Editorial
Der Ukrainekrieg – eine Zeitenwende (auch) für den Cyberraum?

Prof. Dr. Mario Martini[*]

Unzähligen Menschen hat er das Leben gekostet, Familien und Existenzen zerstört sowie öffentliche Infrastruktur in Trümmer gelegt: der völkerrechtswidrige Angriffskrieg Russlands gegen die Ukraine. In seinen Anfangstagen brannten sich Bilder einer Attacke auf den Kiewer Fernsehturm in das kollektive Gedächtnis ein: Mehrere Raketen treffen die Stahlfachwerkkonstruktion, ein Feuerball bildet sich, schwarzer Rauch umhüllt sie. Die Einschläge beschädigen den Kontrollraum und ein Umspannwerk, fünf Menschen sterben. Die Gebäudestruktur bleibt zwar intakt, die ukrainischen Fernsehsender müssen ihre Berichterstattung aber zeitweilig einstellen.

Um die Kommunikationsinfrastruktur des Fernsehturms auszuschalten, hätte es keiner Ballistik bedurft: Auch ein gezielter Hack der IT-Systeme hätte die Datenübertragung und Funktionalität torpedieren können. Warum also offene Gewalt und nicht eine unsichtbare Cyberattacke? Kurzum: Wo ist der Cyberwar?

Zu Beginn des Krieges prognostizierten einige Experten, dass Russland der Ukraine mit Cyberangriffen den „Stecker ziehen" werde. Dieses Schreckensszenario ist nicht eingetreten. Nach allem, was bekannt ist, hat die russische Regierung die analoge Kriegsführung zwar mit Cyberangriffen flankiert. Sie hat jedoch auf dem digitalen Schlachtfeld deutlich weniger Erfolg erzielt, als viele vermutet hatten. Cyberoperationen, wie DDoS- und Wiper-Attacken oder das „Defacement"[1] von Webseiten, sind bislang nicht mehr als ein „Hintergrundrauschen" im Gesamtkontext der kriegerischen Auseinandersetzung.[2] Das hat viele Gründe.

1. Ein Angriffsobjekt mit Cyberwaffen auszuschalten, ist nicht nur technisch sehr aufwendig, sondern auch langwierig und mit erheblicher Unsicherheit behaftet. Je bedeutender das avisierte (militärische) Ziel, umso schwieriger ist es in aller Regel, Cyberangriffe ins Werk zu setzen. Im Rahmen einer offenen militärischen Konfrontation verheißt die Strategie, verdeckt zu agieren, typischerweise auch kaum Vorteile.

2. Die Ukraine hat sich auf die Invasion ihres Nachbarn einschließlich ihrer Cyberimplikationen frühzeitig vorbereitet. Spätestens seit der Krim-Annexion 2014 haben einige NATO-Staaten das osteuropäische Land mit „Cyber"-Training extensiv unterstützt. Die Ukraine verfügt über gut geschultes Personal und die notwendigen Kapazitäten, um Cyberangriffe abzuwehren. So gelang es ihr bspw., russische Attacken auf ihr Starlink-Satellitensystem zu vereiteln. Ca. zwei Drittel aller Angriffe konnte die ukrainische Cyberverteidigung insgesamt abwehren.[3] Dazu haben nicht zuletzt Fortschritte in der Bedrohungsanalyse sowie die Nutzung Künstlicher Intelligenz beigetragen.

---

[*] *Mario Martini* ist Lehrstuhlinhaber an der DUV Speyer und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung. Er dankt insbesondere seinem Forschungsreferenten *Roland Klein* für die sehr gute Unterstützung. Soweit nicht anders angegeben, datieren die Internetquellen vom 1.7.2022.

[1] „Defacement" meint, Webseiten zu entstellen und/oder so zu verändern, dass es den Interessen des Betreibers widerspricht.

[2] Wenn die Methoden ausgefeilter und schlagkräftiger werden, kann solchen Attacken in der Zukunft allerdings eine entscheidende Rolle zuwachsen.

