Expertise

Ukraine vs. Russland – Der erste Cyberkrieg in Europa?[1]

Anatomie einer Auseinandersetzung im digitalen Raum sowie Schlussfolgerung für die Schweiz

MIRKO HELBLING, OLIVER RUGGLI, YANN DONON

Abstract La cybersécurité a pris une place de plus en plus importante dans notre société en raison de la numérisation, en particulier au cours de la dernière décennie, alors que le risque d'actes de guerre dans le cyberespace est devenu de plus en plus présent. Aux yeux de nombreux gouvernements et du grand public, l'année 2022 est devenue un tournant dans la politique de sécurité européenne, déclenché par le conflit en cours en Ukraine. Dans cet essai, nous donnons un aperçu de l'évolution des cyberguerres, des principaux acteurs de la cyberguerre et de leurs moyens et pratiques respectives, en tenant compte des organisations gouvernementales, paragouvernementales, criminelles et décentralisées. Nous analysons et interprétons de manière approfondie ce qui se passe en Ukraine et autour de l'Ukraine et en tirons les enseignements clefs pour la Suisse.

Schlüsselbegriffe Cyberkrieg; Russland; Ukraine; Anonymous; Cybersicherheit
Keywords cyberdéfense; Russie; Ukraine; Anonymous; cybersécurité

MIRKO J. HELBLING M.Sc., MBA, CAS, hat seit dem Abschluss seiner Berufsausbildung mit verschiedenen Bereichen der Informatik und im Speziellen der Cybersicherheit beruflich zu tun. Darüber hinaus doziert er an der Höheren Fachschule TEKO Bern im Nachdiplomstudium Cybersecurity & Privacy und der FFHS. Seit vier Jahren arbeitet er in der Verteidigungsindustrie und setzt sich vertieft mit Themen der angewandten Kryptografie, sicherer Kommunikation sowie Architekturen für sichere Systeme als Head Cyber Defence Technologies auseinander. Zuvor beschäftigte er sich mit Themen der OT und IoT-Security. Zu seinen Zertifikaten gehören u. a. CISSP, CISA, CISM, CEH sowie diverse Weiterbildungen von unterschiedlichsten Hochschulen aus dem In- und Ausland.
E-Mail: mirko-helbling@outlook.de

OLIVER RUGGLI M.Sc., hat nach seinem Abschluss als Informatiker EFZ Erfahrungen im IT-Servicebereich in einem Schweizer Pharmaunternehmen gesammelt, um danach das Studium an der Fachhochschule Nordwestschweiz (FHNW) in Wirtschaftsinformatik und Computer Science auzunehmen. Seit einem Jahr arbeitet er in der Verteidigungsindustrie mit Fokus auf die Themen Requirements Engineering, IT Architekturen und Innovationsprojekte. Seit Anfang dieses Jahres vertieft er sich in Sicherheitsarchitekturen und Innovationskraft.

YANN DONON, Ph.D., ist Data Science Lead für die RUAG Cyber Defence Unit. Nach seinem Studium in Lausanne begann er seine internationale Karriere in der Luft- und Raumfahrtbranche. Seine Doktorarbeit brachte ihm die Mitgliedschaft in einem Institut der Russischen Akademie der Wissenschaften und eine Stelle am CERN ein. Dort arbeitete er als Senior Researcher und führte im Rahmen der DUNE-Kollaboration Postdoc-Arbeiten durch. Seine Hauptforschungsinteressen sind die Erkennung und die Vorhersage von Anomalien, angewandt in den Bereichen Netzwerksicherheit, Bildgebung und Verhaltensanalyse.

Einführung

Der Begriff «Zeitenwende», der seit Februar 2022 die Diskussionen rund um den Ukrainekrieg mitprägt, könnte nicht nur für die Umschreibung der geopolitischen Veränderungen unserer Zeit verwendet werden, sondern dieser Terminus könnte ebenso auf die Analyse der Anatomie dieses Konfliktes in der digitalen Welt und im Bereich der Cybersicherheit gelten. Obschon seit einigen Jahrzehnten über die Gefahren von digitalen Auseinandersetzungen diskutiert und beinahe wöchentlich über neue Cyberangriffe berichtet wird, scheinen sich bereits einige Monate nach Kriegsbeginn interessante und wenig diskutierte Zusammenhänge bezüglich der Cybersicherheit abzuzeichnen. Stoll (2005) veröffentlichte vor über 30 Jahren das viel beachtete Werk «The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage», in dem er aufzeigt, wie sowjetische Dienste in ein dem Department of Defense (DoD)[2] nahestehendes Netzwerk eindrangen. Wenige Jahre später erschien von Shimomura und Markoff (1995) das Werk «The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It», welches ebenfalls viel Beachtung fand und das Thema Cybersicherheit popularisierte. Auch die Filmindustrie nutzte bereits 1983 die Faszination der digitalen Auseinandersetzungen, indem mit der Produktion «War Games» eine Handlung erschaffen wurde, in welcher es einem Jugendlichen gelang, in Computersysteme der US-Streitkräfte einzudringen und beinahe den Dritten Weltkrieg auszulösen. Viele weitere Publikationen und Filme folgten, bis das Thema Cybersicherheit nach den Veröffentlichungen des ehemaligen National Security Agency (NSA) Mitarbeiter Edward Snowden definitiv in der Mitte der Gesellschaft und der Politik angekommen war (Andress und Winterfeld 2011). Sicherheitsspezialisten und Forscherinnen beschäftigen sich hingegen bereits seit über 50 Jahren mit Fragestellungen der Cybersicherheit. Ware (1967) veröffentlichte eine der ersten Publikationen, die sowohl die Cybersicherheit wie auch die Privatsphäre adressierte. Er merkte damals schon an, dass das Teilen von Rechnerressourcen (z. B., Speicher, Prozessorlaufzeit etc.) zwischen einzelnen Benutzern risikobehaftet sei. Yost (2007) veröffentlichte den Artikel «A history of computer security standards», die Einblicke in die Evolution der Cybersicherheit zulässt.

Hintergrund und Theorie von Cyberkriegen

Allgemein ist es herausfordernd, Begrifflichkeiten wie Cy-

berraum, Cybersicherheit oder Cyberkrieg einzuführen und zu diskutieren. Viele dieser Termini beinhalten ein hohes Mass an Interpretationsmöglichkeiten und werden dementsprechend oft divergierend definiert und verstanden (Andress und Winterfeld 2011). Die Vereinten Nationen (UN) definieren den Begriff Cyberraum wie folgt: «Das globale System von Systemen aus vernetzten Computern, Kommunikationsinfrastrukturen, Online-Konferenzeinrichtungen, Datenbanken und Informationsdiensten, das allgemein als das Netz bekannt ist». Hingegen versteht das Eidgenössische Departement für Verteidigung Bevölkerungsschutz und Sport (VBS) unter dem gleichen Terminus: «Alle durch die Armee betriebenen und genutzten Informatiksysteme (IKT-Systeme). Alle Daten und Informationen sowie die Nutzer der IKT-Systeme gehören ebenfalls zum Cyberraum» (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS 2022, S. 9).

