ANALYSE

Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022

Matthias Schulze (Stiftung Wissenschaft und Politik, Berlin)

DOI: 10.31205/UA.267.01

Zusammenfassung

Im Vorfeld des russischen Einmarsches in der Ukraine befürchteten Analyst:innen schwerwiegende Cyber-Angriffe etwa gegen kritische Infrastrukturen, die so Strom oder Kommunikationsnetze abschalten könnten. Größere destruktive Cyber-Vorfälle sind bisher im Kontext des Krieges nicht eingetreten. Das Cyber-Konfliktbild ist von gezielten Angriffen, Cyber-Spionage und den störenden Tätigkeiten von pro-russischen oder pro-ukrainischen Hacktivist:innen gekennzeichnet. Insgesamt haben diese Angriffe jedoch kaum Effekte im Krieg auf dem Boden und in der Luft. Es werden fünf Gründe für das Ausbleiben schwerwiegenderer Cyber-Angriffe genannt: erstens eine gute Defensive der Ukraine, zweitens eine unklare Datenlage, drittens überzogene Erwartungen an ein »Cyber-Pearl Harbor«-Szenario, viertens staatliche Zurückhaltung und fünftens die hohe wechselseitige Verwundbarkeit.

Lehren aus der Vergangenheit

Im Vorfeld der russischen Invasion in der Ukraine warnten zahlreiche IT-Sicherheitsexpert:innen und Behörden vor großen russischen Cyber-Angriffen auf kritische Infrastrukturen. Die US-amerikanische Cybersecurity and Infrastructure and Security Agency (CISA) forderte etwa am 16. Februar, also eine Woche vor Kriegsbeginn, mit markigen Worten US-amerikanische Unternehmen auf, die »Schilde hochzufahren«. IT-Sicherheitspersonal und Administrator:innen sollten besonders wachsam sein. Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte seit Anfang des Jahres mehrfach vor russischen Cyber-Angriffen auf kritische Infrastrukturen in Deutschland.

Dafür gab es berechtigte Gründe. Russland hatte in der Vergangenheit eine ganze Bandbreite seiner offensiven Cyber-Fähigkeiten zur Schau gestellt: Dazu gehörten Cyber-Spionage wie etwa der Bundestagshack 2015 oder die weltweite Solar Winds-Kampagne 2020, sogenannte Hack & Leak-Operationen zur Beeinflussung der amerikanischen und französischen Präsidentschaftswahlen 2016 und 2017 oder die Störungen mit Milliardenschäden durch den Ransomware-Wurm Not-Petya im Jahr 2017. Als Königsdisziplin gelten dabei physische Effekte durch Cyber-Angriffe: Russische Angreifer:innen deaktivierten einmal im Jahr 2015 und einmal im Jahr 2016 mit der Crashoverride/Industroyer Schadsoftware für wenige Stunden den Strom in der ukrainischen Hauptstadt Kyjiw. Die Ukraine wird seit der Annexion der Krim 2014 auch als »Testgebiet für Cyber-Warfare« bezeichnet, da sie in den letzten Jahren immer wieder mit Ausfällen durch Cyber-Angriffe zu kämpfen hatte. Mit der Invasion der Ukraine gab es also Grund zur Annahme, dass Cyber-Operationen kriegsbegleitend oder gar als Vergeltung gegen westliche Sanktionen eingesetzt werden könnten. Seit 2018 warnen westliche Behörden wie zum Beispiel der deutsche Verfassungsschutz, dass russische Bedrohungsakteure es zunehmend auch auf westliche kritische Infrastrukturen wie Stromnetze abgesehen haben.

Dahinter steht die vorwiegend westlich geprägte Sorge vor einem großen strategischen Cyber-Krieg, bei dem digitalisierte Länder aus der Ferne heruntergefahren werden und durch Stromausfälle die Wirtschaft und die Zivilgesellschaft komplett zum Erliegen komme. Solch ein »Cyber-Pearl Harbor«-Bedrohungsszenario geistert seit den 1990er Jahren durch westliche sicherheitspolitische Diskurse. Allerdings hat es wenig mit der Realität zu tun.

