Kapitel 11 Die Cyberdimension in Russlands Angriffskrieg gegen die Ukraine

Arthur de Liedekerke und Kira Frankenthal

Abstract: Der russische Angriffskrieg gegen die Ukraine in 2022 ist weltweit einer der ersten konventionellen Konflikte zwischen zwei Staaten mit fortgeschrittenen Cyberfähigkeiten. Auch wenn die Cyberdimension des Kriegs auf den ersten Blick von geringem Ausmaß erscheint, so ist die Ukraine durchgehend von Cyberangriffen und der Verbreitung von Desinformationen betroffen. Dennoch hat sich die Cyberlage nicht so entwickelt, wie viele Experten es erwartet hatten. Dieses Kapitel befasst sich mit den bisher wichtigsten Entwicklungen, erläutert Ursachen für die Standhaftigkeit der ukrainischen Cybersicherheit und zeigt auf, was im Cyberspace zu erwarten ist, wenn der Krieg weiter fortschreitet.

Schlüsselwörter: Russland-Ukraine-Krieg, Cyberangriffe, Desinformation, Deepfakes, Cyberabwehr, BSI, ENISA

1. Einleitung

Cyberangriffe sind seit geraumer Zeit Teil der modernen Kriegsführung. Tatsächlich betrachten die Russen cybergestützte Operationen sowohl als „einen Arm der russischen Propagandamaschine und ein Mittel zur Schaffung und Verbreitung von Desinformationen, sowie als ein Werkzeug zur Störung der kritischen Infrastruktur oder der militärischen Fähigkeiten eines Gegners".[1]

Angesichts der Anfang 2022 drohenden Invasion warnten Experten vor Russlands ausgeprägten Cyberfähigkeiten. Diese hätten das Potenzial, eine neue Welle von Cyberangriffen auf die Ukraine zu entfesseln, die sich möglicherweise auch auf den Rest der Welt auswirken würde. Seit Beginn des Kriegs lassen sich jedoch entgegengesetzte Einschätzungen über den Charakter und die Bedeutung der Cyberdimension in Russlands Krieg

1 Zitat im Original englisch. Siehe Willet, Marcus: The Cyber Dimension of the Russia-Ukraine War, International Institute for Strategic Studies, 6. Oktober 2022.

gegen die Ukraine beobachten, die von „Cyberkrieg in vollem Umfang" bis hin zu „auffallend abwesend" reichen.

2. *Die Rolle von cybergestützten Operationen in Russlands Krieg gegen die Ukraine in 2022*

Die Ukraine ist nicht erst seit dem 24. Februar 2022 von russischen Cyberoperationen betroffen. Schon seit der Besatzung der Krim im Jahr 2014 hat sich der Kreml u. a. in Kommunalwahlen eingemischt, die kritische Infrastruktur der Ukraine angegriffen, erfolgreich Regierungswebsites kompromittiert und Desinformationen verbreitet.

Seit Jahren ist die Ukraine eine Art Testobjekt für russische Cyberangriffe. Die teilweise sehr fortschrittlichen Cyberwaffen waren mitunter besonders wirkungsvoll und in vielerlei Hinsicht beispiellos. So legte z. B. die *BlackEnergy-Malware* im Jahr 2015 das Kyjiwer Stromnetz lahm und löste dadurch mitten im Winter einen großen Stromausfall aus.[2] Diese und andere verheerende Vorfälle in den folgenden Jahren, wie der Wurm *NotPetya*[3], sind Teil der langjährigen Bemühungen Moskaus, seinen Nachbarn zu destabilisieren, Kyjiws Handlungsfähigkeiten zu schädigen und einen entscheidenden Vorsprung im Cyberraum zu behalten.