Die Frage, ob definitionsgemäss Nutzer zum Cyberraum gehören oder nicht kann in der Praxis relevanter sein, als bei der Ausarbeitung der Definition vielleicht angenommen wird. Noch anspruchsvoller ist der Begriff der Cybersicherheit, welcher allgegenwärtig ist, of benutzt, subjektiviert und selten gleich von allen verstanden wird (Craigen et al. 2014). Darüber hinaus wird der Begriff selten eingeführt, weshalb oftmals nur erahnt werden kann, was die Autoren und Autorinnen darunter verstehen. Oftmals sind im Begriff Cybersicherheit die Kernelemente der vermutlich zwei populärsten Definitionen wiederzufinden. Einerseits die Definition der Internationalen Organisation für Normung (ISO)[3] sowie jene des National Institute of Standards and Technology (NIST)[4]. Auffallend ist der starke Bezug, den die ISO zu den Informationen macht, während die verarbeitenden Systeme mehr oder weniger ausgeblendet werden. Hingegen verfolgt die NIST einen etwas holistischeren Ansatz. Unabhängig davon, sollte die Definition des Begriffes Cyberraum die Grundlage für den Term Cybersicherheit bilden.

Weit komplizierter wird es, den Begriff des Cyberkrieges (englisch: Cyberwarfare) einzuführen. Obgleich der inflationären Nutzung dieses und den darauf aufbauenden Szenarien, scheint eine einheitliche und anerkannte Definition weiterhin zu fehlen. Daraus folgt, dass der Begriff des Cyberkrieges ebenfalls stark subjektiviert und dementsprechend opportunistisch verwendet wird. Singer und Friedman (2014) definieren in ihrem viel gelesenen Werk «Cybersecurity and Cyberwar: What everyone needs to know» den Begriff wie folgt: «Unter Cyberkrieg versteht man den Einsatz von Cyberangriffen gegen einen feindlichen Staat, die vergleichbare Schäden verursachen wie die eigentliche Kriegsführung und/oder lebenswichtige Computersysteme stören». Hingegen definiert einer der einflussreichsten Vordenker der letzten Jahre, der ehemalige Berater des Weissen Hauses für Terrorismusbekämpfung Richard Clarke, den Begriff wie folgt: «Handlungen eines Nationalstaates, die darauf abzielen, in die Computer oder Netzwerke eines anderen Staates einzudringen, um Schaden oder Störungen zu verursachen» (Knake und Clarke 2012). Während gemäss der Definition von Singer und Friedman (2014) ein signifikanter beziehungsweise vergleichbarer Schaden wie in einem konventionellen Krieg entstehen muss, um den Begriff des Cyberkrieges zu rechtfertigen, muss nach Knake und Clarke (2012) lediglich Schaden entstehen. Das Atlantische Bündnis (NATO) hat die Schwierigkeiten um die Einordung dieses Begriffes sowohl im militärischen wie auch juristischen Rahmen erkannt und mit dem «Tallinn Manual» entsprechend ein Hilfswerk für die Staaten erschaffen (Schmitt 2017). Einfachheitshalber interpretieren wir hier den Begriff der digitalen Kriegsführung als Synonym für Cyberkrieg und verstehen darunter staatlich orchestrierte oder durchgeführte Cyberangriffe, welche als Medium drahtgebundene oder drahtlose Technologien, beruhend auf den standardisierten Internetprotokollen (IPv4 / IPv6), verwenden und somit vorwiegend über den Cyberraum stattfinden. Zusätzlich ist in unseren Augen eine deutliche Abgrenzung zum Begriff Informationskrieg notwendig. Ebenfalls grenzen wir den elektromagnetischen Raum vom Cyberraum ab.

«Einfachheitshalber interpretieren wir hier den Begriff der digitalen Kriegsführung als Synonym für Cyberkrieg und verstehen darunter staatlich orchestrierte oder durchgeführte Cyberangriffe, welche als Medium drahtgebundene oder drahtlose Technologien, beruhend auf den standardisierten Internetprotokollen (IPv4 / IPv6), verwenden und somit vorwiegend über den Cyberraum stattfinden.»

Interessiert man sich für die möglichen Fähigkeiten, welche im Bereich einer digitalen Auseinandersetzung zum Einsatz kommen könnten, sind die entsprechenden staatlichen Strukturen zu untersuchen, welche die dafür notwendigen Mittel und Methoden zu Verfügung stellen. Gemäss Saalbach (2019) ist die typische nationale Sicherheitsarchitektur in drei Bereiche aufgeteilt. So unterscheidet Saalbach (2019) den zivilen Bereich, welcher die Absicherung der kritischen Infrastruktur vorsieht, den nachrichtendienstlichen Bereich, welcher für die Analyse der Kommunikation und der Datenströme verantwortlich ist sowie den militärischen Bereich, welcher üblicherweise über Offensivkapazitäten verfügt.

Mit Blick auf die westliche Hegemonialmacht USA ist ein erheblicher Bestandteil der digitalen Schlagkraft in der Intelligence Community anzutreffen, also den staatlichen Nachrichtendiensten (Saalbach 2019). Dabei dient die National Security Agency (NSA) als Fernmelde- und Aufklärungsdienstleister, die mit dem militärischen US Cyber Command Cybercom gemeinschaftlich geführt wird. Dabei liegen operative Kernfähigkeiten bei der Tailored Access Operations Group (TAO), einer Organisationseinheit für digitale Spezialoperationen der NSA, welcher sowohl grosse Kompetenz wie auch eine gewisse Nähe zur Equation Group nachgesagt wird. Die TAO ist, einigen Quellen zu Folge, die grösste und wohl wichtigste Komponente des riesigen Signals Intelligence Directorate (SID) der NSA, das aus mehr als 1000 militärischen und zivilen Computerhackern, Geheimdienstanalysten, Computerhard und -softwareentwicklern sowie Elektroingenieuren besteht (Aid 2013; Loleski 2019). Es ist ohnehin bekannt, dass die NSA enge Verbindungen mit der Industrie und andere Organisationen pflegt und dadurch die Möglichkeit hat, sogenannte Hintertüren (back doors) in Produkte und Algorithmen einzubauen (Hales 2013; Bernstein et al. 2016). Die Equation Group ist hingegen eine Hackergruppe, die im Jahr 2016 durch das russische Sicherheitsunternehmen Kaspersky Lab bekannt gemacht wurde (Emm et al. 2016). Sicherheitsforscher gehen davon aus, dass die Equation Group wiederum an der Entwicklung von STUXNET[5] direkt oder indirekt beteiligt waren. Zusätzlich dazu haben auch die Central Intelligence Agency (CIA) sowie das Department of Homeland Security (DHS) und das Federal Bureau of Investigation (FBI) in meist enger Zusammenarbeit mit der Privatwirtschaft ihre Fähigkeiten über die letzten Jahre ausgebaut. Ferner leitet das FBI die National Cyber Investigative Joint Task Force (NCIJTF), die Informationen und Aktivitäten aus den Bereichen Spionageabwehr, Terrorismusbekämpfung, Nachrichtendienste und Strafverfolgung sowie Aktivitäten von 19 Bundesbehörden bündelt, um Cyberangriffe vorherzusagen und zu verhindern (Pernik et al. 2016).
Russland verfolgt hingegen in der Operationssphäre Cyber einen asymmetrischen Aufbau der Fähigkeiten. Nach der Auflösung des sowjetischen Geheimdienstes KGB wurden vier Folgeorganisationen gegründet: Der FSO zum Schutz des Präsidenten, der FSB als Inlandsgeheimdienst sowie der SVR als Auslandsgeheimdienst, während die Fähigkeiten in der militärischen Nachrichtenaufklärung durch den GRU abgedeckt werden. Man geht davon aus, dass der GRU weitreichende Fähigkeiten sowohl in der Cyber- wie auch der Informationskriegsführung hat.