Vorstellung und Wirklichkeit

Der barbarische Krieg in der Ukraine tobt nun schon über zwei Monate. Derzeit muss allerdings konstatiert werden, dass der große Cyber-Krieg (bisher) ausgeblieben ist. Zu beobachten war schon eine ganze Bandbreite verschiedenster Cyber-Operationen, doch diese haben eher eine geringe bis mittlere Intensität. Physische Schäden, länger anhaltende Ausfälle kritischer Infrastrukturen oder gar Stromausfälle hat es bisher kaum gegeben. Allerdings gab es durchaus Versuche, Substationen des Stromnetzes zu sabotieren, die aber nach öffentlich verfügbaren Informationen abgewehrt werden konnten. Der Chef des britischen Nachrichtendienstes GCHQ fasste in einer Rede die Cyber-Lage wie folgt zusammen: »Während einige Leute nach einem ›Cyber-Pearl Harbor‹ gesucht haben, war es nie unsere Auffassung, dass ein katastrophaler Cyber-Angriff ein zentraler Bestandteil der russischen Cyber-Offensive oder ihrer Militärdoktrin ist.« Stattdessen sehe man eine gezielte Kampagne russischer Cyber-Akteure, die ukrainische Regierungs- und Militärsysteme angreifen und stören.

Der Chef der amerikanischen National Security Agency (NSA) und der United States Cyber Com-

mand (USCYBERCOM) Paul M. Nakasone vertrat in einer Kongressanhörung im März eine ähnliche Position. Man habe bisher nur drei bis vier bemerkenswerte russische Cyber-Angriffe gesehen. Er bezog sich dabei auf eine Serie sogenannter Wiper-Attacken gegen ukrainische Behörden, die Daten exfiltriert und gelöscht hatten. Wiper-Schadsoftware löscht Daten auf Systemen und macht so einzelne Rechner bzw. ganze Netzwerke unbrauchbar. Damit wurde die Arbeit ukrainischer Behörden und somit die Reaktionsfähigkeit auf eine Invasion massiv gestört. Das genaue Ausmaß der gelöschten Daten und betroffenen Ministerien ist bisher unklar. Aber der Einsatz von fünf verschiedenen Wiper-Generationen spricht dafür, dass man hier auf größtmögliche Reichweite setzte. Wiper sind in Cyber-Konflikten eher selten. Normalerweise gibt es nur wenige Vorfälle pro Jahr, da diese Schadsoftwarevariante als sehr aggressiv gilt. Auch wenn genaue Analysen und Attribution zum Teil noch ausstehen, ist anzunehmen, dass diese Schadsoftware-Varianten verschiedenen russischen Bedrohungsakteuren zugeschrieben werden können.

Bemerkenswert ist zudem der Hack von KA-SAT Sattelitenmodems der amerikanischen Firma Viasat. Die Modems von Internet-of-Things-Geräten wie Windturbinen erhielten am 24. Februar, also am Tag der Invasion, manipulierte Steuerungsbefehle, was zum Abbruch der Sattelitenverbindung führte, wobei die Turbinen selbst noch funktionierten. Die Kompromittierung erfolgte laut Viasat über eine gekaperte VPN-Verbindung einer Bodenstation und durch einen Wiper (AcidRain), der die Modems löschte. Da der Ausfall insbesondere die Region in Südosteuropa betraf und auch das ukrainische Militär über KA-Sat kommuniziert, liegt ein Zusammenhang mit dem Krieg nahe. Tausende Windkraftanlagen in Europa waren das Kollateralopfer von diesem Cyber-Angriff, darunter auch Anlagen des deutschen Betreibers Enercon. Viasat hat über 27.000 Kunden weltweit, so dass die Dunkelziffer der Betroffenen sicher noch höher ist. Westliche Nachrichtendienste gehen mittlerweile davon aus, dass das Ziel dieser Cyber-Angriffe die Störung der militärischen Kommunikation (Command & Control) der Ukraine war, um einen russischen Einmarsch zu erleichtern. Einiges spricht dafür, dass dies zumindest in den Anfangstagen des Krieges bis zu einem gewissen Grad erfolgreich war.

