44]. Während Proxy-Ketten[45] lediglich die Rückverfolgung erschweren, grundsätzlich aber nur eine Pseudonymisierung liefern können, ermöglicht das Tor-Netz eine *echte* Anonymisierung. Hierbei muss jedoch beachtet werden, dass das Tor-Netz unter permanenter Beobachtung zahlreicher Behörden, Organisationen sowie der Forschung steht, welche bspw. auch Ausgangsknoten betreiben, den darüber laufenden Datenverkehr untersuchen und Sicherheitsanalysen des Netzes vornehmen.

De-Anonymisierung Grundsätzlich ist eine De-Anonymisierung aufgrund von Programmierfehlern der Tor-Software bzw. Designfehlern im Tor-Protokoll möglich, jedoch sehr selten[46]. Eher anzutreffen ist eine De-Anonymisierung auf Basis von Fehlern im Tor-Browser[47], welcher letztendlich ein für den Zugriff auf das Tor-Netz erweiterter und konfigurierter Firefox-Browser ist, oder auf entsprechende Browser-Plugins[48]. Die häufigste Ursache für De-Anonymisierung ist jedoch fehlerhaftes Nutzerverhalten, bspw. die Verwendung einer Email-Adresse sowohl mittels des Klarnetzes, als auch im Rahmen von Tor[49].

Die Kombination von wenn auch schwierigen De-Anonymisierungsmöglichkeiten[50], einer intensiven Überwachung des Tor-Netzes[51] sowie technischen Restriktionen durch die Architektur des Netzes selbst, schränken den Anwendungsbereich für hochwertige Angriffe in der Praxis ein[52]. Aufgrund dieser Restriktionen findet sich in der Praxis insbesondere auch die Nutzung von ungenügend gesicherten Routern zur Verschleierung der Herkunft, wie bspw. in geleakten Unterlagen des kanadischen CSEC[53] ersichtlich[54]. Der „Home Router Security Report“[55] des Fraunhofer FKIE[56] vom Juni 2020 zeigt die weiterhin sehr hohe Anfälligkeit des IT-Equipments in diesem Bereich und beschreibt ein hohes Gefährdungspotential.

Für die Attribuierung bedeutet diese herausfordernde Situation insbesondere, dass um die notwendige Höhe der Attribuierung zu erreichen und die dafür erforderliche Zeit zu minimieren, ein gesamtstaatlicher Ansatz, welcher die respektiven Informationen aller sicherheitsverantwortlichen Behörden zusammenführt, erforderlich ist. Hier kann bspw. das Cyber-AZ, welches die zentrale Kooperationsplattform aller entspechender Behörden ist[57], eine besondere Rolle einnehmen.

[44] Vgl. Anonymizer des Chaos Computer Club e.V.
[45] Leiten des Datenverkehrs über mehrere Proxy-Rechner im Internet, um die Rückverfolgung zu erschweren.
[46] Vgl. bspw. Tor security advisory: "relay early" traffic confirmation attack
[47] Defend yourself. Download-Seite des Tor-Browsers.
[48] Vgl. bspw. A look to the „NIT Forensic and Reverse Engineering Report, Continued from January 2015“. NIT code was used by the FBI to deanonymize Tor users.
[49] Vgl. bspw. Silk Road: How FBI closed in on suspect Ross Ulbricht
[50] Die NSA scheint daher bspw. den Weg zu präferieren, schon den Download des Tor-Browers oder der Anonymisierungs-Distribution TAILS mittels XKeyscore zu registrieren, vgl. bspw. Nutzer des Tor-Netzwerks Ziel der Spähattacken.
[51] Vgl. bspw. Robert Koch et al., „How anonymous is the tor network? A long-term black-box investigation“, Computer Volume 49 Issue 3, 2016.
[52] Vgl. bspw. Robert Koch, „Hidden in the Shadow: The Dark Web-A Growing Risk for Military Operations?“, 11th International Conference on Cyber Conflict (CyCon), IEEE, 2019.
[53] Communications Security Establishment Canada
[54] LANDMARK-Programm, Nutzung einer sog. Operational Relay Box (ORB) Infrastruktur für ein zusätzliches Level der Nicht-Attribuierbarkeit.
[55] Vgl. Home Router Security Report 2020
[56] Vgl. Fraunhofer FKIE
[57] Vgl. bspw. Das Nationale Cyber-Abwehrzentrum .