Im Bereich der offensiven Fähigkeiten sieht man Parallelen zwischen der amerikanischen TAO sowie der russischen Einheit-26165, welche dem GRU zugeordnet wird. So gehen nicht wenige davon aus, dass ein Grossteil der APTs (z. B., APT28 und APT29) wie auch die Waterburg/Turla-Gruppe sowie die Sandworm/Quedagh-Gruppe neben der Energetic Bear/Dragonfly-Gruppe unter der Kontrolle des GRU und somit der Russischen Föderation stehen. APT steht für Advanced Persistent Threat (d. h. fortgeschrittene andauernde Bedrohung) und beschreibt eine Cyberattacke mit oft weitreichenden Folgen und hoher Komplexität. Die meist unbekannten Gruppen, die hinter diesen Angriffen vermutet werden, taufte man im Anschluss APTx, wobei «x» ein Inkrement darstellt. All diese Gruppen sind bekannt für weitreichende Operationen, die mit der Spionage, der Manipulation von Wahlen oder anderen Angriffen auf kritische Infrastrukturen in Verbindung gebracht werden. Aus westlicher Sicht liegt in Russlands Fähigkeiten eine starke Vermischung zwischen staatlichen und kriminellen Strukturen zugrunde. Dieser Umstand macht die Differenzierung zwischen Kriminalität und staatlich angeordneten Operationen aus Russland äusserst schwierig.

Cyberkriege der vergangenen Jahre

Die Gefahr, die von Cyberangriffen ausgehen, ist altbekannt. Bereits in den 1970er Jahren wurden erste Aktionen registriert, welche zu einem beträchtlichen Sachscha-

den führten (Kabay 2012). Viele dieser Angriffe hatten jedoch einen opportunistischen Hintergrund und entfalteten kaum eine strategische Wirkung (Kabay 2012). Dies änderte sich, als im Jahr 1982 die Tscheljabinsk-Pipeline in der ehemaligen UdSSR durch eine Explosion mit ungefähr 3 Kilotonnen Sprengstoff zerstört wurde. Die UdSSR war in der Zeit des Kalten Krieges auf Hochleistungstechnologie aus Nordamerika zur Steuerung der Pipeline angewiesen. Die Steuerungssoftware war jedoch vor dem Export durch Spezialisten der US-Dienste manipuliert worden, was zu Fehlern in der Komponentensteuerung von Pumpen, Turbinen und Ventilen führte. Darauf wurde der zulässige Höchstdruck in der Pipeline überschritten und eine Explosion war unausweichlich. Dieser Zwischenfall wird heutzutage oftmals als erster Cyberkrieg der Geschichte bezeichnet – Russland dementiert diese Darstellung der Geschehnisse (Saalbach 2019).

Hingegen wird die erste grossangelegte Cyberspionage auf das Ende der 1990er Jahren datiert und trägt den Namen «Moonlight Maze». Mit einer fast zwei Jahre andauernden Aktion gelang es einem Akteur, wertvollste Informationen des amerikanischen Verteidigungsministeriums sowie der Raumfahrtbehörde NASA und weiteren Ministerien zu exfiltireren. Spätere Untersuchungen zeigten auf, dass digitale Spuren in eine ehemalige Republik der UdSSR führten. Der Verdacht liegt nahe, dass Russland als Sponsor dahinterstand, was das Land aber bis heute bestreitet (Haizler 2017). In den Balkankonflikten (1991–2001) wurde die digitale Dimension ebenfalls für die Kriegsführung genutzt, indem z. B. Komponenten der NATO von Hackergruppen angegriffen wurden, nachdem die chinesische Botschaft in Belgrad versehentlich durch Bomben zerstört worden war (Hunker 2010). Vorhergehend wurden verschiedene Telefonnetze durch das Atlantische Bündnis sabotiert, was wiederum andere Autoren als erste cyberkriegsähnliche Massnahme betrachten (Saalbach 2019). Auch in darauffolgenden Konflikten zwischen Russland und Georgien im Jahr 2008 konnten Cyberangriffe als Teil der Kriegsführung dokumentiert werden. So wurden Distributed-Denial-of-Serivce (DDoS)-Angriffe auf staatliche Server ausgeführt, worauf parallel die ersten Artillerie- und Luftangriffe folgten. Aus historischer Sicht war dies der erste Cyberangriff, welcher koordiniert mit klassischen Kampfmittel einherging. Auch im Vorfeld des Krieges zwischen Russland und Georgien 2008 wurden zuerst georgische Rechnersysteme kompromittiert. Neben kritischen Infrastrukturen, Transportunternehmen, waren Webseiten von Medien und Banken betroffen. Als Akteure vermutet man heute die den russischen Diensten nahestehende APT28/Fancy Bear/Sofacy-Gruppe (Gazula 2017). Weitere kriegsähnliche Aktionen im digitalen Raum wurden bei der zweiten sogenannten Tulpenrevolution in Kirgisistan im Jahr 2009 sowie an der darauffolgenden Jasmin Revolution 2010 in Tunesien festgestellt. Eine technische Einheit des kirgisischen Nachrichtendienstes knackte den E-Mail Account von Gennady Pavlyuk, einem der führenden oppositionellen Journalisten. Unter Einbezug von gestohlenen Daten konnten sie ihn in einen Hinterhalt locken und anschliessend eliminieren. In Tunesien wurden während der Revolution sensible Daten aller registrierter Benutzer veröffentlicht, nachdem diese durch den staatsnahen Internetanbieter AMMAR gehackt worden waren (Gazula 2017; Carr 2011). Auch zu Beginn des Konfliktes in der Süd- und Ostukraine in den Jahren 2014 und 2015 konnten sowohl schwerwiegende wie auch äusserst komplexe Angriffe auf kritische Infrastrukturen der Ukraine beobachtet werden (Serpanos und Komninos 2022; Mohee 2022). So wurden Betriebstechnologien, also vorwiegende SCADA Systeme, welche für den Betrieb des Stromnetzes notwendig sind, infiltriert. Dies führte im Dezember des Jahres 2015 zu grossen Stromausfällen mit über 225 000 betroffenen Kunden. Anscheinend gelang es den Angreifern, Schaltkontakte zu öffnen. Simultan folgten Telephone-Denial-of-Service-Attacken (TDoS), um die Verfügbarkeit der entsprechenden Telefonzentralen einzuschränken. Auch wurde die Wiper-Malware KillDisk nachgewiesen, welche die Systeme beschädigen sollten. Heute wird vermutet, dass die Sandworm/Quedagh-Gruppe Urheber der Angriffe war (Saalbach 2019). Weiter gab es Berichte über eine US-Drohne des Typs MQ-5B, welche durch elektromagnetische Störmanöver über der Krimhalbinsel zu einer Notlandung gezwungen worden war. Wiederum Jahre später wurden erneut ausgeweitete Angriffe mittels einer Malware namens Industroyer/CrashOverride in Kiev festgestellt, die ebenfalls einen Blackout zur Folge hatten. Dieser Angriff wird einer Gruppe namens Electum zugeschrieben, welche der Sandworm/Quedagh-Gruppe nahstehen soll (Saalbach 2019). Die IT-Sicherheitsfirma CrowdStrike meldete einen Angriff auf ukrainische Artilleriegeschütze des Typs Howitzer im Jahr 2016, welcher durch eine eigens entwickelte Android Applikation ermöglicht wurde. Diese Applikation

