spotlight

DIGITALE ZEITENWENDE

Aktive Cyberabwehr als Antwort auf Russlands hybride Kriegsführung

Deutschland steht vor einer wachsenden Bedrohung durch staatlich gelenkte Cyberoperationen, insbesondere aus Russland. Während täglich Tausende von Angriffen deutsche Netzwerke treffen, fehlen der Bundesrepublik nach wie vor zentrale rechtliche und organisatorische Grundlagen für eine aktive und effektive Cyberverteidigung. Dieses Spotlight zeigt auf, wie die neue Bundesregierung Deutschlands Cyber-Resilienz stärken kann, ohne auf risikoreiche Instrumente wie offensive Hackbacks[1] zurückzugreifen.

© picture alliance / Julian Stratenschulte/dpa | Julian Stratenschulte.

VON MIKHAIL POLIANSKII

Im Jahr 2024 verzeichnete das Bundeskriminalamt (BKA) 131.391 inländische Cyberdelikte sowie zusätzliche 201.877 Taten aus dem Ausland.[2] Der Digitalverband Bitkom beziffert den jährlichen Gesamtschaden für deutsche Unternehmen auf 178,6 Milliarden Euro.[3] Besonders schwerwiegend sind die kritischen Vorfälle, die laut Bundesamt für Sicherheit in der Informationstechnik (BSI) 2023 auf Ransomware und DDoS-Attacken gegen kritische Infrastrukturen (KRITIS) entfielen. Das BSI registrierte insgesamt 452 gemeldete Vorfälle, wobei der Gesundheitssektor mit 132 Angriffen am stärksten betroffen war. Bei KRITIS-Betreibern gingen 726 Meldungen ein – 236 mehr als im Vorjahr. Über 800 Unternehmen und Institutionen zeigten 2023 Ransomware-Angriffe an, wobei die Dunkelziffer deutlich höher liegt.[4]

Diese Zahlen spiegeln jedoch nur die Spitze des Eisbergs wider. Kombinierte Signals-Intelligence und Malware-Forensik erlauben mittlerweile belastbare Attributionen, die ein strategisches Muster offenbaren: Ein erheblicher Anteil der schweren Angriffe auf Deutschland wird offiziell Russland zugeschrieben.[5] Die meisten dieser sogenannten APT (Advanced Persistent Threat)-Kampagnen werden den russischen Geheimdiensten GRU (Militärgeheimdienst) oder SVR (Auslandsaufklärung) zugeordnet – also staatlich gelenkten Cyberoperationen.[6]

Im deutschen Diskurs werden diese Attacken oft unter dem Begriff des „Hybriden Krieges (hybrid war)“[7] beschrieben, der das Zusammenspiel nicht-militärischer und digitaler Instrumente unterhalb der Kriegsschwelle charakterisiert.

Dieser Begriff war und bleibt allerdings in wissenschaftlichen und politiknahen Diskussionen in diesem Zusammenhang höchst umstritten.[8] Dieses Spotlight möchte nicht zu dieser terminologischen Auseinandersetzung beitragen, sondern konzentriert sich auf die Cyber-Komponente – also die Sicherheit von Systemen, Software und Netzwerken – der gegenwärtigen Auseinandersetzung mit Russland und die erheblichen Handlungsdefizite Deutschlands in diesem Zusammenhang.

DEUTSCHLANDS STRUKTURELLE SCHWÄCHEN IM CYBERRAUM

Trotz zahlreicher Angriffe, auch auf politische Einrichtungen wie etwa auf die SPD-Parteizentrale 2024,[9] bleibt die Politik zurückhaltend.[10] Noch immer

verfügt Deutschland über keine der aktuellen Bedrohungslage gewachsene ressortübergreifende Nationale Cyberstrategie. Stattdessen gibt es nur eine Cyber-Sicherheitsstrategie von 2021,[11] verfasst vor dem Ukrainekrieg und damit in einer anderen Sicherheitslage.[12] Längst wird eine Nationale Cyberstrategie von unterschiedlichen Gruppen in Wirtschaft, Gesellschaft und Politik gefordert.[13] Es wird vor allem gefordert, dass die Bundesrepublik sich aus der reinen Defensive lösen und über eine Reaktion auf das Handeln anderer Akteure hinausgehen sollte,[14] ohne dabei internationales Recht zu verletzen oder Eskalation hervorzurufen.[15]