Bereits im Vorfeld der groß angelegten militärischen Offensive intensivierte Russland seine digitalen Angriffe auf ukrainische Ziele. Ein Ende April 2022 veröffentlichter Microsoft-Bericht bestätigt, dass Russland-nahe Akteure vermutlich bereits seit März 2021 entsprechende Vorbereitungen trafen.[4] So wurden z. B. seit Ende 2021 regelmäßig Websites von Regierungsinstitutionen entstellt. Hacker, die direkt vom Kreml gesponsert wurden oder sehr stark mit dessen Interessen verbunden waren, setzten u. a. zerstörerische *Malware* – insbesondere Datenlöschprogramme – auf Regierungsnetzwerke, einschließlich des Außenministeriums der Ukraine, frei. Nicht zuletzt wurde am 14. Januar 2022 eine ominöse Warnung auf offizi-

2 Zetter, Kim: „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", WIRED, 3. März 2016.

3 *NotPetya*, abgeleitet von der 2016 erstmals aufgetauchten *Petya-Malware*, war eine hochgradig zerstörerische Erpressungssoftware (*Ransomware*), die erstmals gegen die Ukraine eingesetzt wurde und Mitte 2017 Tausende von Unternehmen weltweit betraf. Viele Länder haben seitdem die russische Regierung beschuldigt, hinter diesen Angriffen zu stecken.

4 Digital Security Unit: Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine, Microsoft, 27. April 2022.

ellen ukrainischen Websites verbreitet: „Habt Angst und erwartet das Schlimmste".[5] Nur ein paar Stunden vor dem Einmarsch in die Ukraine griff Russland erneut eine Reihe wichtiger Einrichtungen im Land an was dazu führte, dass die Computersysteme mehrerer Regierungs-, Militär- und kritischer Infrastrukturbereiche stark in ihrer Funktionsfähigkeit eingeschränkt wurden. Dies ähnelte in vielerlei Hinsicht den Angriffen, die Russland 2008 gegen Georgien und 2014 im Rahmen des Überfalls auf die Krim durchgeführt hatte.[6]

Seit Beginn des Kriegs im Februar 2022 erhöhte sich die Zahl der Cyberangriffe noch einmal deutlich. Dabei konnte der Einsatz einer ganzen Bandbreite von russischen Cyberwaffen beobachtet werden: *Wiper-Malware*, *Distributed Denial of Service* (DDoS; Überflutung eines Servers mit Internetverkehr, um zu verhindern, dass Nutzer auf die betreffende Website zugreifen), *Phishing*-Kampagnen und vor allem die Unterbrechung satellitengestützter Internetdienste – die inzwischen berüchtigte Sabotageaktion, die Russland zugeschrieben wird[7] und durch die das KA-SAT-Netz von *Viasat*, auf das das ukrainische Militär, der Geheimdienst und die Polizei angewiesen sind, teilweise vom Netz genommen wurde.[8]

Mit dem Fortschreiten des Kriegs hat der Kreml seine Cyberoperationen weiter verstärkt, insbesondere solche, die kritische Infrastrukturen angreifen. Eine russische Cyberoperation gegen *Ukrtelecom* – einen großen nationalen Telekommunikationsbetreiber – legte Ende März die Kommunikationsdienste in der Ukraine für mehrere Stunden lahm.[9] Anfang April wurde *Industroyer2*, eine verbesserte Variante einer Malware, die 2016 Stromausfälle in Kyjiw verursacht hatte, auf den Systemen eines der größten Energieversorger des Landes identifiziert und neutralisiert.

Zusätzlich zu den Cyberangriffen konnten zahlreiche anhaltende und groß angelegte Desinformationskampagnen und Informationsoperationen beobachtet werden. Auch diese greifen auf die Möglichkeiten des Cyberspace hinsichtlich der Verbreitung und der Geschwindigkeit des Aus-

5 Harding, Luke: „Ukraine hit by ‚massive' cyber-attack on government websites", The Guardian, 14. Januar 2022.

6 Willet, The Cyber Dimension of the Russia-Ukraine War, 6. Oktober 2022.

7 Rat der Europäischen Union: Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, 10. Mai 2022.

8 Pearson, James/Satter, Raphael/Bing, Christopher/Schectman, Joel: „Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say", Reuters, 12. März 2022.