Neben destruktiven Wiper Angriffen betreibt Russland auch vermehrt Cyber-Spionage. Am 7. März meldete Googles Threat Analysis Group, dass sie vermehrte Aktivität von Phishing und Spionagekampagnen von APT28 (Russland) und Ghostwriter/UNC1151 sehen (vermutlich Belarus). Advanced Persistent Threats (APT) beschreiben Angriffskampagnen, die sich über lange Zeit auf wenige Ziele konzentrieren, um dauerhaften Zugriff zu erhalten. Meist sind dies staatliche Cyber-Operationen mit dem Ziel der Spionage oder der Sabotage von Systemen. APT sind im Vorgehen komplexer und kompetenter als etwa Cyber-Kriminelle oder Hacktivist:innen und sind deswegen gefährlicher. Auch die russische IT-Sicherheitsfirma Kaspersky meldete am 10. März, dass man seit Anfang Februar eine erhöhte Aktivität von Command & Control (C2) Infrastruktur der APT Gamaredon sehe. Gamaredon (auch Primitive Bear genannt) wird dem russischen Geheimdienst FSB zugeschrieben. Cyber-Angreifer steuern ihre Schadsoftware über eine derartige C2-Infrastruktur aus der Ferne und nutzen die Systeme auch zur automatisierten Verbreitung von Phishing-Mails und für andere Komponenten von Cyber-Operationen.

Zwei Wochen später wurde berichtet, dass die vermutlich russische APT Sandworm mittels ASUS-Routern ein neues Botnet (genannt Cyclops Blink) aufbaute, vermutlich ebenfalls als C2-Infrastruktur für eine neue Angriffswelle. Sandworm wird dem russischen Militärgeheimdienst G(R)U zugeschrieben und griff in der Vergangenheit auch westliche Ziele an. Dies kulminierte schließlich in der Warnung von US-Präsident Joe Biden am 21. März, dass man »aktuelle Informationen« habe, dass Russland Optionen für Cyber-Angriffe gegen den Westen prüfe. Am 31. März tauchte schließlich ein Bericht in ungarischen Medien auf, welcher von einer umfassenden Kompromittierung des ungarischen Außenministeriums durch russische Spionagekampagnen sprach. Diese Kompromittierung gehe teils Jahre zurück, da es Ungarn aufgrund fehlender Kompetenzen und politischem Willen nicht gelang, die Angreifer permanent aus den Netzwerken zu werfen. Ungarische Insider berichten von erhöhter Aktivität der Angreifer im Januar. Sie hätten über das ukrainische Außenministerium Fernzugriff auf sensible Datenkanäle der EU und NATO bekommen, während zeitgleich diverse NATO- und EU-Krisenkonferenzen im Hinblick auf den bevorstehenden Krieg in der Ukraine tagten.

Diese gezielteren Aktivitäten russischer Nachrichtendienste entsprechen ungefähr dem, was man auch in der Vergangenheit, etwa mit Hacks gegen diverse Außenministerien (darunter auch das deutsche), beobachten konnte. Diese Angriffe sind eher leise und auf wenige Ziele fokussiert, aber dafür auf dauerhaften Zugang ausgelegt. Nur dadurch lassen sich wertvolle nachrichtendienstliche Informationen extrahieren. Da Russland Informationen über die westliche Positionierung innerhalb der EU und NATO, etwa bei der Unterstützung von Sanktionen oder Waffenlieferungen sucht, ist Cyber-Spionage das Mittel der Wahl. Das Ziel dürfte mittel- bis langfristig sein, Keile zwischen die westlichen Staaten zu treiben, um die Sanktionen oder die Militärhilfe der Ukraine zurückzufahren. Darin dürfte der größte Wert von Cyber-Spionage im Kontext des Krieges in der Ukraine liegen.

Cyber-Scharmützel

Neben verborgener staatlicher Aktivität ist die digitale Dimension des Ukraine-Krieges von einer Vielzahl kleinerer Scharmützel zwischen pro-russischen und pro-ukrainischen Hacktivist:innen gekennzeichnet. Weltweit schlossen sich IT-Expert:innen und Hacker:innen dem ukrainischen Aufruf zur Bildung einer IT-Army an. Mittlerweile haben sich um die 70 Hacktivist:innengruppen, von GhostSec, Anonymous, Network Battalion 65, aber auch Cyberkriminelle wie Ransomware-Gruppen auf die ukrainische Seite geschlagen. Es gibt aber auch Gruppen, die Russland unterstützen wie Conti, KillDisk oder Xaknet, die bereits Cyber-Angriffe auf westliche Ziele gestartet haben. Der Begriff Hacktivist beschreibt den losen Zusammenhang global verteilter Hacker:innen, die sich ad hoc für gemeinsame Aktivitäten verbünden, aber nicht zentral gesteuert werden.

