Zur Aktualität

Digital gegen Russland kämpfen – bringt es das?

Hackerinnen weltweit beteiligen sich an Cyberaktionen gegen Russland. Was davon zu halten ist – und wie man sich wirksamer engagieren könnte.

Von Adrienne Fichter, 07.03.2022

Es scheint gerade einfacher denn je, vom eigenen Laptop aus gegen den Krieg zu kämpfen. Fast jeder von uns, so wirkt es, kann einen Beitrag leisten – dank Tech, Internet und Social Media.

- So erklärte die Hackergruppe Anonymous dem russischen Präsidenten den «digitalen Krieg». Verschiedene Websites der Regierung – insbesondere des Verteidigungsministeriums –, die Websites der Börse sowie der grössten russischen Bank waren zeitweise nicht erreichbar. (Ob alles davon auf das Konto von Anonymous geht, ist umstritten.)
- Elon Musk schaltete den Satelliten-Internetdienst Starlink für die Ukraine frei. Damit könnten Ukrainerinnen auch dann im Internet surfen, wenn Mobilfunk- und andere Dienste kriegsbedingt ausfallen sollten.
- Die ukrainische Regierung formiert eine freiwillige globale IT-Armee, der sich jeder mit den entsprechenden Skills anschliessen kann. Das Ziel: russische Angriffsziele hacken, etwa das Erdgasunternehmen Gazprom, den Ölkonzern Lukoil oder die Zensurbehörde Roskomnadzor.
- Und in der Schweiz vertwittert der SP-Co-Präsident Cédric Wermuth (mittlerweile bereits offline gegangene) Links, die zu Diensten führen, welche russische Websites zum Erlahmen bringen sollen.

Für uns alle, die wir seit zwei Wochen ohnmächtig hinter dem Bildschirm sitzen, vielleicht sogar selbst Verwandtschaft oder Freunde in der Ukraine haben und uns mit der Bevölkerung solidarisieren wollen, wirken solche Ankündigungen im ersten Moment wie ein Befreiungsschlag: Endlich können wir konkret etwas gegen den übermächtigen Angreifer tun, statt tatenlos dabei zuzusehen, wie mitten in Europa Bomben auf Häuser fallen.

Doch nach der kurzen Genugtuung folgt möglicherweise ein mulmiges Gefühl. Und ein paar Fragen. Etwa: Was genau passiert, wenn ich auf einen dieser Links klicke? Werde ich als beteiligte Hackerin automatisch zur digitalen Kriegspartei? Läuft hier schon ein sogenannter Cyberwar, und was bewirkt das überhaupt?

Gemäss Völkerrechts- und IT-Security-Expertinnen ist klar: In der gegenwärtigen Hektik werfen verschiedene Akteure wild und unsorgfältig mit militärischen Begriffen um sich. So sympathisch Sie das digitale Engage-

ment vielleicht finden mögen: Es kann politisch und rechtlich problematisch sein – aus mehreren Gründen.

1. Sie nehmen damit am Kampf teil

Wer sich, wie die lose Gruppierung Anonymous, an Cyberattacken beteilige und Russland den digitalen Krieg erkläre, könne damit zur Kombattantin werden, sagte etwa IT-Security-Experte Manuel Atug zum Deutschlandfunk. Wenn verschiedene Angreifer IT-Sicherheitslücken ausnutzen, Schadsoftware installieren und damit gegenseitig die Infrastruktur zum Erliegen bringen, also eine Art «digitales Jekami» losgehe – jede kann mitmachen –, werde das Internet allgemein unsicherer.

Ausserdem: Rechtlich gesehen kann eine Hackergruppe einem Staat gar keinen Krieg im Internet «erklären».

2. «Krieg» ist völkerrechtlich klar definiert

«Der Begriff ‹Cyberwar› gehört abgeschafft», sagt Sanija Ameti, Doktorandin mit Schwerpunkt Cybersecurity und Völkerrecht.