9 Vallance, Chris: „Ukraine war: Major internet provider suffers cyber-attack", BBC, 28. März 2022.

tauschs von Inhalten zu. Ergänzt wurde dies durch traditionelle Propaganda mit inszenierten Szenen in den russischen Medien und einer strengen Kontrolle der Berichterstattung in der Presse und auf anderen Medienplattformen. Mithilfe von relativ neuen Technologien wurden zudem *Deep-fakes* – manipulierte Videos und Audiodateien – im Internet verbreitet, darunter gefälschte Clips vom ukrainischen Präsidenten Wolodymyr Selenskyj sowie dem russischen Machthaber Wladimir Putin.[10] Das Ziel war es, Chaos zu stiften, die Ukraine zu destabilisieren und ihre Cyberabwehr zu erschöpfen, um damit Russlands konventionelle Operationen zu unterstützen.

Dennoch erwarteten die meisten Experten weitaus größere Störungen oder gar ein noch nie dagewesenes Ausmaß an „*shock and awe*"[11]. Die Tatsache, dass dies zum Zeitpunkt der Fertigstellung dieses Kapitels[12] so nicht eingetreten ist, sollte nicht dazu verleiten, den doch bereits entstandenen Schaden herunterzuspielen. Denn, das Tempo und die kumulative Wirkung dieser Angriffe hatten doch einen sehr disruptiven Effekt. Zudem kann davon ausgegangen werden, dass viele Vorfälle im Rahmen verdeckter operativer Aktivitäten entweder unentdeckt blieben oder nicht gemeldet wurden. Dennoch haben wir es nicht mit einem Vorfall katastrophalen Ausmaßes zu tun, einem „Cyber-Pearl-Harbour", der ganze Teile der kritischen Infrastruktur oder lebenswichtige Kommando- und Kontrollsysteme der Ukraine in die Knie zwingt. Das Ausmaß der russischen Cyberangriffe seit Beginn des Kriegs ist weit entfernt von dem, was vorhergesagt wurde und hat Moskau wenn überhaupt eher einen geringen strategischen Nutzen für seine Kriegsziele gebracht.

3. Der Cyber-Widerstand der Ukraine

Zu den Ursachen der eher eingeschränkten Auswirkungen von russischen Cyberoperationen im Krieg gegen die Ukraine kursieren verschiedene Thesen:

---

10 Simonite, Tom: „A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be", WIRED, 17. März 2022.

11 *Shock and Awe* ist eine militärische Strategie, die darauf abzielt, den Gegner bereits zu Beginn eines Konflikts durch den Einsatz überwältigender Gewalt (in diesem Fall in Form von Cyberangriffen) in „Angst und Schrecken" zu versetzen, um dadurch dessen Widerstandswillen zu brechen. HarperCollins: Shock and Awe, 2022.

12 Dieser Beitrag wurde im November 2022 eingereicht.

Erstens, die Fähigkeit der Ukraine sich effektiv gegen die Flut verschiedener Cyberangriffe zu wehren bzw. diese einzudämmen, ist u. a. das Ergebnis der unmittelbaren Erfahrungen, die das Land in acht Jahren Krieg gegen den Kreml und seine Stellvertreter gesammelt hat. Die ständige Bedrohung durch vom Kreml gesponserte Cyberakteure führte dazu, dass die Ukraine sich seit 2014 intensiv auf potenzielle Gefahren aus dem Cyberbereich vorbereiten konnte – wie z. B. mit einer Cybersicherheitsstrategie, einem Cybersicherheitsgesetz, einer Umgestaltung ihrer Nachrichtendienste sowie verstärkten Fähigkeiten zur Reaktion auf Vorfälle beim CERT-UA (Computer Emergency Response Team of Ukraine).

Zweitens spielt die Unterstützung, die die Ukraine von NATO-Verbündeten und Industriepartnern erhalten hat, eine wichtige Rolle. Wie der Direktor der Nationalen Sicherheitsbehörde und des US-Cyberkommandos, General Paul Nakasone, selbst zugab, reiste im Dezember 2021 ein „*Hunt-Forward*"-Team der *Mission Force* in die Ukraine, um beim Aufbau der Widerstandsfähigkeit gegen Cyberangriffe zu helfen.[13] Große Technologieunternehmen des privaten Sektors waren von Beginn der Kampfhandlungen an sehr proaktiv und boten ihre Fähigkeiten zur Verteidigung der Ukraine an. Dazu gehörte die Migration von Daten und Diensten der ukrainischen Regierung auf verteilte *Cloud-Server* und die kontinuierliche Bereitstellung von Bedrohungsdaten. Diese enge Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor und sogar die Beteiligung von gemeinnützigen Organisationen im Rahmen einer „gesamtgesellschaftlichen Reaktion" hat die ukrainische Regierung bei der Stärkung ihrer Cyber-Resilienz erheblich unterstützt.