Ein Großteil ihrer Aktivität ist insbesondere durch zahlreiche Distributed Denial of Service-Angriffe (DDoS) gekennzeichnet. Immer wieder werden russische Websites wie vom Kreml, von Ministerien, Botschaften, von Geheimdiensten wie dem FSB, Banken, aber auch russischen Staatsmedien temporär überlastet. DDoS-Angriffe dauern meist nur kurz an und sind reversibel. Sie werden auch immer wieder gegen ukrainische Internetdienstanbieter (ISP) gerichtet, was teilweise zu partiellen Konnektivitätsverlusten in einzelnen Regionen führt. Daneben gibt es auch zahlreiche Website-Defacement-Angriffe, bei denen Anti-Kriegsbotschaften und die berühmte »Guy Fawkes«-Maske auf Websites platziert werden.

Daneben wenden Hacktivist:innen eine Hack & Leak-Strategie gegen Russland an. In Netzwerke und Server von Ministerien, Behörden und Unternehmen wird eingebrochen, deren Daten gestohlen und zum Download zur Verfügung gestellt. Hacktivist:innen behaupten unter anderem in die folgenden Institutionen eingebrochen zu sein: die russische Zentralbank, die russische Weltraumbehörde, Gazprom, Rosneft Deutschland (das BKA ermittelt), Transneft, die Medienregulationsanstalt Roskomnadzor, Rüstungsunternehmen wie Rostec, Tetraedr und Kronshtadt, Nuklearforschungsinstitute sowie Medien. Diese Leaks beinhalten auch wertvolle strategische Informationen: so wurden die Namen und Dienstnummern von den über 120.000 russischen Soldat:innen in der Ukraine veröffentlicht. Zudem wurden detaillierte Informationen über 620 Agenten des russischen Geheimdienstes FSB veröffentlicht. Diese Daten sind für westliche und weitere Nachrichtendienste ein Fundus und dürften allesamt übersetzt und ausgewertet werden, um nachrichtendienstliche Vorteile zu erlangen. Ein Beispiel hierfür ist die Enttarnung von Geheimdienstagenten durch die Korrelation von Handydaten und Essensbestellungen bei Lieferdiensten durch die NGO Bellingcat.

Daneben gibt es noch eine ganze Reihe von Hacks mit diversen Zielen, etwa um die russische Internetzensur zu umgehen und der russischen Bevölkerung ein anderes Bild des Krieges zu zeigen. Ziel solcher »Informationsoperationen« ist es, die Informationshoheit der Staatspropaganda in Russland zu durchbrechen. So hackte Anonymous mit dem Internet verbundene Drucker, um Anti-Kriegsflugblätter zu drucken. Überwachungskameras wurden gehackt und in ihre Videofeeds Anti-Kriegsbotschaften eingebettet. Das russischsprachige soziale Netzwerk VK wurde angeblich gehackt, um ähnliche Informationen zu verbreiten. Vieles lässt sich nur schwer verifizieren. Zur Umgehung von Staatspropaganda in Russland werden zudem auch andere Mittel genutzt wie zum Beispiel Email-Spam an russische Email-Adressen, SMS- und WhatsApp-Spam über ein eigens von Hacktivist:innen entwickeltes Tool, sowie klassische Anrufe bei russischen Telefonnummern, um vom Krieg zu berichten. Es gibt zudem Berichte, dass Live-Streams von russischen Fernsehsendern gehackt wurden, um pro-ukrainische Botschaften zu zeigen. Wie erfolgreich diese Initiativen sind, ist schwer abzuschätzen.