war von einem ukrainischen Offizier entwickelt worden, um die Berechnung von Zieldaten zu beschleunigen. Die Malware der APT28/Fancy Bear/Sofacy-Gruppe wurde dabei verdeckt in ein Android Paket eingepackt. Quellen zufolge, erhöhte sich dadurch der Verlust von Artilleriegeschützen auf ukrainischer Seite um 30 % auf 80 % im Vergleich zu den Vorjahren, bei denen die Verlustquote bei 50 % gelegen war (Saalbach 2019).

Interpretationen des aktuellen Konfliktgeschehens

Im aktuellen Konflikt zwischen Russland und der Ukraine können sowohl gezielte wie auch opportunistische Angriffe beobachtet werden. Opportunistische Angriffe verfolgen das Ziel, «irgendwelchen» Schaden dem Gegner oder mit dem Gegner in Verbindung stehenden Organisationen zuzufügen, unabhängig von den übergeordneten strategischen Zusammenhängen. Losgelöste Hackerkollektive wie Anonymous oder andere Einzelkämpfer, die sogenannten «Lone Wolfs», gehören dieser Gattung an, indem sie gefühls- und meinungsgeleitet Ziele evaluieren oder solche übernehmen (Geers et al. 2014). Gezielte Angriffe werden hingegen oftmals von staatlichen Organisationen durchgeführt, welche im Rahmen einer vordefinierten Strategie die Ziele lokalisiert, und diese entsprechend infiltriert (Aditya und Richard 2013). Die Auswirkungen von Cyberkriegen sowie deren praktischen Nutzen ist bis heute schwierig einzuschätzen und noch schwieriger vorherzusagen, im Speziellen, wenn opportunistische Elemente in einem höheren Masse Bestandteil der vorliegenden Taktik sind. Maschmeyer und Cavelty (2022) zweifelt deren strategischen Nutzen stark an, da militärische Cyberoperationen in einem hybriden Kriegsgeschehen entweder zu langsam, zu schwach oder nicht genügend zuverlässig sind – verglichen mit anderen zur Verfügung stehenden Kampfmitteln.

Unter all den zuvor genannten Hackergruppen sticht ein Name in der Öffentlichkeit hervor: Anonymous. Anonymous wurde 2003 gegründet und wird fälschlicherweise oft als strukturierte Organisation dargestellt, die die «Guy-Fawkes-Maske» als Herold trägt. Auf die Frage «Wer steckt hinter der Maske?» gibt die Organisation selbst die Antwort: Jeder, der unsere Aktionen zu einem bestimmten Zeitpunkt unterstützt (Harry 2014). Am 24. Februar 2022 erklärte einer der Haupt-Twitter-Accounts der Gruppe den «Cyberkrieg gegen die russische Regierung». Bei dieser Gruppierung handelt es sich um eine Ansammlung von Individuen mit unterschiedlichen Computerkenntnissen, die i. d. R. mit keiner Regierung oder strukturierten Organisation verbunden sind – obschon angenommen werden kann, dass auch staatliche Akteure dieses Kollektive längst unterwandert haben. (Gabriella 2013). Anstelle von Angriffen, die auf eine bestimmte Infrastruktur durchgeführt oder koordiniert werden, kann man sich einen Schwarm vorstellen, welcher in Versuchung steht, ein «Gebiet» zu plündern. Seit dem 24. Februar 2022 wurden hunderte solcher Angriffe gegen Russland dokumentiert (Patrick 2022; Olivia und Stevan 2022; Denys und Wiktor 2022), bei denen angeblich Medien sowie die Webseite des russischen Verteidigungsministeriums stillgelegt, interne Inhalte privater, mit Russland verbundener Unternehmen der Militärindustrie und der russischen Zentralbank veröffentlicht oder gefälschte Nachrichten im Namen von wichtigen Personen der russischen Öffentlichkeit versendet wurden. (@YourAnonTV 2022; Strepkov 2022). Dieser Modus Operandi wird durch die Verringerung der technischen Komplexität beim Eindringen in Computersysteme erleichtert. Aktuelle Studien haben die Möglichkeit aufgezeigt, funktionierende Schadprogramme für Preise unter 10 Dollar zu erwerben (Mikalauskas 2021). Mit diesen Produkten ist es für jeden und jede mit grundlegenden IT-Kenntnissen möglich, sich an Angriffen zu beteiligen. Derzeit wird darüber spekuliert, ob das Anbieten dieser Produkte für die breite Öffentlichkeit Teil der Strategie bestimmter Staaten zur Cyberkriegsführung ist. Bestätigt ist hingegen nur die Tatsache, dass Anonymous dem russischen Staat den «digitalen Krieg» erklärt hat und somit zumindest vermeintlich eine autonome Kriegspartei an der Seite der Ukraine darstellt (Harding 2022).