Drittens wird davon ausgegangen, dass die Massenmobilisierung ukrainischer (und schließlich internationaler) freiwilliger Hacker und patriotischer Programmierer – viele unter dem Banner der „IT-Armee" – einen Beitrag zur Gegenoffensive geleistet hat. Mit einem Talentpool von bis zu 300.000 Fachleuten im Vorfeld des Kriegs konnte sich Selenskyj somit auf viele technisch versierte Männer und Frauen verlassen, die als zweite Verteidigungslinie fungierten.[14]

Viertens hat Russland es versäumt, Cyberoperationen sinnvoll in seine konventionellen Operationen zu integrieren. Moskau hat bisher noch keine Cyberoperationen in einer Weise eingesetzt, die eindeutig mit militä-

13 Smalley, Suzanne: „Nakasone says Cyber Command did nine ‚hunt forward' ops last year, including in Ukraine", CyberScoop, 4. Mai 2022.

14 Mäder, Lukas: „Im Ukraine-Krieg kämpft eine ‚IT-Armee' online gegen Russland. Die Freiwilligen attackieren sogar Apotheken und Universitäten", Neue Züricher Zeitung, 23. Juli 2022.

rischen Einheiten koordiniert und darauf ausgelegt ist, den Vormarsch von Boden- oder Luftstreitkräften zu erleichtern. So haben russische Cybereinheiten bspw. die Stromversorgung oder Internetverbindungen in der Ukraine noch nicht – etwa unmittelbar vor einer Offensive – in großem Umfang lahmgelegt. In einem Artikel in *Foreign Affairs* weist der stellvertretende NATO-Generalsekretär für Nachrichtendienste und Sicherheit, David Cattler, auf Russlands „missteps and struggles" hin, die mit ziemlicher Sicherheit dazu führten, dass Russland bislang nicht in der Lage war, sein Cyberprogramm zur Unterstützung seiner konventionellen Streitkräfte in vollem Umfang einzusetzen.[15]

Schließlich vermuten einige Experten, dass Russland seine Angriffe taktisch zurückgehalten hat, um zu vermeiden, dass bestimmte strategische Gegebenheiten offengelegt werden. Die limitierten Angriffe könnten aber auch damit zusammenhängen, dass Russland vorsichtig ist, massive Auswirkungen – auch über die Ukraine hinaus – zu verursachen, die eine Reaktion des Westens auslösen könnten.[16] Von Moskau willkürlich verursachte Schäden, die sich weit über das Kriegsgebiet hinaus ausbreiten und an *NotPetya* erinnern, könnten die NATO in den Kampf hineinziehen. Das Bündnis erklärte, dass nicht nur ein äußerst schädlicher Cyberangriff auf ein Mitglied des Bündnisses Artikel 5 auslösen könnte, sondern auch eine Häufung kleinerer Angriffe (die von Fall zu Fall beurteilt werden).

4. Die Auswirkungen der russischen Cyberangriffe auf Europa und Deutschland

Neben den direkten Auswirkungen auf die Ukraine, konnte auch eine gewisse Ausweitung russischer Cyberaktivitäten auf andere Länder beobachtet werden.[17]

Ein Bericht von *Moody's Investors Service* im Oktober 2022 stellte fest, dass der russische Einmarsch in die Ukraine zu einem erheblichen Anstieg

15 Cattler, David/Black, Daniel: „The Myth of the Missing Cyberwar", Foreign Affairs, 6. April 2022.

16 De Liedekerke, Arthur/Laudrain, Arthur: Russia's Cyber War: What's Next and What the European Union Should Do, Council on Foreign Relations, 30. März 2022.