[3] *Microsoft*, Defending Ukraine: Early Lessons from the Cyber War, 22.6.2022, S. 11; https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Die Ukraine verfügt mit eigenen Cyberkräften sowie der sog. „IT Army of Ukraine" außerdem über Cyberschlagkraft, die sie offensiv gegen Russland einsetzt. Russland hat demgegenüber einen starken „Brain-Drain" im IT-Sektor zu verzeichnen.[4] Genaues ist zwar – wie so oft im Krieg – nicht bekannt. Es zeigt sich jedoch: Die Ukraine ist allen Unkenrufen zum Trotz weder an der analogen noch an der digitalen Front ein leichtes Opfer.

Dennoch: Der Krieg findet nicht nur in der Luft und am Boden, sondern auch im digitalen Raum statt. Er ist *auch* ein Cyberkonflikt. Gleich zu Beginn der russischen Invasion legte bspw. eine Attacke das KA-SAT-Satellitennetzwerk des Anbieters *Viasat* lahm – mit merklichen Folgen auch außerhalb der Ukraine. Unter anderem brachte dieser Angriff Windturbinen in Deutschland zum Stillstand.[5] Überdies gelang es Russland, die Computersysteme zahlreicher ukrainischer Behörden, Militäreinrichtungen und Kritischer Infrastrukturen vorübergehend auszuschalten. Ende März führten bspw. russische Hacker einen mehrstündigen Ausfall des ukrainischen Telekommunikations- und Internetanbieters *Ukrtelecom* herbei.[6]

Russland sah sich in den vergangenen Monaten seinerseits einer Vielzahl digitaler Angriffe der Ukraine sowie einer internationalen Hackerbewegung ausgesetzt, die sich für das angegriffene Land engagiert. In ihr Fadenkreuz gerieten unter anderem die russische Raumfahrtbehörde *Roskosmos* und die staatliche Fernseh- und Rundfunkanstalt *WGTRK*. Über einzelne „Nadelstiche" scheinen die Erfolge dieser Bewegung aber (jedenfalls soweit bekannt) noch nicht hinauszugehen.[7]

An Warnungen vor den nachhaltigen Risiken, die eine feindselige Auseinandersetzung im Cyberspace für andere Staaten mit sich bringt, hat es nicht gemangelt. Gleich zu Anfang des Krieges warnte bspw. die amerikanische *Cybersecurity and Infrastructure Security Agency* (CISA) mit einer „Shields Up"-Meldung vor erheblichen Gefahren, die von russischen Cyberattacken ausgehen können.[8] Ebenso machten die IT-Sicherheitsbehörden Australiens, Großbritanniens, Kanadas und Neuseelands eindringlich auf erhöhte Risiken aufmerksam.[9] Ähnlich stellte das *Bundesamt für Sicherheit in der Informationstechnik* (BSI bereits am 25. Februar eine erhöhte Bedrohung für Deutschland fest[10] – und hielt alle privaten und staatlichen Akteure an, die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um der geänderten Sicherheitslage Rechung zu tragen.

---

[4] *Anonymous*, Zehntausende IT-Fachkräfte verlassen Russland, Spiegel online, 14.4.2022, https://www.spiegel.de/wirtschaft/soziales/zehntausende-it-fachkraefte-verlassen-russland-a-77efa62b-53fd-451e-ad98-014f2cdd4144.

[5] *Sanger/Conger*, Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds, N.Y. Times online vom 10.5.2022, https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html.

[6] *Brewster*, 'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider, Forbes Magazine, 28.3.2022, https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyber attack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/.

[7] Auf dem digitalen Feld des „Informationskrieges" könnten sich jedoch angeblich durch Hacks gewonnene Leaks russischer Geheimdienstdatenbanken und anderer russischer Institutionen noch als effektvoll herauskristallisieren.

[8] *CISA*, Shields Up, https://www.cisa.gov/shields-up.

[9] *CISA*, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, 20.4.2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

[10] *BSI*, Einschätzung der aktuellen Cyber-Sicherheitslage in Deutschland nach dem russischen Angriff auf die Ukraine, Pressemitteilung v. 25.2.2022, https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement.html.