«Die Auswirkungen von Cyberkriegen sowie deren praktischen Nutzen ist bis heute schwierig einzuschätzen und noch schwieriger vorherzusagen.»

Dieser Umstand führt dazu, dass ein überstaatlicher Cyberkrieg in Osteuropa beobachtet werden kann. Während der GRU im Februar 2022 versuchte,

mittels DDoS-Angriffen Behördendienste sowie kritische Infrastrukturen anzugreifen, um deren Verfügbarkeit einzuschränken, legten diverse russische Hackergruppen nach, indem sie mittels DanaBot einer Malware-as-a-Service-Plattform weitere DDoS-Angriffe gegen das ukrainische Verteidigungsministerium initiierten (Pierluigi 2022). Dabei wurden HTTP-Anfragen an den E-Mail-Server gesendet, welcher unter https://post.mil.gov.ua erreichbar ist.

Der DDoS-Angriff wurde mit dem Download- und Ausführungsbefehl (Befehl 2048 / Unterbefehl 9) von DanaBot gestartet, um eine neue in Delphi geschriebene und ausführbare Datei bereitzustellen. Begleitend wurden diverse Wiper Angriffe detektiert, welche alle ein ähnliches Strickmuster aufwiesen. So wurden unterschiedliche Wiper Schadprogramme mit den Namen WhisperGate, HermeticWiper, Double Zero, IsaacWiper sowie CaddyWiper seit Beginn des Jahres auf ukrainischen Systemen detektiert. Als Wiper wird ein destruktives Schadprogramm bezeichnet, welches ähnlich wie ein Eraser funktioniert. Solche Schadprogramme sind dazu gedacht, auf dem infizierten Computer die Festplatte oder Teile davon zu zerstören. Wie dies umgesetzt werden kann, zeigt die Betrachtung der einzelnen Schadfunktionen der oben genannten Wipern. Eine Analyse von Fierro (2022a), welche bei der IBM arbeitet wurde, hat folgende Erkenntnisse gebracht:

So führt beispielsweise CaddyWiper die Funktion «DsRoleGetPrimaryDomainInformation» aus, um herauszufinden, ob es sich bei dem Hostsystem um ein Domain-Controller handelt oder nicht. Im Falle, dass das System die Rolle «DsRole RolePrimaryDomainController» besitzt, terminiert die CaddyWiper. Anderenfalls führt die Malware eine rekursive Löschung ausgehend von dem Verzeichnis %SystemDrive%\Users aus. Dabei werden sowohl versteckte wie auch betriebssystemrelevante Dateien berücksichtigt. Bei Dateien, welche ≥ 10 MByte gross sind, werden nur die ersten 10 MByte überschrieben. Nach C:\Users wiederholt CaddyWiper den gleichen Vorgang für alle verfügbaren Laufwerke von D:\ bis Z:\. Wenn alle verfügbaren Laufwerke gelöscht wurden, löscht CaddyWiper die Festplattenpartitionen von \\.\PHYSICALDRIVE9 bis \\.\PHYSICALDRIVE0, indem die ersten 1920 Bytes mit NULL überschrieben werden. Hingegen zielt die IsaacWiper zunächst auf das physische Laufwerk ab, indem diese mit einem Mersenne-Twister-Pseudozufallszahlengenerator (PRNG) die ersten 0x100000 Bytes des physischen Laufwerks mit zuvor erstellten Zufallszahlendaten überschreibt (Pierluigi 2022). Der Name des Mersenne-Twister-PRNG leitet sich von dem Sachverhalt ab, dass die Periodizität entsprechend einer Mersenne-Primzahl gewählt wurde (Tan 2016). Der Mersenne-Twister-PRNG ist mitunter einer der Weitverbreitetsten in Softwaresystemen und somit oftmals auf dem Hostsystem vorzufinden. Weiter zeigte die Analyse von Dwyer und Henson (2022) auf, dass nach dem Überschreiben des physischen Laufwerks, die IsaacWiper mit dem Überschreiben von Laufwerken und Dateien beginnt. Wenn die Wiper eine Datei nicht öffnen kann, wird die Datei in eine temporäre Datei unbenannt, welche aus dem Begriff «Tmf» und einer zufälligen vierstelligen Zeichenfolge besteht (z. B. Tmf3678.tmp). Anschliessend wird diese Datei mit Zufallszahlendaten überschrieben. Wenn auf ein Volume nicht zugegriffen werden kann, erstellt IsaacWiper ein verstecktes temporäres Verzeichnis und schreibt eine Datei in das Stammverzeichnis des entsprechenden Volumes. Die temporäre Datei Tmf3678.tmp wird anschliessend mit Zufallsdaten gefüllt, bis der Speicherplatz auf dem Volume erschöpft ist. Im Gegensatz dazu zählt HermeticWipe eine Reihe von bis zu 100 physischen Laufwerken in einer Schleife von 0–100 auf. Diese verwendet den standardmässigen Partitionsmanager, der zwischenzeitlich im System geladen wurde, um alle Master Boot Record (MBR) für jedes physische Laufwerk im System zu beschädigen (Fierro 2022b). Zusätzlich beschädigt HermeticWiper auch alle verfügbaren Partitionen, die sowohl das FAT- als auch das NTFS-Dateisystem unterstützen. Bei NTFS wird ebenfalls die Master File Table (MFT) beschädigt, die alle Informationen über eine Datei enthält, um sicherzustellen, dass die Daten nicht wiederhergestellt werden können (Fierro 2022b). WhisperGate greift ebenfalls den Master Boot Record (MBR) direkt an und überschreibt diesen mit einem manipulierten Bootloader. Beim anschliessenden Systemstart wird eine Erpressungsmeldung dargestellt und die eigentliche Schadfunktion ausgelöst. In regelmässigen Abständen überschreibt der Bootloader Sektoren der gesamten Festplatte eines infizierten Rechners. Der Bootloader greift über den BIOS-Interrupt 13h im LBA-Modus (Logical Block Addressing) auf die Festplatte zu und überschreibt jeden 199. Sektor, bis das Ende der Festplatte erreicht ist. Nachdem ein Datenträger beschädigt ist, überschreibt WhisperGate den nächsten in der Liste der erkannten Datenträger.