17 Sabbagh, Dan: „Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief", The Guardian, 10. Mai 2022.

an Cyberangriffen in der EMEA-Region[18] beigetragen hat.[19] Auch wenn die Angriffe intensiver und raffinierter geworden sind, betonte Juhan Lepassaar, Direktor der Agentur der Europäischen Union für Cybersicherheit (ENISA), dass es trotz einer „herausfordernden" Bedrohungslandschaft keine „radikale Veränderung der Cyberbedrohungen" gegeben habe.[20]

Auch Deutschland ist von den Auswirkungen des Konflikts im Cyberbereich nicht verschont geblieben. Am 15. März warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) Nutzer vor der Anwendung jeglicher vom Moskauer Softwareentwickler *Kaspersky Lab* entwickelter Sicherheitssoftware. Diese berge ein erhöhtes Risiko, von russischen Behörden dazu angehalten zu werden, sich in die Netzwerke der Kunden einzuhacken.[21] Wenige Tage später schaltete ein Cyberangriff auf die Bodeninfrastruktur des *KA-SAT*-Netzes Tausende von Windkraftanlagen im Lande ab.[22] Mitte Oktober wurden bei einem Vorfall mit vermuteter russischer Beteiligung die Glasfaserkabel des staatlichen Bahnkonzerns Deutsche Bahn durchtrennt, wodurch der Zugverkehr für drei Stunden zum Erliegen kam.[23] Obwohl es sich dabei letztlich um einen eher physischen Akt handelte, unterstrich dieser Vorfall die Menge an frei verfügbaren Online-Informationen über die kritischen Systeme in Deutschland.

Auch wenn Deutschland nach Angaben der Bundesregierung im Vergleich zu anderen europäischen Partnern von russischen Angriffen relativ verschont geblieben ist[24], haben diese Ereignisse das Bundesministerium des Innern und für Heimat (BMI) im Juli dazu veranlasst, eine neue Cybersicherheitsagenda vorzulegen.[25]

---

18 EMEA bezeichnet im Englischen den Wirtschaftsraum „**E**urope", „**M**iddle **E**ast" und „**A**frica".

19 Xiao, Menghan: „Cyberattacks accelerating in Europe, Moody's says", SC Media, 17. Oktober 2022.

20 Kabelka, Laura: „EU's cybersecurity agency chief warns to keep guard up", Euractiv, 27. September 2022.

21 Nasr, Joseph: „Germany issues hacking warning for users of Russian anti-virus software Kaspersky", Reuters, 15. März 2022.

22 Burgess, Matt: „A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", WIRED, 23. März 2022.

23 Hoyer, Katja: „Germans are under attack. Can they adapt?", The Washington Post, 25. Oktober 2022.

24 Kabelka, Laura: „Germany still not affected by Russia-linked cyberattacks", Euractiv, 6. Mai 2022.

25 Deutsche Welle: „Germany bolsters defenses against Russia cyber threat", 12. Juli 2022; Bundesministerium des Innern und für Heimat: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode, Juni 2022.

5. Erste Lehren

Es wäre verfrüht, auf der Grundlage des zum Zeitpunkt der Fertigstellung dieses Beitrags noch laufenden Krieges endgültige Schlussfolgerungen zu ziehen. Nichtdestotrotz können aus den bisherigen Aktivitäten im Cyberspace erste wichtige Lehren gezogen werden.

Der Krieg in der Ukraine sollte Experten dazu veranlassen, das Konzept Cyberkrieg bzw. die Rolle des Cyberraumes in einem konventionellen Krieg neu zu bewerten. Es ist wahrscheinlich, dass die Erwartungen an „shock and awe" unrealistisch waren. Dennoch kann die sich derzeit in der Ukraine entfaltende Situation ein fundiertes Beispiel für den Beitrag des Internets zu einem konventionellen Konflikt liefern. Vor allem die beeindruckende Cyberabwehr der Ukraine könnte Deutschland und anderen europäischen Ländern als Vorbild für die eigene Verteidigung im Cyberbereich dienen. Dabei spielen besonders Technologieunternehmen eine entscheidende Rolle, die mit ihren High-End-Fähigkeiten wertvolle Erkenntnisse aus einer riesigen Menge verarbeiteter Daten gewinnen können. Aber auch die Notwendigkeit einer engeren Zusammenarbeit öffentlicher und privater Akteure sowie die Unterstützung durch Verbündete sollte nicht unterschätzt werden. Hierfür könnten Regierungen z. B. die Einrichtung von sogenannten „Datenbotschaften"[26] im Ausland in Betracht ziehen.