Was sind Maßnahmen zur Verbesserung des Schutzes eigener Systeme?

Schon der Schutz gegen Angriffsvektoren der unteren Ebene ist in der Praxis oftmals nur eingeschränkt möglich. Selbst bei Vorhandensein eines Patches kann sich die Installation herausfordernd darstellen, bspw. durch die Notwendigkeit der Rezertifizierung im Bereich der Luftfahrt und bei medizinischem Gerät, oder durch 24/7-Betrieb und seltene Wartungsfenster, bspw. im Bereich der Stromversorgung. In solchen Bereichen sind oftmals weiterhin harte Echtzeitanforderungen an die Kommunikationssysteme gestellt[58], welche durch einen Patch nicht negativ beeinflusst werden dürfen. Auch ist zu berücksichtigen, dass die Patchqualität nicht immer genügend ist, Schwachstellen nicht notwendigerweise vollständig geschlossen werden, Systemfunktionalitäten negativ beeinflusst oder gar neue Schwachstellen geöffnet werden können.

In solchen Fällen kann eine Mitigation durch andere Maßnahmen erforderlich werden, welche typischerweise Nachteile beinhalten. So kann sich die Einbringung einer zusätzlichen Firewall oder eines Systems zur Einbruchserkennung[59] mit Sperrregeln gegen maliziösen Verkehr negativ auf die Echtzeitfähigkeit des Netzes auswirken und auch durch die Einbringung von Schutzsystemen kann sich die Angriffsoberfläche erhöhen und im Extremfall somit in einer weiteren *Schwächung* des zu schützenden Systems resultieren. Bspw. hat Tavis Ormandy wiederholt demonstriert, wie Architektur- und Programmierfehler von Antivirensoftware bis zur entfernten Übernahme mit administrativen Rechten von eigentlich durch die Software zu schützenden Systemen führen können[60]. Die Nutzung nicht-intrusiver Verfahren wie bspw. eine Angriffserkennung auf Basis der Auswertung des Stromverbrauchs des Systems[61] kann insbesondere im Bereich KRITIS eine Möglichkeit zur Verbesserung des Schutzniveaus auch für Bestandssysteme darstellen, wobei zu beachten ist, dass bei nicht-intrusiver Umsetzung auch keine automatisierte Reaktion auf einen Angriff erfolgen kann.

Maßnahmen auf Softwareebene Neben der Implementierung geeigneter Schutzsysteme gilt es daher insbesonders, die Systembasis zu härten. Bei geeigneter Nutzung von Open Source können hierbei positive Effekte erzielt werden. Für sicherheitskritische Systeme, insbesondere im Bereich von KRITIS und Steuerungssystemen, ist die Nutzung von Mikrokernen wie bspw. der L4-Mikrokernel-Familie[62] von grundlegender Bedeutung zur Minimierung der Angriffsoberfläche. Die Möglichkeiten, die Hürde für Angreifer durch die Nutzung formaler Methoden wie beim mathematisch verifizierten Mikrokern seL4 deutlich zu erhöhen, wurden durch das HACMS-Programm[63] der DARPA[64] eindrucksvoll demonstriert[65]. Insbesondere hat das Programm gezeigt, dass sich auch Bestandssysteme härten lassen; die Komplexität des zu betrachtenden Systems und entsprechende Grenzen müssen hierbei natürlich berücksichtigt werden.

[58] Vgl. bspw. Norm IEC 61850 (International Electrotechnical Commission) im Bereich der Automatisierung von Schaltanlagen.
[59] Intrusion Detection System, IDS
[60] Vgl. z.B. Tavis Ormandy, „How to Compromise the Enterprise Endpoint“, Google Project Zero, 2016.
[61] Vgl. bspw. Robert und Teo Kühn, „Defending the Grid: Backfitting Non-Expandable Control Systems“, 9th International Conference on Cyber Conflict (CyCon), IEEE, 2017.
[62] Vgl. bspw. The L4 µ-Kernel Family
[63] Vgl. High-Assurance Cyber Military Systems (HACMS) (Archived)
[64] Defense Advanced Research Projects Agency
[65] Vgl. bspw. Kathleen Fisher et al., „The HACMS program: using formal methods to eliminate exploitable bugs“, Philosophical Transactions, Series A, Mathematical, Physical, and Engineering Sciences Vol. 375,2104, 2017.