Dieser kurze Einblick in die Schadfunktion einzelner «Cyberwaffen», hilft den Begriff des Cyberkrieges zu kontextualisieren. Einige Indizien deuten auf eine Beteiligung der Gruppe Sandworm hin (Antoniuk 2022). Auch APT28 trat mit einer breit ausgelegten Phishing Kampagne auf die Mediengruppe UKRNet in Erscheinung. Zusätzlich wurde zu Beginn der Eskalation der ukrainische Satelliten Konzern Visat Outage durch eine ausgeweitete Aktion von russischer Seite schaden zugeführt, was zu gravierenden Einschränkungen im Bereich der Kommunikation auf ukrainischer Seite führte. Der bis heute als schwerwiegendste Cyberangriff dieses Konfliktes betrachtet wird, wurde ebenfalls mit einer Wiper namens AcidRain durchgeführt (Reed 2022). Die Kampagnen wurden von latenten Spionageangriffen wie z. B. von der Cameradon Backdoor begleitet. Noch lässt sich das Bild nicht abschliessend zeichnen, jedoch sieht man an den Bemühungen von russischer Seite eine längere Vorbereitungs- und Infiltrationsphase, sowie die vermeintlich taktische Absicht, die mittels Cyberangriffen verfolgt wird. Nicht Wenige gehen davon aus, dass Russland sehr granular versucht, die taktische Kommunikation der ukrainischen Kräfte einzuschränken und begleitend Aktionen startet, um die gegnerische IT-Armee zu binden. Auf der anderen Seite steht eine ukrainische IT-Armee, unterstützt durch ausländische Kräfte (z. B. Cyber Rapid Response Team der EU), welche damit beschäftigt ist, defensive Aufgaben zu übernehmen, während sie weltweit Hacktivisten zu offensiven Tätigkeiten auffordern und somit auch Anonymous ins Spiel brachte. Typischerweise sind Hacktivisten politisch und/oder ideologisch motivierte Hacker, die ihren Protest mit digitalen Aktionen kundtun. Basierend auf dieser Taktik können russische IT-Spezialisten gebunden werden. Diese opportunistischen Angriffe, welche oftmals un- oder schlecht koordiniert und in der taktischen Wirkung eingeschränkt sind, besitzen ihr Gefahrenpotenzial einzig in der Quantität und der Möglichkeit, eines daraus resultierenden Lucky Punch, also einem Glückstreffer. Die Sanktionen auf den High-Tech Sektor, welche beispielsweise die Auslieferung von sicherheitsrelevanten Updates und Patches betreffen, erhöhen die Angriffsfläche gegenüber Russland auf eine künstliche Art und Weise (Goud 2022). Die Kombination von vielen tausend Hacktivisten, die ihr Glück im russischen Netzwerk suchen und dabei zunehmend auf ungesicherte Systeme stossen werden, mit der Möglichkeit, dass in der westlichen Hemisphäre die Strafverfolgung für digitale Straftaten in Russland vielleicht milder geahndet wird, erschwert die Situation für russische IT-Spezialisten. Auch wurde mit RURansom ein gefährliches und auf Russland ausgerichtetes Wiper Schadprogramm entdeckt. Entsprechend reagierte die russische Führung mit einschneidenden Massnahmen im Bereich des Internets und der Förderung des Runet, eines eigens für Russland entwickeltes Internet, um den Schaden so gering wie möglich zu halten. Die Sanktionen im Bereich des High-Tech Sektors kombiniert mit der Orchestrierung von Hacktivisten über die ukrainische IT-Armee sowie die Unterstützung durch externe Dienste verfolgt klar eine Verteidigung-bei-Angriff Strategie, in dem versucht wird, die russischen IT-Spezialisten mit defensiven Tätigkeiten zu binden und somit deren Kapazitäten einzuschränken.

«Der erste koordinierte Angriff, welcher neben den verschiedenen Teilstreitkräften auf Cyberoperationen setzte, datiert auf das Jahr 2008.»

Schlussfolgerung

In diesem Essay wird veranschaulicht, dass die Termini Cybersicherheit und Cyberkrieg jeweils unterschiedlich definiert und interpretiert werden können (vgl. Kapitel 2). Beim Begriff des Cyberkrieges weiten sich die Definition hinsichtlich des Schadenausmasses, von Eindringen oder Störung bis hin zu Schäden, welche mit klassischen Kampfmitteln vergleichbar sind. Der erste koordinierte Angriff, welcher neben den verschiedenen Teilstreitkräften auf Cyberoperationen setzte, datiert auf das Jahr 2008 (vgl. Kapitel 3). Ein solch koordinierter Angriff konnte seither nur wenige Male festgestellt und dokumentiert werden. Dies ist einerseits darauf zurückzuführen, dass solche Angriffe im Verhältnis zu anderen klassischen Kampfmitteln eine hohe Komplexität sowie eine gewisse Unzuverlässigkeit haben.[6] Andererseits hat es in den letzten 30 Jahren wenige klassische Kriege zwischen vergleichbar digitalisierten Staaten gegeben, was die Interpretation solch historischer Daten erschwert. Cyberkriege sind – entgegen der gängigen Annahme – nur partiell die direkte Auseinandersetzung zwischen zwei staatlichen Akteuren. Oftmals sind unterschiedlichste Entitäten involviert und zivile

«Cyberkriege sind – entgegen der gängigen Annahme – nur partiell die direkte Auseinandersetzung zwischen zwei staatlichen Akteuren. Oftmals sind unterschiedlichste Entitäten involviert und zivile Einrichtungen im Fokus der Operationen.»

Einrichtungen im Fokus der Operationen.[7] Speziell die Kombination von wirtschaftskriegerischen sowie weitgehenden und anhaltenden cyberkriegerischen Handlungen ist risikobehaftet und hat das Potenzial ein Land mittelfristig zu entdigitalisieren und somit das Wirtschaftswachstum negativ zu beeinflussen.

«Darüber hinaus müssen zivile und militärische Strukturen im Bereich der Cybersicherheit synchronisiert werden, damit im Ernstfall eine abgestimmte Reaktion sowie ein einheitliches Lagebild möglich ist. Resultierend aus der Tatsache, dass strategische- und opportunistische Muster im Cyberraum vorhanden sind, muss eine allgemein hohe Sicherheitsmaturität erreicht werden.»

Die daraus resultierenden sozialen und ökonomischen Folgen sind kausal. Eine gewisse Unabhängigkeit der Wirtschaft und die Förderung von Technologiesouveränität, also die Entwicklungs-, Produktions- und Verteilungskompetenz, kann dem entgegenwirken. Darüber hinaus müssen zivile und militärische Strukturen im Bereich der Cybersicherheit synchronisiert werden, damit im Ernstfall eine abgestimmte Reaktion sowie ein einheitliches Lagebild möglich ist. Resultierend aus der Tatsache, dass strategische- und opportunistische Muster im Cyberraum vorhanden sind, muss eine allgemein hohe Sicherheitsmaturität erreicht werden.