Westliche Beobachter sollten jedoch nicht davon ausgehen, dass die Strategie mit der Kyjiw Russlands Angriffe im Cyberspace so erfolgreich abgewehrt hat, auf einfache Weise auf die eigenen Länder übertragen werden könne. Viele Aspekte sind spezifisch für den ukrainischen Kontext:

- Erstens ist die Ukraine in der Lage, auf eine hohe Anzahl komplexer Cyberangriffe von verschiedenen staatlichen und staatlich geförderten Akteuren zu reagieren und diese zu entschärfen. Das ist u. a. das Ergebnis der direkten Erfahrungen, die das Land in acht Jahren Krieg gegen den Kreml und seine Stellvertreter gesammelt hat.
- Zweitens stellt die Massenmobilisierung ukrainischer freiwilliger Hacker und patriotischer Programmierer eine Besonderheit dar. Selenskyj konnte sich auf eine gesamtgesellschaftliche Reaktion stützen, bei der sich neben der Regierung auch der private Sektor und gemeinnützige Organisationen an den Verteidigungsanstrengungen beteiligten. Dies

26 Die Einrichtung von Datenbotschaften ist ein innovativer Ansatz, der zuerst von den Esten erforscht wurde. Das Konzept zielt darauf ab, die digitale Kontinuität von Nationalstaaten durch staatliche Serverressourcen außerhalb ihrer Landesgrenzen zu gewährleisten.

ist zum großen Teil dem Status der Ukraine als globales „IT-Powerhouse" zu verdanken, einer lebendigen digitalen Zivilgesellschaft sowie einer Tradition des Aktivismus. In vielen westlichen Ländern würde der Einsatz einer solchen „IT-Armee" jedoch unter Umständen auf erhebliche Hürden stoßen – einschließlich rechtlicher und ethischer Vorbehalte aufgrund von Datenschutz- und Sicherheitsrisiken für potenzielle Kollateralopfer der Angriffe von Hackerkollektiven.

- Drittens spielen auch die „Informationsoperationen" rund um den Kriegsschauplatz eine entscheidende Rolle. Der Erfolg der Ukraine kann u. a. darauf zurückgeführt werden, dass sie mit den russischen Desinformationskampagnen vertraut ist und auf diese entsprechend reagieren kann. Dabei kommt vor allem der effektiven Nutzung von Sozialen Medien eine große Bedeutung bei der Streuung von Gegennarrativen zu. Hinzu kommt die Fähigkeit der Ukrainer, in der russischen Sprache kommunizieren zu können. So wandte sich bspw. Selenskyj selbst am Vorabend der Invasion mit seiner Botschaft direkt an das russische Volk – und zwar auf Russisch.[27]

6. Fazit

Auch wenn sich die bisherigen Entwicklungen und Auswirkungen im Bereich der Cyberkriegsführung im Rahmen halten, wäre es ein großer Fehler euphorisch zu sein. Ein in die Enge getriebenes Russland, das mit einer Reihe von Niederlagen auf dem Schlachtfeld konfrontiert ist und wenige andere Optionen auf dem Tisch hat – die nukleare Dimension einmal ausgeschlossen – wird vermutlich verstärkt auf den Cyberraum zurückgreifen. Dieser wird sich als ideale Grundlage erweisen, um eine Isolation zu umgehen, westliche Verteidigungspläne auszuspionieren und zu stören, Technologie und geistiges Eigentum zu stehlen sowie globale Unruhen zu verstärken.