Eine strategische Lücke manifestiert sich in unklaren Zuständigkeiten und fehlenden Rules of Engagement zwischen den verschiedenen Behörden.[16] Die föderale Struktur verstärkt diese Problematik zusätzlich. Mit 16 verschiedenen Länder-CERTs (Computer Emergency Response Teams) und komplexen Zuständigkeiten zwischen BSI, BKA, BND und Bundeswehr ist die deutsche Cyber-Sicherheitsarchitektur stark fragmentiert. Das seit 2011 bestehende Nationale Cyber-Abwehrzentrum (NCAZ) fungiert zwar als „Kooperations-, Kommunikations- und Koordinationsplattform" der acht Kernbehörden[17], ist jedoch keine eigenständige Behörde mit Weisungsbefugnissen. Die Koordination erfolgt auf freiwilliger Basis unter Beibehaltung der jeweiligen gesetzlichen Befugnisse. Ob diese Struktur für schnelle, koordinierte Reaktionen auf bundesweite Bedrohungen ausreicht, bleibt umstritten – eine zentrale Incident-Authority mit echter Durchgriffsmacht fehlt nach wie vor.

Auch personell zeigt sich ein gravierender Fachkräftemangel: Der Branchenverband Bitkom schätzt, dass in Deutschland derzeit rund 137.000 IT-Fachkräfte fehlen – inklusive in staatlichen Cyber-Security-Behörden.[18] Diese Lücke wird durch die Konkurrenz mit der Privatwirtschaft und unattraktive Vergütungsstrukturen im Öffentlichen Dienst verschärft.

Eine weitere Herausforderung besteht darin, dass eine aktivere Abwehr in Deutschland in einer rechtlichen Grauzone stattfinden würde. Das Grundgesetz erlaubt dem Bund offensive Maßnahmen nur zur Verteidigung gegen bewaffnete Angriffe; Cyberangriffe bleiben jedoch meist unter dieser Schwelle. Die verfassungsrechtliche Trennung von Polizei, Nachrichtendiensten und Militär erschwert einheitliches Handeln zusätzlich. Die Paragrafen 202a und 303b des Strafgesetzbuches kriminalisieren unbefugtes Eindringen; eine Ausnahmebefugnis für staatliche Maßnahmen der aktiven Cyberverteidigung fehlt völlig.[19] Obwohl der BND in gegnerischen Netzen für Aufklärungszwecke eindringen darf, ist sein Handeln – zum Beispiel beim aktiven Stören laufender Cyberoperationen oder beim Unterbrechen von Datendiebstahl bei deutschen Unternehmen – sehr eingeschränkt.[20]

Vor diesem Hintergrund rückt die Debatte um „Hackbacks" als besonders umstrittene Form der aktiven Gegenmaßnahmen ins Zentrum. Völkerrechtlich bewegen sich Hackbacks in einem komplexen Spannungsfeld zwischen dem *ius ad bellum* (Recht zum Krieg) und dem *ius in bello* (Recht im Krieg). Auf der Ebene des *ius ad bellum* sind Hackbacks nur als *ultima ratio* zulässig, wenn sie notwendig, verhältnismäßig (zum Beispiel als Alternative zu einem konventionellen Schlag) und einem Staat zweifelsfrei zuzuordnen sind.[21] Aber auch in diesem Fall bleibt die Gefahr ungewollter Eskalation hoch, da Schadsoftware häufig zivile Netzwerke tangiert und grenzüberschreitende Kollateralschäden verursachen kann.