Es gibt zudem erste Berichte, dass auch Ransomware eingesetzt wird. Ransomware verschlüsselt Daten auf Zielsystemen und macht sie für ihre Besitzer:innen unbrauchbar. Ransomware ist ein weitverbreitetes Mittel von Cyber-Kriminellen, um Lösegeld zur Wiederfreigabe der verschlüsselten Daten zu erpressen. Die Systeme der russischen Firma Miratorg, einem der größten Fleischproduzenten des Landes, wurden angeblich verschlüsselt, ohne dass eine Lösegeldzahlung abgesetzt wurde. Zudem behauptete die »Belarussian Cyber Guerilla«, das Logistiknetzwerk der belarusischen Eisenbahn mit Ransomware lahmgelegt zu haben, um die Verlegung russischer Truppen in Belarus zu verhindern. Allerdings gab es auch physische Sabotageakte entlang der belarusischen Eisenbahnlinien, so dass unklar ist, ob Schadsoftware oder brennende Kabelschächte die Ausfälle auslösten. Diverse Ransomware-Gruppen, darunter Stormous oder auch Conti sind auf russischer Seite in den Konflikt eingestiegen. Conti behauptet etwa für einen Ransomware-Angriff auf das deutsche Windenergieunternehmen Nordex im April 2022 verantwortlich zu sein. Conti war in der Vergangenheit für über 800 Ransomware-Vorfälle weltweit verantwortlich, die meisten in den USA. Die Gruppe wurde aber selbst Opfer eines Datenlecks: einer ihrer Mitarbeitenden war Ukrainer und veröffentlichte große Teile der internen Jabber-Kommunikation der Gruppe, aus der Kontakte zum russischen FSB sowie diverse Managementprobleme sichtbar wurden. Dieses Datenleck allein erlaubt einen einmaligen Einblick in das verborgene Geschäftstreiben von Cyber-Kriminellen.

Zusammenfassend kann man sagen, dass all diese Vorfälle eher kleinere Störungen sind, eine recht unkoordinierte Taktik der tausend Nadelstiche. Sie beeinflussen die Ereignisse am Boden nicht wirklich. Allerdings können die zahlreichen Datenlecks mittel- bis langfristig Russland schaden. Die schiere Summe der veröffentlichten Daten dürften ein Fundus für Nachrichtendienste weltweit darstellen und seltene Einblicke in das Innenleben des geheimniskrämerischen russischen Staates geben. Für sich genommen erzielt die Vielzahl der Vorfälle aber kaum militärische Effekte und beeinflusst Geschehnisse auf dem physischen Schlachtfeld kaum.

Erklärungsversuche

In der akademischen Community entbrannte eine Diskussion hinsichtlich der Frage, wie diese Befunde einzuordnen sind. Warum ist der große Cyber-Krieg ausgeblieben? Warum gab es bisher keine größeren Stromausfälle? Es gibt eine Reihe konkurrierender Hypothesen.

Erstens scheint plausibel, dass die ukrainische Cyber-Abwehr sehr erfolgreich arbeitet und bisher das Schlimmste verhindern konnte. So konnte das ukrainische Computer Emergency Response Team (CERT) am 8. April einen Stromausfall verhindern, indem eine Schadsoftware namens Industroyer2 rechtzeitig identifiziert und unschädlich gemacht wurde. Industroyer2 basiert auf einer Schadsoftware, die bereits 2016 in Kyjiw kurz den Strom ausschaltete. Ukrainische Cyber-Spezialist:innen studierten diesen Angriff intensiv und lernten daraus, was letztlich sinnvoll für die Vorbereitung gewesen sein dürfte. Die Ukraine gilt seit 2014 als »Testgebiet für Cyber-Krieg« und hat seitdem, wohl wie kein zweites Land auf der Welt, praktische Erfahrung in der Abwehr von Cyber-Angriffen machen können. Zudem erhält die ukrainische Cyber-Abwehr schlagkräftige Unterstützung von weltweiten IT-Sicherheitsunternehmen wie ESET und Microsoft, welche ihre Informationen zu laufenden Angriffskampagnen mit der Ukraine teilen. Auch die USA und die NATO (über das Cyber-Kompetenzzentrum in Tallinn) teilen sogenannte »threat intelligence« (taktische Informationen zu laufenden Operationen) mit der Ukraine, um besser gegen laufende Angriffe gewappnet zu sein.

Zweitens ist anzunehmen, dass wir das wahre Ausmaß der bisherigen Cyber-Angriffe durch den »Nebel des Krieges« nicht wahrnehmen können. Russland kommuniziert in der Regel eigene Cyber-Operationen bzw. Cyber-Vorfälle im eigenen Land nicht. Außerdem gibt es, anders als in westlichen Ländern, auch keine Berichtspflichten für Unternehmen. Insofern ist es möglich, dass größere Cyber-Sicherheitsvorfälle im Hintergrund stattfanden und bisher nicht öffentlich wurden.