Nachdem die westlichen Staaten ihre Unterstützung für die Ukraine in den letzten Monaten verstärkten, konnten eine Reihe von „Strafmaßnahmen" durch russische Cyberakteure gegen bestimmte Länder beobachtet

27 Für weitere Einzelheiten siehe: De Liedekerke, Arthur/De Rivoire, Hector: „Ukraine's cyber resistance is impressive – but hard to replicate", euobserver, 26. September 2022.

werden – vor allem in Finnland[28], Estland[29] und Montenegro[30]. Diese Einschätzung wird von der im November veröffentlichten *ENISA Threat Landscape 2022* geteilt, die davon ausgeht, dass westliche bzw. NATO-Verbündete (insbesondere Einrichtungen der kritischen Infrastruktur) mit hoher Wahrscheinlichkeit als Teil von Vergeltungsmaßnahmen verstärkt ins Visier genommen werden.[31]

Je mehr westliche Unternehmen sich aus Russland zurückziehen – eine Art strategische Entkopplung – desto mehr Anreize hat Russland, Cyberwaffen gegen Unternehmen und andere Staaten einzusetzen. Selbst wenn Moskau einer Art Waffenstillstand zustimmt, wäre der verstärkte Einsatz von Cyberangriffen und Desinformationskampagnen eine der wenigen zur Verfügung stehenden Möglichkeiten, um der Ukraine und dem Westen in einer Art Grauzone – dann wieder unterhalb der Schwelle einer direkten Konfrontation – Schaden zuzufügen.

Langfristig werden jedoch verlorene Investitionen, ein eingeschränkter Zugang zu Schlüsseltechnologien sowie grundsätzliche Einschränkungen der russischen Wirtschaft die Fähigkeit Russlands, einen Krieg im Cyberraum zu führen, stark beeinträchtigen. Die Entschlossenheit des Westens und die Unterstützung anderer gleichgesinnter Partner bei der Aufrechterhaltung der notwendigen Sanktionen werden entscheidend dazu beitragen, die Fähigkeiten von Putins Cyberarmee zu drosseln.

Literaturverzeichnis

Bundesministerium des Innern und für Heimat: Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode, Juni 2022, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html, 28.11.2022.

Burgess, Matt: „A mysterious satellite hack has victims far beyond Ukraine“, Wired, 23. März 2022, https://www.wired.com/story/viasat-internet-hack-ukraine-russia/, 19.11.22.

28 Teivainen, Aleksi: „Finnish Parliament's website brought down by Russian hacker group“, Helsinki Times, 10. August 2022.

29 Sytas, Andrius: „Estonia says it repelled major cyber attack after removing Soviet monuments“, Reuters, 18. August 2022.

30 Euractiv: „Cyberattack hits Montenegro government, defence minister points at Russia“, 28. August 2022.

31 ENISA: ENISA Threat Landscape 2022, 3. November 2022.

Cattler, David/Black, Daniel: „The myth of the missing cyberwar", Foreign Affairs, 1. August 2022, https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar, 19.11.22.

De Liedekerke, Arthur/De Rivoire, Hector: Ukraine's cyber resistance is impressive – but hard to replicate, euobserver, 26. September 2022, https://euobserver.com/opinion/156126, 28.11.2022.

De Liedekerke, Arthur/Laudrain, Arthur: „Cyber War: What's next and what the European Union should do, Council on Foreign Relations", 30. März 2022, https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do, 19.11.22.

Deutsche Welle: „Germany bolsters defenses against Russia cyber threat", 12. Juli 2022, https://www.dw.com/en/germany-bolsters-defenses-against-russian-cyber-threats/a-62442479, 19.11.22.

Digital Security Unit: Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine, Microsoft, 27. April 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd, 19.11.22.

ENISA: ENISA Threat Landscape 2022, 3. November 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, 28.11.2022.

Euractiv: „Cyberattack hits Montenegro Government, defence minister points at Russia", 28. August 2022, https://www.euractiv.com/section/global-europe/news/cyberattack-hits-montenegro-government-defence-minister-points-at-russia/, 19.11.22.

Harding, Luke: „Ukraine hit by 'massive' cyber-attack on government websites", The Guardian, 14. Januar 2022, https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers, 19.11.22.