INTERNATIONALE ANSÄTZE, BESCHRÄNKUNGEN UND DEUTSCHE HANDLUNGSOPTIONEN

Ein internationaler Vergleich zeigt sowohl erfolgreiche Modelle als auch deren Grenzen auf. Die USA betreiben seit 2018 eine Strategie des *persistent engagement* in Verbindung mit dem bekannten „Defend Forward"-Ansatz, bei der der US Cyber Command feindliche Netze kontinuierlich beobachtet und stört.[22] Diese Strategie beruht jedoch auf enormen Kapazitäten und jahrzehntelanger Erfahrung, die Deutschland nicht ohne weiteres replizieren kann. Zudem ist eine Orientierung an der US-Praxis problematisch, spätestens seit die Trump-Administration einen möglichen Rückzug aus russischen Systemen signalisiert hat, was die Abschreckungswirkung schwächen könnte.[23]

Estland, Lettland und Litauen bieten realistischere Vorbilder.[24] Trotz der überschaubaren Größe dieser Staaten investieren sie nachweislich mehr als Deutschland (gemessen am BIP) in Cyber-Abwehr,[25] unterhalten das angesehene NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn und testen regelmäßig Hunt-Forward-Teams mit den USA.[26] Bemerkenswert ist dabei, dass russische Gruppen baltische Staaten deutlich seltener angreifen als Deutschland – ein klares Indiz für die wahrgenommenen Risiken von Sanktionen oder Gegenangriffen.[27]

Die Erfahrungen europäischer Verbündeter zeigen auch, dass wirksame Cyberabwehr nicht nur technische Fähigkeiten erfordert, sondern auch klare rechtliche Rahmenbedingungen und verlässliche internationale Kooperationsstrukturen. Finnland und Schweden stellen in diesem Zusammenhang ein gutes Vorbild dar.[28] Da diese Länder immer öfter zu Zielen russischer Angriffe nach dem NATO-Beitritt geworden sind,[29] diskutieren sie aktive Cyberabwehr-Optionen, haben jedoch strikte Aufsichtsgremien installiert, um Missbrauch zu verhindern. Deutschland könnte von deren „Responsible Reaction"-Modellen profitieren, ohne die vollen Risiken offensiver Cyberoperationen einzugehen.

Mit anderen Worten: Zwischen rein defensivem Patch-Management und risikoreichen Hackbacks liegt der Mittelweg *der aktiven Cyberabwehr* – temporäres Eindringen in gegnerische Infrastruktur, um laufende Angriffe zu unterbinden oder Beweise zu sichern. Technisch offensiv, strategisch defensiv – diese Maßnahmen könnten Deutschland handlungsfähiger machen, ohne die Eskalationsrisiken umfassender Hackback-Strategien einzugehen.

Das Ziel solcher Operationen wäre nicht die Vergeltung, sondern die Verhinderung von Vorteilen für den Gegner. Wenn

etwa russische APTs Datenbanken abschöpfen, könnten deutsche Cyberteams unbemerkt falsche Daten oder Malware in die gestohlenen Daten einschleusen. Oder falls Moskau Hintertüren in deutsche Software einbaut, könnten Gegenmaßnahmen diese Portale isolieren und neutralisieren, bevor sie genutzt werden. Ziel ist es, dem Gegner den Gewinn zu entziehen: Wenn gestohlene Informationen wertlos oder gegnerische Werkzeuge unbrauchbar werden, hat der Kreml keinen Nutzen mehr vom Angriff.

Das würde den heutigen, rein defensiven Ansatz Deutschlands im Bereich Cybersicherheit, der überwiegend auf die Abwehr gegnerischer Attacken setzt, deutlich ausweiten.[30] In der vorgeschlagenen Form aktiver Cyberabwehr werden die Hacker abgeschreckt, indem jeder Einbruch gezielt ins Leere geführt oder jede Mission verfolgt wird. Solche Gegenmaßnahmen schaffen Unsicherheit und Frustration im Lager des Angreifers und erhöhen potenziell die Kosten russischer Aggression, ohne eine komplette Eskalation des Cyberkriegs zu riskieren. In einer Zeit, in der viele Angriffe zunehmend automatisiert ablaufen und KI-Cyberangriffe zur Routine werden (und damit der Offensive einen deutlichen Vorteil verschaffen), ist es sinnvoll, sich frühzeitig in den Netzwerken der Angreifer zu positionieren, bevor der Angriff erfolgt. Solche Operationen sind aber aufwendig und nehmen meistens mehrere Wochen Vorbereitung in Anspruch.[31] Die Umstellung auf die aktive Cyberabwehr würde dieses Vorgehen ermöglichen.