Eine dritte Hypothese, die insbesondere in der akademischen Cyber-Konfliktforschung vertreten wird, ist, dass die Erwartung eines desaströsen Cyber-Angriffs schlichtweg auf einer Fehlcharakterisierung von »Cyber War« in westlichen Ländern basiert. In der akademischen Literatur wird schon lange der Mythos entzaubert, dass Cyber-Angriffe eine Revolution der Kriegsführung bedeuten. Das hypothetische »Cyber-Pearl Harbor«-Szenario, ein Industrieland aus der Ferne auszuschalten, hat wenig mit der operativen Wirklichkeit von Cyber-Operationen zu tun. Cyber-Angriffe unterliegen zahlreichen Einschränkungen wie langen Vorbereitungszeiten, einer gewissen Fehlerrate sowie der Ungewissheit von Effekten. Generell ist es sehr schwierig und zeit- und ressourcenintensiv, physische Effekte wie einen landesweiten Stromausfall auszulösen. Deswegen sind derartige, hochintensive Cyber-Angriffe extrem selten. Die Charakteristika von Cyber-Vorfällen haben trotz ihres militärischen »Framings« als »Cyber-Angriff« wenig mit Krieg zu tun. Krieg ist durch massive Gewalt, Tod und Zerstörung gekennzeichnet. Die meisten Cyber-Angriffe sind in ihren Effekten weitaus niedrigschwelliger und vor allem reversibel. Temporäre Störungen etwa durch Ransomware oder DDoS Angriffe, Cyber-Kriminalität, Hack & Leak-Operationen und Spionage bestimmen das Cyber-Konfliktbild. Und dies repräsentiert auch die Mehrzahl der dokumentierten Cyber-Vorfälle um den Ukrainekrieg.

Die vierte Hypothese leitet sich daraus ab: Es ist schwierig, mit Cyber-Angriffen physische Effekte hervorzurufen. Einfacher ist es, dies mit konventionellen Mitteln zu tun. Da Russland ohnehin mit konventionellen Truppen in der Ukraine präsent ist, können Strom oder Internetausfälle auch einfach durch Raketenbeschuss oder das Kappen von Leitungen hervorgerufen werden. Das ist einfacher, billiger und schneller. Aber vor allem ist die Erfolgswahrscheinlichkeit verglichen mit einer Cyber-Operation höher. Insofern argumentieren einige Forschende, dass Cyber-Operationen im Kontext eines Bodenkrieges eher ungeeignet sind. Stattdessen eignen sie sich weitaus besser für den Wettbewerb zwischen Nachrichtendiensten. Cyber-Operationen haben viel mehr Ähnlichkeiten mit dem subversiven Vorgehen von Geheimdiensten, das etwa auf die verborgene Beschaffung von Information und die subversive Beeinflussung von Diskursen in anderen Gesellschaften durch sogenannte »aktive Maßnahmen« abzielt. Dies ist im Übrigen auch die primäre Charakterisierung von Cyber-Aktivitäten in autoritären Regimen wie China und Russland: Dort wird nicht von Cyber-Krieg gesprochen, sondern vom übergeordneten Konzept des Informationskrieges. Cyber-Operationen sind darin nur eine Subkategorie und damit nur ein Werkzeug von vielen, was dem Ziel der Informationsüberlegenheit und Kontrolle dienen soll.

Eine fünfte Hypothese ist, dass die wechselseitige Interdependenz von vernetzten Systemen über das Internet zu Zurückhaltung auf staatlicher Seite führt. Staaten schrecken vor destruktiven Cyber-Angriffen mit langan-