Das VBS ist, im Verbund mit seinen Partnern, bei Bund und Kantonen, Wirtschaft und Hochschulen sowie bei Bedarf internationalen Partnern, für die Cyberdefence der Schweiz zuständig. Es analysiert und antizipiert zudem Herausforderungen und Bedrohungen im Cyberraum und erbringt diverse Sicherheitsleistungen im Umgang mit Cybervorfällen (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS 2021). Somit werden sowohl der militärische wie auch vorwiegend der nachrichtendienstliche Anteil der Cybersicherheit in der Schweiz durch das VBS organisiert (vgl. Kapitel 2). Der zivile Bereich, also vorwiegend die privatisierten kritischen Infrastrukturen, handeln mehrheitlich selbstverantwortlich. Die Schnittstelle in die Wirtschaft – und somit der dritte nach (Saalbach 2019) genannte Bereich – wird teilweise durch die MELANI (NCSC) abgedeckt. Speziell in diesem Bereich sind viele liberale sowie föderale Aspekte erkennbar, weshalb der Dienst an der Wirtschaft und der Öffentlichkeit kaum über Empfehlungen und Beratungen hinausgeht. Die Armee beschreibt in der «Gesamtkonzeption Cyber» alle Fähigkeiten, die es braucht, um die armeeeignen Verbände, Infrastrukturen und Netze gegen Bedrohungen im Cyber- und Elektromagnetischen Raum (CER) über alle Lagen zu schützen, unabhängig davon, ob es sich um technisches Versagen, menschliches Versagen oder Umwelteinflüsse handelt (Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS 2022). In der Schweizer Wirtschaft kann als Beispiel für einen Verbund zur Erhöhung der Sicherheitsmaturität das Secure Swiss Finance Network genannt werden, welches von der SIX Group und der Schweizerischen Nationalbank initiiert und umgesetzt wurde. (SIX Group 2021). Der Umstand, dass die hoch fragmentierte und hauptsächlich aus KMUs bestehende Schweizer Wirtschaft nicht die Möglichkeit hat, vergleichbare Anstrengungen im Bereich der Cybersicherheit zu unternehmen, wurde erkannt, und Ideen scheinen sich zu entwickeln. Das Fehlen von Sicherheitspatches und Updates als Folge von Strafmassnahmen wie z. B. Exportkontrollen, Sanktionen etc. können Cyberrisiken steigern; dies ist darauf zurückzuführen, dass die Angriffsfläche auf eine künstliche Art und Weise erhöht wird (vgl. Kapitel 4).

Ein Auslieferungsstopp von sicherheitsrelevanter Technik kann auch entstehen, wenn die Schweiz nicht am Konflikt des Technologieexporteures beteiligt ist (z. B., Lieferkettenprobleme, Exportkontrollen etc.). Der High-Tech-Sektor in der Schweiz ist stark abhängig von aus dem Ausland importierten Technologieprodukten. In solchen Szenarien kommt der Gedanke von souveräner Technologie auf, um die Abhängigkeit von Technologieunternehmen in kritischen Lagen einzugrenzen

«Das Fehlen von Sicherheitspatches und Updates als Folge von Strafmassnahmen wie z. B. Exportkontrollen, Sanktionen etc. können Cyberrisiken steigern; dies ist darauf zurückzuführen, dass die Angriffsfläche auf eine künstliche Art und Weise erhöht wird.»

oder zumindest zu verteilen. Die EU initiiert mit dem European Chips Act (European Union 2019) den Fähigkeitsaufbau Mikrochips lokal herzustellen. Die Frage dabei ist, bis zu welcher Ressource die Lieferkette von Non-EU Ländern unabhängig werden kann.
Zusammenfassend wollten wir eine Einführung in die Termini Cyberkrieg und Cybersicherheit, Cyberkonstrukte und -organisationen, so wie sie die Staaten USA und Russland aufgebaut haben, sowie einen Einblick in vergangene Cyberattacken und -vorfälle geben, aber auch den Einsatz von Cybermitteln parallel zum andauernden Konflikt in der Ukraine erarbeiten. Als Konsequenz in Bezug auf die Schweiz erkennen die Autoren vier Punkte:

1. Es existiert kein einheitliches Verständnis, wann der Begriff Cyberkrieg auf einen Vorfall angewendet werden kann oder sogar muss.
2. Cyberattacken sind selten ein «Staat-gegen-Staat-Konflikt». Aktivisten, Gruppen und Opportunisten beteiligen sich daran, entweder aus Überzeugung, monetären Motiven oder auch aus technischer Neugierde. Sie fokussieren sich dabei nicht unbedingt auf Staatsstrukturen, sondern haben sämtliche Zielen im Cyberraum im Visier.
3. Daraus resultiert, dass im ganzen Land eine hohe Sicherheitsmaturität erreicht werden muss. Dieses Ziel kann effektiver und effizienter in Verbünden erreicht werden.
4. Die Gefahren, die von Technologiesanktionen und die damit resultierenden Sicherheitslücken ausgehen, müssen vermehrt in den Fokus der Debatte gerückt werden.

«Der Ukrainekrieg wird voraussichtlich nicht als erster Cyberkrieg von Europa in die Geschichte eingehen. Viel mehr wird durch diesen Konflikt verdeutlicht, welche strategische Bedeutung der Cyberraum in zukünftigen Konflikten haben muss – also, wo die operativen Chancen und Risiken im Kontext eines hybriden Gefechts liegen.»

Der Ukrainekrieg wird voraussichtlich nicht als erster Cyberkrieg von Europa in die Geschichte eingehen. Viel mehr wird durch diesen Konflikt verdeutlicht, welche strategische Bedeutung der Cyberraum in zukünftigen Konflikten haben muss – also, wo die operativen Chancen und Risiken im Kontext eines hybriden Gefechts liegen. ◆

Endnoten

1 Der vorliegende Artikel wurde bereits in der Mai 2022 Ausgabe des SwissIT Magazins in einer verkürzten Version veröffentlicht.
2 Als Department of Defense (DoD) wird das Verteidigungsministerium der Vereinigten Staaten bezeichnet.
3 «Preservation of confidentiality, integrity and availability of information in the Cyberspace.» (Organization 2012)
4 «The ability to protect or defend the use of cyberspace from cyber attack.» (Kissel 2013)
5 STUXNET ist die Bezeichnung für eine Malware, welche dafür eingesetzt wurde, Zentrifugen in einer Iranischen Einrichtung zu beschädigen.
6 Cyberattacken auf ein Ziel mit einem ganz bestimmten Zweck in einem vordefinierten Zeitfenster sind äusserst filigran und erfordern eine akribische Vorbereitung die zeitlich nicht einheitlich schätzbar sind.
7 Medienunternehmen, die Finanzwelt und private finanzkräftige Unternehmen oder Einzelpersonen sind Ziele von opportunistisch gesinnten Gruppen.

Literaturverzeichnis

Aditya, S. und E. Richard (2013). Targeted Cyberattacks: A Superset of Advanced Persistent Threats.

Aid, M.. Inside the NSA's Ultra-Secret China Hacking Group – Foreign Policy. (URL https://foreignpolicy.com/2013/06/10/ inside-the-nsas-ultra-secret-china-hacking-group/,).