Krieg: Das ist etwas, was zwischen Staaten stattfindet und, gemäss der Uno-Charta, auch Gewaltanwendung beinhaltet (die Auslegung der Charta für den Cyberspace ist das entsprechende Tallinn Manual). Es gehe beim Krieg immer um bewaffnete Konflikte zwischen Staaten, sagt Ameti. Das Lahmlegen von Websites eines Staates ist eine Störungsaktion und Sabotage. Die eigentlichen Kriegshandlungen aber finden ganz konventionell statt.

«Wird ein russisches Spital und dessen Medizinalgeräte gehackt und sterben Leute dabei, dann kann man eher von einem Gewaltakt sprechen», sagt Ameti. «Aber selbst dann müsste die Zuordnung dieser Aktion zu einem oder mehreren konkreten Staaten erfolgen, um von einem ‹Cyberwar› sprechen zu können. Das ist nicht der Fall bei Individuen einer führungslosen Anonymous-Gruppe, die über den ganzen Globus verteilt sind.»

3. Die Wirkung ist beschränkt

Solche Cyberoperationen – etwa eine Attacke auf ein Stromversorgungsunternehmen oder Desinformationskampagnen auf Social Media – sind immer Handlungen, die ein strategisches Ziel vorbereiten oder unterstützen: Es geht dabei um die Schwächung des Gegners. Deshalb sprechen die meisten Cybersecurity-Expertinnen von einem «hybriden Krieg»: Mit digitalen Angriffen wird ein Staat geschwächt, mit Falschinformationen seine Bevölkerung manipuliert, offline aber findet der richtige Krieg statt.

Das sieht auch Myriam Dunn Cavelty so, die an der ETH zu Cybersecurity forscht: «Die Cyberdimension wird in der medialen Debatte überschätzt. Sie beeinflusst kaum das wirkliche Kriegsgeschehen.» Das, was Anonymous und weitere Gruppierungen hier gerade planten und umsetzten, beeindrucke die russischen Militärs nicht. Diese fokussierten auf die Strassen. Und setzten auf Panzer, Granaten, Raketen.

Auch die amerikanischen Big-Tech-Riesen scheinen diese Einschätzung zu teilen. Google, Facebook und Microsoft publizieren regelmässig, was sie in ihren Netzwerken beobachten. Die Security-Forscher von Microsoft sind

erstaunt darüber, wie planlos im Moment die russischen Cyberangriffe auf die Ukraine erfolgen. Ob nun noch was Grösseres folgt, ist derzeit unklar.

Die Ukraine dagegen ist ein digital kompetenter Staat, der aufgrund der jahrelangen Cyberattacken und Gängeleien durch den grossen russischen Nachbarn auch gelernt hat, sich selbst zu helfen, und dabei resilienter geworden ist. (Mehr dazu lesen Sie im Republik-Beitrag von Digitaljournalistin Eva Wolfangel.*)*

Wie der ukrainische Staat im Netz vorgeht

Die ukrainische Regierung weiss genau, was sie von welchen Akteurinnen einfordern kann:

- So fordert sie die Netzverwaltung Icann dazu auf, Russland vom globalen Internet zu isolieren (was abgelehnt worden ist).
- Es war der Digitalminister der Ukraine, der Elon Musk via Twitter fragte, ob er, statt den Mars zu erobern, doch seine Starlink-Satelliten für die Ukraine freischalten könnte, um das Internet für die Ukraine aufrechtzuerhalten. Dieser lieferte umgehend Empfängeranlagen in die Ukraine (eine Hauruck-Aktion, die sich als gefährlich herausstellen könnte, weil die Signale von Russland geortet und abgefangen werden können).
- Google und Apple schalteten auf Geheiss des ukrainischen Staates Echtzeit-Verkehrsinformationen im Land ab, um die Bevölkerung zu schützen.