haltenden Schäden zurück, weil sie selbst abhängig und verwundbar sind. Die meisten Staaten nutzen ähnliche Hard- und Software (zum Beispiel Windows-Betriebssysteme, Android- oder iPhone-Smartphones oder Open-Source-Bibliotheken in Webservern). Es werden immer wieder Schwachstellen veröffentlicht, die ein Großteil aller mit dem Internet verbundenen Systeme betreffen, wie etwa Heartbleed (2014) oder Log4J (2021). Darüber sind alle Staaten, die entsprechende Software nutzen, gleichermaßen angreifbar. Wenn Russland kritische Infrastrukturen im Ausland mit einer Schadsoftware angreift, die zum Beispiel die Log4J-Schwachstelle ausnutzt, ist zu befürchten, dass etwa die USA in Russland Ähnliches tun könnten. Russland beschwerte sich in der Vergangenheit, dass das United States Cyber Command in russischer kritischer Infrastruktur aktiv ist. Auch Russlands Bemühungen im Bereich der IT souverän zu werden und somit auf westliche Dienste zu verzichten, sind in diesem Licht zu interpretieren. Es existiert also bei destruktiven Cyber-Angriffen hoher Intensität eine Art Gleichgewicht des Schreckens, zumindest zwischen der NATO und Russland.

Zudem ist es nicht unwahrscheinlich, dass ein schwerwiegender Cyber-Angriff gegen westliche Staaten rechtlich als »bewaffneter Angriff« interpretiert werden könnte und den NATO-Verteidigungsfall nach Artikel 5 auslöst. Das dürfte nicht in Russlands Interesse sein. Zurückhaltung wird auch durch die schwere Kontrollierbarkeit von Cyber-Angriffen befördert: Ein außer Kontrolle geratener Angriff könnte auch Drittparteien in den Konflikt ziehen. Die Effekte von Cyber-Angriffen gegen weitverbreitete Systeme sind mitunter schwer zu kontrollieren und können wie ein Bumerang wirken, der ungeplante Kaskadeneffekte auch in eigenen Systemen auslöst. Der russische Not-Petya-Angriff löschte weltweit Daten, darunter auch russischer Firmen, obwohl er sich ursprünglich gegen ukrainische Systeme gerichtet hatte. Im konkreten Falle von Russlands Krieg gegen die Ukraine gibt es Evidenz für diese Interdependenzthese: Es gibt etwa Hinweise, dass die russische Militärkommunikation teils unverschlüsselt über öffentliche Netze wie das Internet oder auch das Mobilfunknetz läuft. Wenn Russland diese Dienste per Cyber-Angriff ausschalten würde, könnte es selbst nicht mehr kommunizieren.

Fazit

Der brutale Krieg in der Ukraine tobt nun schon seit mehr als zwei Monaten. Insofern ist es zu früh für weitreichende Schlussfolgerungen. Cyber-Operationen sind letztlich Werkzeuge staatlichen Handelns, die an politische Ziele angepasst werden müssen. Ändert sich der Fokus und das Ziel des Krieges, so ist auch eine Veränderung in der Nutzung von Cyber-Operationen wahrscheinlich. Vieles deutete darauf hin, dass Russland einen kurzen Enthauptungsfeldzug plante und dass folglich Cyber-Operationen auf dieses Ziel hin angepasst wurden. Darauf deutet die koordinierte, taktische Verwendung von Wipern in der Frühphase des Krieges hin. Ändert sich das Kriegsziel zu einem langwierigen und strategischen Zermürbungskrieg, der sich auch gegen Zivilist:innen wendet, dann dürften auch Cyber-Operationen vermehrt diesem Zweck folgen. Insofern sind größere, strategische Cyber-Operationen etwa gegen Stromnetze in der Ukraine nicht mehr auszuschließen. Es gibt zudem vermehrt Hinweise, dass Russland auch Cyber-Operationen gegen den Westen ausweitet, etwa gegen kritische Infrastrukturen im Energiesektor wie Windenergie-Betreiber. Wenn Deutschland und Europa die Abhängigkeit vom russischen Gas mithilfe von Windenergie reduzieren wollen, dann dürften diese Industrien somit auch in den Fokus russischer Attacken geraten. Auch die amerikanische Cyber-Behörde CISA (Cybersecurity and Infrastructure Security Agency) warnte jüngst erneut, dass sich russische Hacker:innen für industrielle Steuerungsanlagen im Bereich Energieversorgung interessieren und dafür Schadsoftware entwickeln. Insofern ist es wahrscheinlich, dass sich der Westen auf einen länger anhaltenden Cyber-Konflikt mit Russland einstellen muss und dass das vormals ukrainische Testlabor von Cyber-Aktivitäten nun auch auf westliche Staaten ausgeweitet wird.
Stand: 25. April 2022

Über den Autor
Dr. *Matthias Schulze* ist der stellvertretende Leiter der Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik. Er forscht zu Cyber-Konflikten, Spionage und Cyber-Kriminalität. Er betreibt einen Blog und Podcast zum Thema unter www.percepticon.de.