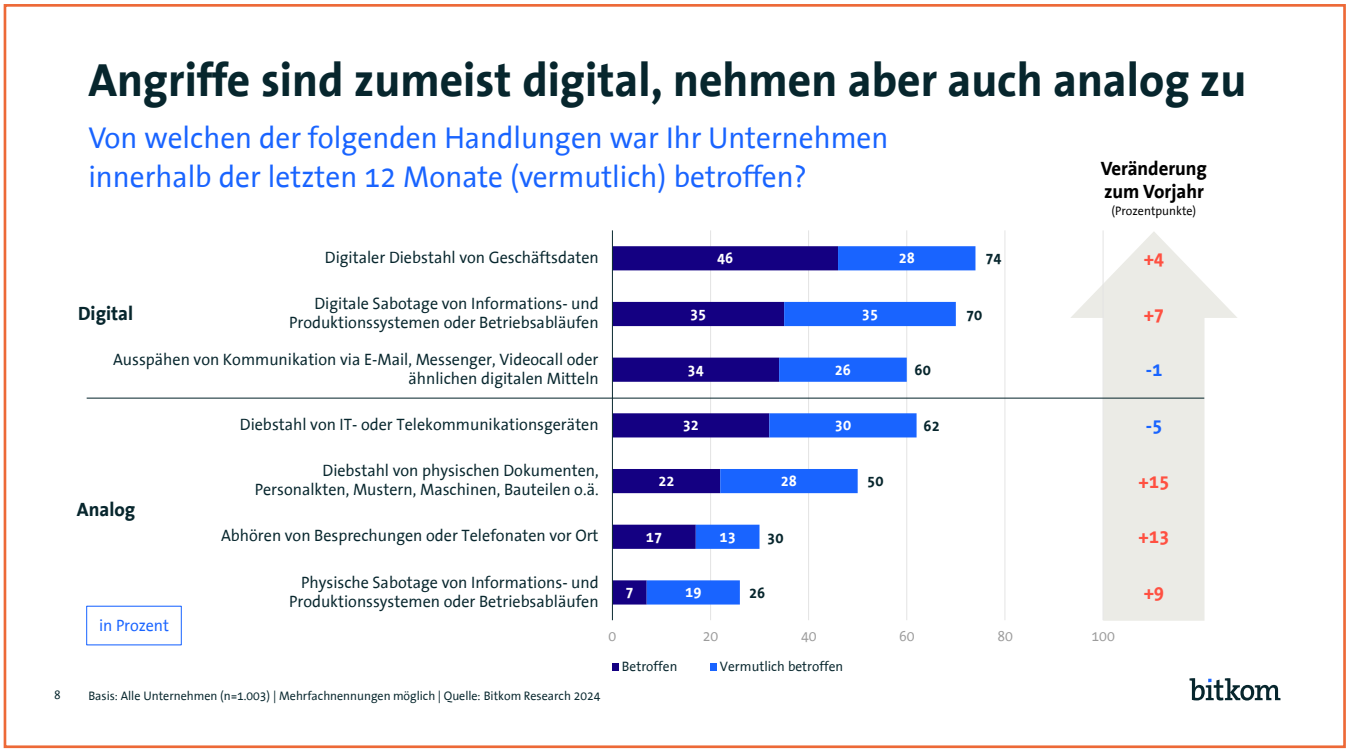
FAZIT UND HANDLUNGSEMPFEHLUNGEN

Deutschland kann die wachsende digitale Bedrohung weder ignorieren noch mit überhasteten Hackback-Strategien beantworten. Resilienz, Attributionstransparenz und international eingebettete aktive Cyberverteidigung bilden die realistische Alternative, um Kosten für Angreifer zu erhöhen und gleichzeitig rechtliche wie politische Risiken zu minimieren.

Der Weg zu einer wirksameren deutschen Cyberstrategie erfordert strukturelle Reformen auf mehreren Ebenen. Zunächst braucht Deutschland eine neue Nationale Cyberstrategie, die ressortübergreifende Zuständigkeiten klärt und verbindliche Rules of Engagement etabliert. Diese Strategie muss Lehren aus dem Ukrainekrieg ziehen und realistische Bedrohungsszenarien für kritische Infrastrukturen durchspielen.