Gemäss Völkerrecht darf die angegriffene Ukraine selbst mit ihren Soldaten zum Gegenschlag ausholen, also einen «Hackback» gegen die mutmasslich russischen Angreiferinnen durchführen, sofern die Zuordnung des Angriffs und die Angreifer rechtzeitig identifiziert werden konnten. Doch so was braucht Zeit und viele Ressourcen.

Was aber, wenn der Staat, wie am 25. Februar, die globale digitale Zivilgesellschaft zur Mithilfe ruft? Die ukrainische Regierung hat eine freiwillige «IT Army» ins Leben gerufen, die sich über Telegram koordiniert und 270'000 Mitglieder umfasst – ein absolutes Novum für eine Demokratie.

Darf sie das?

Hier wird es etwas komplizierter.

Sollte sich die Ukraine offiziell zu allen ab diesem Zeitpunkt erfolgten globalen Hackerangriffen gegen Russland bekennen, wären sie tatsächlich als staatliche Cyberoperationen zu werten. Aber ob die ukrainische Regierung in der gegenwärtigen Lage imstande ist, die Cyberaktionen aller Hackerinnen ihrer digitalen Brigade auf der Welt zu kontrollieren, ist zu bezweifeln.

Dass Staaten auch für die Aktionen ihrer privaten Hackerbanden im eigenen Land mitverantwortlich sein sollten, wird seit den identifizierten kriminellen Cyberbanden aus Russland, dem Iran, China und Nordkorea immer wieder auf internationaler Ebene diskutiert. Doch bisher wurde keine entsprechende Norm eingeführt. Denn sie wäre kaum durchsetzbar: Dazu müsste eine Regierung ihre Hackergruppen rundum überwachen, sagt Dunn Cavelty.

Und damit gilt für «Hacktivisten» – also Hacker und Aktivisten – an den Schreibtischen von Lwiw, Sankt Petersburg, Berlin, Sydney oder Nairobi nur ein Straftatbestand: Ihre Aktionen sind wohl rechtlich je nachdem als Cybercrime oder Datenschutzverletzung einzustufen, und zwar gemäss ukrainischem und russischem Recht.

Eine weitere mögliche Konsequenz für Einzelpersonen: «Wer sich nicht optimal schützt, kann auf Listen russischer Geheimdienste landen», sagte Sven Herpig, Cybersicherheitsspezialist der Berliner Denkfabrik Stiftung Neue Verantwortung, dem «Spiegel»-Magazin.

Die von der Republik befragten Experten sind sich in einem weiteren Punkt einig: Der Nutzen von freiwilligen und unkoordinierten offensiven Operationen ist begrenzt, die Kollateralschäden dagegen sind hoch. Denn: «Die Zivilbevölkerung leidet am Schluss – und nicht der Kreml», sagt ETH-Expertin Dunn Cavelty. Dies zeigt sich auch am geleakten Datensatz der Sberbank mit Informationen von russischen Bankkundinnen, den sich verschiedene Hackergruppen auf die Fahne schreiben. Damit wurden Daten von Vermögen von unbeteiligten Bürgern im Netz zugänglich gemacht.

Wenn also einiges problematisch ist – was kann oder soll man dann tun, wenn man zu denen gehört, die gern im Netz aktiv werden?

Was wäre eine wirklich sinnvolle Hilfe im Cyberspace?

Tatsächlich können erfahrene und ethische Hackerinnen in beheizten Wohnzimmern etwas tun, indem sie die ukrainische Cyberverteidigung stärken, wie Manuel Atug sagt. Dies könne etwa durch das Suchen nach Sicherheitslücken in ukrainischer Infrastruktur geschehen, beispielsweise bei Stromversorgungsunternehmen oder Wasserwerken – und mit dem sofortigen Melden an die ukrainische Regierung.

Diese Lücken sollten dann schnellstmöglich geschlossen werden – sofern die Betreiber der kritischen Infrastruktur überhaupt die Zeit dafür haben. Und nicht auf den nächsten anrollenden Panzer schiessen müssen.