HarperCollins: Shock and Awe, https://www.collinsdictionary.com/de/worterbuch/englisch/shock-and-awe, 29.11.2022.

Hoyer, Katja: „Germans are under attack. Can they adapt?", The Washington Post, 25. Oktober 2022, https://www.washingtonpost.com/opinions/2022/10/25/russia-sabotage-germany-railroads-hacking-drones/, 19.11.22.

Kabelka, Laura: „EU's cybersecurity agency chief warns to Keep Guard up", Euractiv, 28. September 2022, https://www.euractiv.com/section/cybersecurity/news/eus-cybersecurity-agency-chief-warns-to-keep-guard-up/, 19.11.22.

Kabelka, Laura: „Germany still not affected by Russia-linked cyberattacks", Euractiv, 6. Mai 2022, https://www.euractiv.com/section/cybersecurity/news/germany-still-not-affected-by-russia-linked-cyberattacks/, 19.11.22.

Mäder, Lukas: „Im Ukraine-Krieg kämpft eine ‚IT-Armee' online gegen Russland. Die Freiwilligen attackieren sogar Apotheken und Universitäten", Neue Züricher Zeitung, 23. Juli 2022, https://www.nzz.ch/technologie/ukraine-krieg-freiwillige-it-armee-greift-russische-ziele-an-ld.1689428, 29.11.2022.

Nasr, Joseph: „Germany issues hacking warning for users of Russian anti-virus software Kaspersky", Reuters, 15. März 2022, https://www.reuters.com/technology/germany-issues-hacking-warning-users-russian-anti-virus-software-kaspersky-2022-03-15/, 19.11.22.

Pearson, James/Satter, Raphael/Bing, Christopher/Schectman, Joel: „Exclusive: U.S. Spy Agency probes sabotage of satellite internet during Russian invasion, sources say", Reuters, 11. März 2022, https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/, 19.11.22.

Rat der Europäischen Union: Russian cyber operations against Ukraine: Declaration by the high representative on behalf of the European Union, 10. Mai 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/, 19.11.22.

Sabbagh, Dan: „Russian hackers targeting opponents of Ukraine invasion, warns GCHQ chief", The Guardian, 10. Mai 2022, ://www.theguardian.com/technology/2022/may/10/russian-hackers-targeting-opponents-of-ukraine-invasion-warns-gchq-chief, 19.11.22.

Simonite, Tom: „A Zelensky Deepfake was quickly defeated. The next one might not be", Wired, 17. März 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/, 19.11.22.

Smalley, Suzanne: „Nakasone says Cyber Command did nine 'hunt forward' ops last year, including in Ukraine", CyberScoop, 4. Mai 2022, https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/, 19.11.22.

Sytas, Andrius: „Estonia says it repelled major cyber attack after removing Soviet monuments", Reuters, 18. August 2022, https://www.reuters.com/world/europe/estonia-says-it-repelled-major-cyber-attack-after-removing-soviet-monuments-2022-08-18/, 19.11.22.

Teivainen, Aleksi: „Finnish Parliament's website brought down by Russian Hacker Group", Helsinki Times, 10. August 2022, https://www.helsinkitimes.fi/finland/finland-news/domestic/22011-finnish-parliament-s-website-brought-down-by-russian-hacker-group.html, 19.11.22.

Vallance, Chris: „Ukraine war: Major internet provider suffers cyber-attack", BBC News, 28. März 2022, https://www.bbc.com/news/60854881, 10.11.22.

Willett, Marcus: The Cyber Dimension of the Russia–Ukraine War, International Institute for Strategic Studies, 6. Oktober 2022, https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war, 19.11.22.

Xiao, Menghan: „Cyberattacks accelerating in Europe, Moody's says", SC Media, 18. Oktober 2022, https://www.scmagazine.com/analysis/vulnerability-management/cyberattacks-accelerating-in-europe-moodys-says, 19.11.22.

Zetter, Kim: „Inside the cunning, unprecedented hack of Ukraine's power grid", Wired, 3. März 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 19.11.22.