Andress, J. und S. Winterfeld (2011). Chapter 1 – What is Cyber Warfare? (URL https://www.sciencedirect.com/science/article/pii/B9781597496377000010).

Antoniuk, D. (2022, 4). A deeper look at the malware being used on Ukrainian targets. (URL https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/,).

Bernstein, D., T. Lange und R. Niederhagen (2016). Dual EC: A standardized back door. Carr, J. (2011, 2). Real Cyber Warfare: Carr's Top Five Picks. (URL https: //www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks/?sh=79281ba82ef5,).

Craigen, D., N. Diakun-Thibault und R. Purse (2014). Defining cybersecurity. Technology Innovation Management Review 4.

Denys, S. und M. Wiktor (2022). Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine. – .

Dorn, F., N. Potrafke und M. Schlepper (2022). Zeitenwende in der Verteidigungspolitik? 100 Mrd. Euro Sondervermögen für die Bundeswehr – (k) ein grosser Wurf. ifo Schnelldienst 75, 37–45.

Dwyer, J. und K. Henson (2022, 3). New Wiper Malware Used Against Ukranian Organizations. (URL https://securityintelligence.com/posts/new-wiper-malware-used-against-ukranian-organizations/,).

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2021). Die Strategie Cyber VBS.

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (2022). Gesamtkonzeption Cyber.

Emm, D., R. Unuchek, M. G. ad Alexander Liskin, D. Makrushin und F. Sinitsynr (2016). IT threat evolution in Q3 2016. Kaspersky Labs, Moscow, Russia, Tech. Rep.

European Union (2019). European Chips Act. (URL https:// ec.europa.eu/ info/strategy/priorities-2019-2024/europe-fit-digital-age/ european-chips-act_en/,).

Fierro, C. D. (2022a, 3). CaddyWiper: Third Wiper Malware Targeting Ukrainian Organizations. (URL https://securityintelligence.com/posts/ caddywiper-malware-targeting-ukrainian-organizations/,).

Fierro, C. D. (2022b, 2). New Destructive Malware Used In Cyber Attacks on Ukraine. URL https://securityintelligence.com/posts/ new-destructive-malware-cyber-attacks-ukraine/,).

Gabriella, C. (2013, 9). Anonymous in Context: The Politics and Power behind the Mask. INTERNET GOVERNANCE PAPERS, 11.

Gazula, M. B. (2017). Cyber warfare conflict analysis and case studies.

Geers, K., D. Kindlund, N. Moran und R. Rachwald (2014). World War C: Understanding World War C: Understanding Today's Advanced Cyber Attacks.

Goud, N. (2022). Microsoft to stop Windows security updates in Russia – Cybersecurity Insiders. (URL https://www.cybersecurity-insiders.com/ microsoft-to-stop-windows-security-updates-in-russia/,).

Haizler, O. (2017). The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. Cyber, Intelligence, and Security 1, 31–45.

Hales, T. (2013). The NSA back door to NIST. Notices of the AMS 61, 190–192. Harding, L. (2022, 2). Anonymous: the hacker collective that has declared cyberwar on Russia — Ukraine — The Guardian. (URL https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia,).

Harry, H. (2014). The philosophy of Anonymous: Ontological politics without identity. Radical Philosophy 176.

Haucap, J. (2022). Zeitenwende. Perspektiven der Wirtschaftspolitik 23, 1–2. Hunker, J. (2010). Cyber war and cyber power. Issues for NATO doctrine.

Kabay, M. (2012). History of computer crime. Computer security handbook, 1–2.

Kissel, R. (2013, 5). Glossary of key information security terms. URL https://nvlpubs. nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf,).

Knake, R. K. und R. A. Clarke (2012). Cyber war: the next threat to national security and what to do about it. The ECSSR.

Loleski, S. (2019, 1). From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers. Intelligence and National Security 34, 112–128. URL https://doi.org/10.1080/02684527.2018.1532627,). DOI: 10.1080/02684527.2018.1532627.

Maschmeyer, L. und M. D. Cavelty (2022). Goodbye Cyberwar: Ukraine as Reality Check. Policy Perspectives 10, 3.

Mikalauskas, E. (2021). Buying your own malware has never been easier. Mohee, A. (2022). Cyber war: The hidden side of the Russian-Ukrainian crisis. Olivia, S. und E. Stevan (2022). Hacktivism's Threat to Cyber Security Today.

Organization, I. S. (2012). ISO/IEC 27032:2012(en), Information technology — Security techniques — Guidelines for cybersecurity.

Patrick, O. (2022). Ukraine: The Cyber Battlefield.

Pernik, P., J. Wojtkowiak und A. Verschoor-Kirss (2016). National cyber security organisation: United States. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Pierluigi, P. (2022, 2). White House and UK Gov attribute DDoS attacks on Ukraine to Rus- sia's GRU. (URL https://securityaffairs.co/wordpress/128174/ cyber-warfare-2/russia-gru-ddos-ukraine.html,).

Reed, J. (2022, 5). AcidRain Malware Shuts Down Thousands of Modems in Ukraine. (URL https://securityintelligence.com/news/ acidrain-malware-modems-ukraine-germany/,).

Saalbach, K.-P. (2019, 7). Cyberwar: Grundlagen-Methoden-Beispiele.

Schmitt, M. N. (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Serpanos, D. und T. Komninos (2022). The Cyberwarfare in Ukraine. Computer 55, 88–91. Shimomura, T. und J. Markoff (1995). Takedown: the pursuit and capture of Kevin Mitnick, America's most wanted computer outlaws-by the man who did it. Hyperion Press.

Singer, P. W. und A. Friedman (2014). Cybersecurity and Cyberwar: What everyone needs to know. oup usa.

SIX Group (2021). Secure Swiss Finance Network - Für eine sichere, flexible und resiliente Datenkommunikation. URL https://www.six-group.com/de/ products-services/ banking-services/ssfn.html/,).

Stoll, C. (2005). The cuckoo's egg: tracking a spy through the maze of computer espionage. Simon and Schuster.

Strepkov (2022, 2). Hackers hacked into the equipment control of the Selyatino agro-hub and tried to spoil 40,000 tonnes of frozen pro- ducts. (URL http://asorps.ru/novosti/news_post/hakery-vzlomali-upravlenie-oborudovaniem-agrohaba-selyatino-i-pytalis-is).

Tan, Y. (2016). GPU-Based Random Number Generators. Gpu-Based Parallel Implementation of Swarm Intelligence Algorithms, 147–165.

Ware, W. H. (1967). Security and Privacy in Computer Systems. S. 279–282. Association for Computing Machinery. URL https://doi.org/10.1145/1465482.1465523,).

Yost, J. R. (2007, 1). A history of computer security standards.

@YourAnonTV (2022, 3). Anonymous war. URL https://twitter.com/YourAnonTV/ status/1506769001040551937,).