Lesetipps

- David Sanger (2018) The perfect weapon, War, sabotage, and fear in the cyber age, New York, Melbourne, London, Crown Publishers; Scribe.
- Andy Greenberg (2019) Sandworm, A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers, New York, Doubleday, 2019.
- Nicu Popescu & Stanislav Secrieru (2019) Hacks, leaks and disruptions. Russian cyber strategies. Challiot Paper No. 148, October 2018, European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

- Matthias Schulze (2020) Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations, in: Jančárková, T./Lindström, L./Signoretti M./Tolga G. Visky (Eds), 2020 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, Tallinn. https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf.
- Lennart Maschmeyer (2021) "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", International Security, Vol. 46, No. 2, 2021, 51–90.
- Microsoft (2022) Special report Ukraine. An overview of Russia's cyberattack activity in Ukraine. 27.04.2022, abrufbar unter https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

DOKUMENTATION

Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022)

Tabelle 1: Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022)

Datum des Cybervorfalls	Kurzbeschreibung des Cybervorfalls
14.01.2022	Die Websites des ukrainischen Regierungskabinetts, von sieben Ministerien und des nationalen Notfallservice sind vorübergehend nicht erreichbar. Eine Botschaft wird platziert: »Habt Angst und erwartet das Schlimmste«.
17.02.2022	Website des Außenministeriums Russlands ist vorübergehend offline.
17.02.2022	Sabotage von Glasfaserleitungen in dem von der Ukraine kontrollierten Gebiet der Region Luhansk reduziert die Leistungsfähigkeit des Mobilfunknetzwerkes von Vodafone um 70 Prozent.
18.02.2022	Dutzende von Computern in zwei Regierungsbehörden der Ukraine wurden mit Whispergate-Schadsoftware gelöscht.
23.02.2022	Bericht von Trend Micro zu einem neuen Botnet, genannt Cyclops Blink. Hauptzweck des Botnets ist es, eine Infrastruktur für weitere Angriffe auf hochwertige Ziele in der Ukraine aufzubauen.
23.02.2022	Die IT-Firma ESET entdeckte eine neue Wiper-Malware (Hermetic Wiper), die in der Ukraine verwendet wurde. ESET-Telemetrie zeigt, dass sie auf Hunderten von Geräten im Land installiert wurde.
23.02.2022	Die Websites der Verteidigungs-, Außen- und Innenministerien der Ukraine wurden mit DDoS Angriffen überlastet. Darüber hinaus löschte Hermetic Wiper Daten auf Hunderten von Computern in der Ukraine, Lettland und Litauen.
25.02.2022	Das Anonymous-Kollektiv ist offiziell in den Cyberkrieg gegen die russische Regierung eingetreten.
26.02.2022	Hacktivst:innen von DDoSecrets veröffentlichen 200 GB an Daten des belarusischen Verteidigungsunternehmens Tetraedr.
26.02.2022	Die Ukraine rekrutiert Hacktivist:innen (IT-Armee der Ukraine) und definiert Ziellisten von Domains, die über »alle Vektoren und mit DDoS« angegriffen werden sollen.
27.02.2022	Das Anonymous-Network Battalion 65 veröffentlicht Dateien des russischen Instituts für Nuklearforschung.
28.02.2022	Das Ghostsec Kollektiv behauptet, es verfügt über einen Remote-Zugriff auf den NICA-Teilchenbeschleuniger des russischen Kernforschungsinstituts.
01.03.2022	Microsoft meldet, dass ukrainische Einrichtungen kurz vor der Invasion mit Foxblade Wiper angegriffen wurden.
01.03.2022	ESET-Forscher:innen entdecken einen neuen Wiper, der ukrainische Organisationen befällt (IsaacWiper).
01.03.2022	Die Ukrainska Prawda veröffentlicht Daten von 120.000 russischen Soldat:innen, die in der Ukraine kämpfen.
01.03.2022	Sberbank, eine russische staatliche Bank, wurde gehackt. Webserver-Daten wurden veröffentlicht.

Fortsetzung auf der nächsten Seite