Maßnahmen auf Hardwareebene Manipulationen auf Hardwareebene zeichnen sich durch eine besonders herausfordernde Detektierbarkeit aus. Zwar entwickelt sich auch dieser Bereich und Detektionsmöglichkeiten werden zunehmend erforscht und (weiter-)entwickelt, unterliegen in der Praxis aber immer noch umfassenden Restriktionen[66]. Entsprechend sind eigene Kapazitäten im Bereich der Hardwareproduktion wünschenswert. Während in einigen Spezialbereichen wie bspw. TPM-Chips[67] deutsche Unternehmen führend sind, besteht eine hohe Abhängigkeit im Bereich von General-Purpose Hardware.

Der Aufbau umfassend eigener, autarker Kapazitäten ist aufgrund des erforderlichen Know-Hows, insbesondere aber auch aus Kostengründen kaum möglich. Selbst groß angelegte Programme wie das „Trusted Foundry Program“ des United States Department of Defense stoßen dabei immer wieder an Grenzen[68]. Entsprechend ist im Bereich der Hardware eine Fokussierung auf Systemanteile erforderlich, welche zum einen eine hohe Relevanz für die Sicherheit des Gesamtsystems haben, zum anderen aber realistisch erreichbar sind. Gerade im Bereich von hochsicheren und Steuerungssystemen offerieren sich diesbzgl. Möglichkeiten, da entsprechende Systemkomponeten typischerweise weniger komplex sind und oftmals keine „High-End“ Performance abbilden müssen. Entsprechend können Open Source Prozessordesigns wie der RISC-V[69] Basis für ein hochsicheres, in eigenen Produktionskapazitäten gefertigtes System sein. Der MiG-V[70] ist Beispiel eines RISC-V basierten Prozessors Made in Germany, welcher zusammen mit dem verifizierten Mikrokern seL4 eingesetzt und somit die Basis für ein hochsicheres System liefern kann[71].

Neue Technologien Mit der exponentiellen technologischen Entwicklung eröffnen sich vielversprechende Möglichkeiten zur Erhöhung der Cybersicherheit. Bekannte Beispiele sind abhörsichere Kommunikationsverbindungen auf Basis von Quantenschlüsselaustausch[72] oder selbstheilende Systeme, welche Angriffe automatisch erkennen und analysieren können, Patche für die entsprechenden Schwachstellen entwickeln und diese ebenfalls automatisch anwenden. Das Finale der „Cyber Grand Challenge“ der DARPA im Jahre 2016[73] hat eindrucksvoll demonstriert, welches Potential in diesem Forschungsgebiet liegt.

Beachtet werden muss jedoch, dass auch bei Systemen mit in der Theorie perfekter Sicherheit wie bspw. im Bereich des Quantenschlüsselaustauschs, in der Praxis immer Angriffsvektoren durch die physikalische Implementierung verbleiben, bspw. durch Seitenkanalangriffe aber insbesondere durch Angriffe der oberen Ebene - dem bewussten Einbringen von Schwachstellen durch einen hochwertigen Angreifer. So kann bspw. die tatsächliche Sicherheit eines Quantenschlüsselaustauschs von der Qualität der zugrundliegenden Zufallszahlen abhängen[74] - diese sind in der Praxis per se schwierig zu erzeugen, schwer erkennbare Angriffe können die Sicherheit des betroffenen Systems nachhaltig schwächen[75].

[66] Vgl. bspw. Sam Thomas, Aurélien Francillon, „Backdoors: Definition, Deniability and Detection“, Proceedings of the 21st International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2018.
[67] Trusted Platform Module
[68] Vgl. bspw. A Crisis In DoD's Trusted Foundry Program?
[69] Reduced Instruction Set Computer, RISC-V
[70] Made in Germany RISC-V, MiG-V
[71] Vgl. bspw. MiG-V: First RISC-V Made in Germany with HW Security Features
[72] Quantum Key Distribution, QKD. Vgl. bspw. die BB84 und Ekert91 Protokolle.
[73] Vgl. Cyber Grand Challenge (CGC) (Archived)
[74] Vgl. bspw. Hong-Wei Li et al., „Randomness determines practical security of BB84 quantum key distribution“, Scientific Reports 5, 16200, 2015.
[75] Vgl. bspw. Georg T. Becker et al., „Stealthy Dopant-Level Hardware Trojans“, International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2013.