Die föderale Koordination erfordert eine grundlegende Neuorganisation. Ein Bundes-CERT-Ops-Center, das zusammen mit dem schon bestehenden Nationalen Cyber-Abwehrzentrum mit permanenter Lagekarte und automatisiertem Threat-Sharing zwischen Bund und Ländern arbeitet, könnte die bestehende Fragmentierung überwinden. Gleichzeitig sollte eine zentrale Incident-Authority geschaffen werden, die bei schweren Cyberangriffen schnell und koordiniert reagieren kann.

Personell muss Deutschland massiv in die Rekrutierung und Ausbildung von Cyber-Expert*innen investieren. Die Konkurrenzfähigkeit mit der Privatwirtschaft erfordert attraktivere



ZUM AUTOR

Dr. Mikhail Polianskii ist Postdoctoral Researcher am PRIF im Projekt PATTERN. Er forscht zur Außenpolitik Russlands sowie den Russland-EU/NATO-Beziehungen im Rahmen der Europäischen Sicherheit.

KONTAKT
polianskii@prif.org

PRIF, Baseler Str. 27–31, 60329 Frankfurt am Main
PVst, DPAG 43853, Entgelt bezahlt, ISSN-2512-627X

Vergütungsstrukturen und Karrierewege im Öffentlichen Dienst. Internationale Kooperationen, insbesondere mit der NATO (wie CCDCOE), der EU und anderen interessierten Parteien, sollten weiterverfolgt und vertieft werden. Konkret könnte Deutschland eine europäische Cyber-Resilienz-Initiative vorantreiben, die gemeinsame Standards, Ausbildungsprogramme und Forensik-Kapazitäten entwickelt. Völkerrechtliche Initiativen für Due-Diligence-Pflichten bei staatlichen Cyberangriffen können langfristig zu einer Normierung des Cyberraums beitragen.

Rechtlich sollte Deutschland eine gesetzliche Verankerung aktiver Cyberverteidigung im BSI-Gesetz erwägen – als zeitlich, räumlich und sachlich eng begrenztes Instrument zur Gefahrenabwehr, beaufsichtigt durch interdisziplinäre Gremien und parlamentarische Kontrolle. Im Jahr 2024 forderte BSI-Präsidentin Claudia Plattner eine Grundgesetzänderung zur besseren Zusammenarbeit von Bund und Ländern bei der Aufklärung von Cyberangriffen, die aber prompt abgelehnt wurde.[32] Auch bessere und schnellere Attribuierungsverfahren können die politischen Kosten für Angreifer erhöhen.[33]

Die Herausforderung für die neue Bundesregierung ist nicht der Mangel an technischen Möglichkeiten im Land, sondern die fehlende oder zögerliche politische Bereitschaft, bestehende Strukturen zu reformieren und neue Kapazitäten aufzubauen. Nur mit einer umfassenden Neuausrichtung lässt sich Deutschlands Sicherheit im Cyberraum nachhaltig stärken – ohne die Eskalationsspirale eines vollumfänglichen digitalen Schlagabtauschs zu riskieren. Deutschland braucht eine kohärente, rechtlich fundierte und international eingebettete Cyberstrategie, die der Realität permanenter digitaler Bedrohungen gerecht wird.

Der Text entstand im Rahmen des Projekts PATTERN: How Does the Past Matter? Der russische Aggressionskrieg gegen die Ukraine und der Kalte Krieg, das 2025 einen Fokus auf Hybride Bedrohungen legt.

PRIF SPOTLIGHT: Das Peace Research Institute Frankfurt (PRIF) ist das größte Friedensforschungsinstitut in Deutschland. PRIF analysiert die Ursachen gewaltsamer internationaler und innerer Konflikte, erforscht die Bedingungen des Friedens und arbeitet daran, den Friedensgedanken zu verbreiten.

V.i.S.d.P.: Karin Hammer, Öffentlichkeitsarbeit (PRIF), Baseler Straße 27–31, Frankfurt am Main, Telefon (069) 959104-0, info@prif.org, www.prif.org. Design: Anja Feix · Layout: PRIF · Druck: Druckerei Spiegler

Fußnoten und weiterführende Links:
prif.org/spotlight0625-fn
DOI 10.48809/prifspot2506

Peace Research Institute Frankfurt
Leibniz-Institut für
Friedens- und Konfliktforschung

30 Jahre Leibniz Gemeinschaft