Beschränkte sich das BSI in seinen Vorschlägen noch auf passive Vorkehrungen, erschallt unterdessen auf der politischen Bühne immer häufiger der Ruf nach offensiven Cybermaßnahmen. In ihrem Koalitionsvertrag hatten die Ampelparteien sog. „Hackbacks" als staatliches Handlungsmittel noch kategorisch ausgeschlossen.[11] Unmittelbar nach Kriegsbeginn forderte Innenministerin *Nancy Faeser* jedoch, die Sicherheitsbehörden mit der Fähigkeit auszustatten, „zurückhacken" zu können.[12] Die Bundesrepublik solle auf Cyberangriffe (grenzüberschreitend) mit einem offensiven Gegenschlag antworten können, indem staatliche Akteure in fremde IT-Systeme eindringen.[13]

Das „Können" setzt allerdings das rechtliche „Dürfen" voraus – und dieses sieht sich zahlreichen Hürden ausgesetzt. Staatliche Cyberangriffe gegen ausländische Einrichtungen sind nicht nur am innerstaatlichen Recht, sondern auch an völkerrechtlichen Maßstäben zu messen. Ein Hackback kann gegen das Gewaltverbot (Art. 2 Nr. 4 UNCh) oder das Interventionsverbot verstoßen sowie die Souveränität eines anderen Staates verletzen.

Solche Eingriffe können zwar unter Umständen z. B. als Selbstverteidigung (Art. 51 UNCh) gerechtfertigt sein – die Schwelle hierfür liegt aber auch im Cyberspace hoch. Denn um ein Selbstverteidigungsrecht auszulösen, muss die ausländische Cyberattacke die Schwere eines bewaffneten Angriffs erreichen, also in Ausmaß und Wirkung dem Einsatz kinetischer Waffen gleichen. Bisher lässt sich allenfalls ein Präzedenzfall finden, der diese Voraussetzungen erfüllen könnte: der Fall Stuxnet (also der – mutmaßlich – amerikanisch/israelische Netzwerkwurm, der die Steuerungssysteme iranischer Atomanlagen infizierte und deren physische Zerstörung verursachte). Im Ukrainekrieg ist demgegenüber bis dato kein Vorfall bekannt, der für sich genommen die Ukraine zur Selbstverteidigung berechtigen könnte.

Offensive Cyberoperationen greifen nicht nur staatliche Infrastrukturen an, sondern können auch Individuen und damit die internationalen Menschenrechte verletzen, insbesondere das Menschenrecht auf Datenschutz und Datensicherheit (s. bspw. Art. 8 EMRK) sowie im Einzelfall das Recht auf Leben (s. bspw. Art. 2 EMRK) oder Eigentum (s. bspw. Art. 1 Zusatzprotokoll EMRK).[14]

Die Menschenrechte schieben einem Hackback zwar nicht gänzlich einen Riegel vor – sofern er auf einem Gesetz beruht, das die notwendigen Sicherheitsmaßnahmen gegen Missbrauch vorsieht. Gerade mit Blick auf seine einschneidende Wirkung muss die Rechtsgrundlage für den Hackback aber nicht nur hinreichend bestimmt sein, sondern auch – ebenso wie seine Durchführung im Einzelfall – strengen Verhältnismäßigkeitsanforderungen, insbesondere dem Gebot der Angemessenheit, genügen.

---

[11] *SPD/Bündnis 90/Die Grünen/FDP*, Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, 2021, S. 16 f.

[12] Inzwischen hat sie die Aussage etwas revidiert, s. *Neuerer/Specht*, Interview mit Bundesinnenministerin Nancy Faeser, Handelsblatt online 1.5.2022, https://www.handelsblatt.com/politik/deutschland/interview-innenministerin-nancy-faeser-es-ist-auf-jeden-fall-sinnvoll-einen-notvorrat-zu-hause-zu-haben/28290850.html.

[13] Ein solches Vorgehen sieht auch die jüngst vorgestellte Cybersicherheitsagenda der Bundesregierung (ohne den Begriff „Hackback" ausdrücklich zu erwähnen) vor, s. *BMI*, Cybersicherheitsagenda des BMI, Juni 2022, S. 6, 12; vgl. auch *Kharraz*, Cybersicherheitsagenda des Bundes wird modernisiert, beck-aktuell, 12.3.2022, https://rsw.beck.de/aktuell/daily/meldung/detail/cybersicherheitsagenda-des-bundes-wird-modernisiert.

[14] Dazu demnächst ausführlich *Martini/Klein*, Hackbacks im Lichte der internationalen Menschenrechte, S. 16 ff. des Typoskripts.