Möglichkeiten und Grenzen der Resilienz Mit Blick auf die derzeitige Systemlandschaft kann deren Resilienz insbesondere auch im Bereich KRITIS durch bspw. die genannten Technologien noch erheblich gesteigert werden. Eine 24/7-Überwachung von Netzen und Systemen, ausreichende Kapazitäten im Bereich Incident Response und der IT-Forensik sowie stetige Investitionen in den Bereich Cyber-Awareness sind essentiell, ebenfalls sind Maßnahmen und Programme zur Erhöhung der Digitalen Souveränität in diesem Kontext besonders zu begrüßen.

Beachtet werden muss jedoch, dass sich die Situation unsicherer Systeme nicht einfach und schnell ändern lässt, sondern es selbst unter *optimalen* Bedingungen viele Jahre dauern kann, bis eine spürbare und effektive Härtung des Gesamtsystems erreicht wird. Die lange Nutzungsdauer des Mobilfunkstandards GSM und dessen Verfügbarkeit auch noch in modernen Netzen, oder die lange Transition vom Internet Protokoll (IP) Version 4[76] zur Version 6[77] mit Parallelnutzung beider Varianten und daraus resultierender Sicherheitsimplikationen sind Beispiele für die praktischen Herausforderungen bei der Weiterentwicklung komplexer Netze und Systeme. Auch gilt, dass grundsätzliche Architektureigenschaften des Internets, welche für einen zuverlässigen Betrieb erforderlich sind, auch künftig ausgeklügelte Angriffe erlauben werden; RFCs[78] und darauf basierende Standardisierungen ermöglichen oftmals einen gewissen Interpretationsspielraum[79], welcher bewusst vorhanden ist, um die Kompatibilität und Interoperabilität der Implementierungen verschiedener Hersteller zu unterstützen. Ein solcher Interpretationsspielraum resultiert bspw. in unterschiedlichen initialen Werten für die "Lebenszeit"[80] eines IP-Pakets. Da diese somit vom Hersteller bzw. System abhängen können, kann dies bspw. zur Erkennung eines eingesetzten Betriebssystems bei einem Netzscan herangezogen werden[81]. Die vorhandenen Freiheitsgrade lassen sich aber bspw. auch für die Implementierung von schwer detektierbaren Seitenkanälen nutzen[82], auch auf unteren Schichten des ISO/OSI-Referenzmodells.

Die Aktivitäten zahlreicher professioneller Angreifergruppen[83] werden absehbar nicht verschwinden. Dazu kommen die latente Gefährdung durch bereits in Systeme eingebrachte Hintertüren sowie Angriffe der oberen Bedrohungsebene, nicht komplett vermeidbare Implementierungsfehler, unerwartete Seiteneffekte oder neue Technologiesprünge, welche Handlungsmöglichkeiten auch für Angreifer eröffnen. Neue Schutzverfahren ziehen neue Angriffsverfahren nach sich, neue Technologien und Erkenntnisse eröffnen neue Schwachstellen.

Die Erhöhung der Systemresilienz ist unter dem Einfluss der zahlreichen realen Bedrohungsvektoren die absolut notwendige Grundlage, aber auch absehbar nicht ausreichend. Dies erfordert das Vorhalten offensiver Fähigkeiten, um bspw. bei der Entwicklung einer Cyberkrise handlungsfähig zu sein und zu bleiben. Insbesondere auch im militärischen Bereich muss jederzeit mit Cyber-Hochwertfähigkeiten von Akteuren gerechnet werden, was die Verfügbarkeit offensiver Cyberkapazitäten zwingend für den sicheren Betrieb, als auch für die Durchsetzungsfähigkeit macht.

[76] Internet Protocol, RFC 791
[77] Internet Protocol, Version 6 (IPv6), RFC 2460 (obsolete), RFC 8200
[78] Requests for Comments sind Veröffentlichungen der Internet Society und zugehöriger Gruppen wie bspw. der Internet Engineering Task Force (IETF), welche für die (Weiter-) Entwicklung von Internetstandards verantwortlich ist.
[79] Vgl. insb. RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels".
[80] TTL, Time-to-Live
[81] Vgl. RFC 793, RFC 1122, Sektion 3.2.1.7 und RFC 1700. Der derzeitig *empfohlene* Default-Wert beträgt 64.
[82] Covert Channels. Vgl. bspw. R.P Murphy, "IPv6/ICMPv6 Covert Channels".
[83] Vgl. bspw. APT Groups and Operations