Nichts anderes gilt für den Eingriff in die nationalen Grundrechte, allen voran das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) – und das nicht nur im Hinblick auf rein innerstaatliche Einsatzszenarien von Hackbacks. Denn spätestens seit dem BND-Urteil des Bundesverfassungsgerichts ist klar: Die Bindung der deutschen Staatsgewalt an die Grundrechte macht nicht an der deutschen Staatsgrenze Halt (Art. 1 Abs. 3 GG); auch Ausländer im Ausland genießen den Schutz der Grundrechte des Grundgesetzes.[15] Um einen digitalen Gegenschlag zu gestatten, ist daher ein Gesetz erforderlich, das dem verfassungsrechtlichen Verhältnismäßigkeitsprinzip genügt.

Während im Verteidigungsfall nach Art. 87a Abs. 2 GG der Bundeswehr im Grundsatz die notwendigen Ermächtigungen zur Verfügung stehen, um offensive Cyberoperationen durchzuführen, fehlen solche Grundlagen für den Fall der offensiven, nicht militärischen Cyberoperation. Da es sich in ihrem Fall um eine Maßnahme der Gefahrenabwehr handelt, fällt sie grundsätzlich in die Zuständigkeit der Länder. Eine Rechtsgrundlage für Hackbacks auf Bundesebene einzuführen, wäre daher nur nach einer Grundgesetzänderung[16] möglich.[17]

Aber selbst wenn sich rechtlich alle Hürden nehmen ließen, macht das den Hackback noch nicht notwendigerweise zu einem sinnstiftenden Instrument der Cybersicherheit. Auch bei rechtskonformer Ausgestaltung birgt sein Einsatz in vielen Fällen mehr Nachteile als Vorteile.

Denn zunächst ist nicht ausgemacht, dass ein Hackback überhaupt den Richtigen trifft. Einen Angriff im Cyberraum exakt zuzurechnen, ist und bleibt ein sehr schwieriges Unterfangen. Trifft er den Falschen, verpufft seine Wirkung nicht nur im Äther des Cyberspace, sondern beschwört auch erhebliches Eskalationspotenzial herauf. Er kann unerwartete Kaskadeneffekte mit unkalkulierbarem Schadensausmaß nach sich ziehen. Zu Unrecht Angegriffene holen dann womöglich ebenfalls zu einem Gegenschlag aus. Eine „Hackback"-Eskalationsspirale beginnt sich zu drehen. Diese Dynamik gilt es normativ einzufangen und sowohl beabsichtigte als auch unbeabsichtigte Wirkungen auf Dritte mit rechtlichen Sicherungsmechanismen zu begrenzen.

Die Fähigkeit, Hackbacks durchzuführen, setzt typischerweise auch voraus, dass der Staat Cybersicherheitslücken sammelt – vor allem bisher ungeschlossene (sog. Zero-Day-Exploits). Dies schwächt die Cybersicherheit im Allgemeinen, aber auch jedes Einzelnen. Denn jeder, der dieses Einfallstor kennt, kann es für seine (ggf. illegalen) Zwecke ausnutzen. Zero-Day-Exploits zu sammeln, statt Sicherheitslücken zu schließen, ist daher rechtlich und ethisch alles andere als unbedenklich. Jedenfalls bedarf es einer hinreichend klaren Rechtsgrundlage.

Um den angestrebten umfassenden Schutz des digitalen Raums zu verbürgen, gibt es für Deutschland also noch viel zu tun. Bevor nun vorschnell Rufe nach einem Ausbau offensiver Cyberfähigkeiten für Friedenszeiten ertönen, sollten die politischen Entscheidungsträger ihren Fokus auf die bereits verfügbaren defensiven Handlungsoptionen zum Schutz Kritischer Infrastrukturen richten.

In der globalen Ordnung des 21. Jahrhunderts ist Frieden in Europa vor allem Frieden nach außen. Ohne resiliente IT-Systeme wird es diesen im Cyberspace nicht geben. Das gilt nach der Zeitenwende des Ukrainekrieges mehr denn je.

---

[15] BVerfGE 154, 152 (152 f., Ls. 1).
[16] Die neue Cybersicherheitsagenda vom 12. Juli 2022 plant eine solche; *BMI*, Cybersicherheitsagenda des BMI, Juni 2022, S. 6.
[17] A. A. *Franck,* RDV 2022, 3 (4).