DGAP MEMO
Deutsche Gesellschaft für Auswärtige Politik e. V.

Nr. 43
August 2025

Aktive Cyberabwehr: Von der Wirkung zur Toolbox

Dr. Valentin Weber, Senior Research Fellow, DGAP
Ferdinand Gehringer, Policy Advisor Innere Sicherheit und Cybersicherheit, Konrad-Adenauer-Stiftung

Die neue Bundesregierung will in dieser Legislaturperiode den Grundstein für eine erweiterte aktive Cyberabwehr legen. Entscheidend bei diesem Prozess ist, zunächst die angestrebte Wirkung klar zu benennen – ob sie technischer, kognitiver, rechtlicher oder sozioökonomischer Art ist. Darauf aufbauend gilt es, eine Reaktionstoolbox zu entwickeln, die geeignete Maßnahmen der aktiven Cyberabwehr bündelt und deren Chancen und Risiken aufzeigt.

Im Koalitionsvertrag halten die Regierungsparteien fest: „Im Rahmen des verfassungsrechtlich Möglichen bauen wir unsere Fähigkeiten zur aktiven Cyberabwehr aus." Nun stellt sich die Frage, wie dieser Ausbau umgesetzt werden kann. Welche Fähigkeiten der aktiven Cyberabwehr soll Deutschland künftig haben und wer genau sollte darüber verfügen?

Eine einheitliche Definition von aktiver Cyberabwehr gibt es in Deutschland bisher noch nicht. Grundsätzlich umfasst die **aktive Cyberabwehr** alle informationstechnischen Maßnahmen unterhalb der Schwelle des bewaffneten Konflikts, die darauf ausgelegt sind, Cyberangriffe abzuwehren, aufzuklären oder zu stoppen. Die Maßnahmen werden ergriffen, wenn ein konkreter Cyberangriff unmittelbar bevorsteht oder bereits begonnen hat. Zu den einzelnen Maßnahmen der aktiven Cyberabwehr gehören: die Manipulation des Daten- und Internetverkehrs, die Abkopplung, Übernahme oder Ausschaltung der vom Angreifenden genutzten Netzwerk-Ressourcen, die Beseitigung von Schwachstellen und Schadsoftware auf den Systemen des Angegriffenen und das Ausnutzen von (öffentlichen und nicht-öffentlichen) Schwachstellen.

Um dieses Ziel der aktiven Cyberabwehr umzusetzen, sollte die Bundesregierung zunächst Folgendes angehen: **Erstens** festlegen, was sie konkret unter aktiver Cyberabwehr versteht, und **zweitens**, welche Wirkungen durch die verschiedenen Formen der aktiven Cyberabwehr erzeugt werden sollen.

Aus den erforderlichen, anvisierten Wirkungen, die die Maßnahmen erzeugen, lässt sich eine **Reaktionstoolbox** entwickeln, in der die Maßnahmen nach Kategorien – etwa technische Eingriffe, Aufklärung, Täuschung oder internationale Kooperation – geordnet und jeweils mit möglichen Chancen und Risiken verknüpft würden. So ließe sich für verschiedene Anwendungskontexte – zum Beispiel akute Schadensbegrenzung, Abschreckung oder Aufklärung – gezielt eine passende Maßnahme auswählen.

Derzeitige Analysen konzentrieren sich zumeist auf die Möglichkeiten von aktiver Cyberabwehr. Sie konzentrieren sich vorwiegend auf die Infrastruktur des Angreifenden und des Angegriffenen und vernachlässigen dabei die jeweils erzielten weitergehenden Wirkungen. Eine systematisierte Betrachtung der Wirkungen ermöglicht eine umfassendere Kosten-Nutzen-Rechnung und lässt die Folgen der Maßnahme besser abschätzen. Ziel ist ein besseres Verständnis der politischen Handlungsoptionen.

In unserem Memo konzentrieren wir uns daher auf die verschiedenen Wirkungen von Maßnahmen der aktiven Cyberabwehr. Diese lassen sich in technische, kognitive, rechtliche und sozioökonomische Wirkungen kategorisieren. Darauf aufbauend kann im nächsten Schritt eine effektive Reaktionstoolbox entwickelt werden, die künftig für die aktive Cyberabwehr Deutschlands zentral ist.

DIE VERSCHIEDENEN WIRKUNGEN AKTIVER CYBER-ABWEHRMASSNAHMEN

Technische Wirkung: Werkzeuge verändern und Praktiken aufklären

Die technische Wirkung aktiver Cyber-Abwehrmaßnahmen besteht vor allem darin, (gegnerische) Operationen

zu stören oder zu unterbrechen, etwa durch das Ausschalten von Command-and-Control-Servern oder das Umleiten von Datenströmen. Durch gezielte Maßnahmen lassen sich Werkzeuge des Angreifenden verzögern, sabotieren oder vollständig neutralisieren (technische Veränderung). Gleichzeitig können Maßnahmen wertvolle technische Details zu den Infrastrukturen und Schwachstellen des Gegners gewähren (technische Aufklärung). Aktive Cyberabwehr birgt jedoch stets auch das Risiko unbeabsichtigter Nebenwirkungen in unbeteiligten Systemen.

Kognitive Wirkung: Angreifende taktisch irreführen und strategisch abschrecken

Aktive Cyberabwehr kann auf der taktischen Ebene eine kognitive Wirkung bei **staatlichen sowie nichtstaatlichen Akteuren (darunter Cyberkriminelle oder private Gruppen)** hervorrufen. Sie können irreführend, manipulierend oder verunsichernd sein. Um einen Angriff abzumildern, könnten beispielsweise in den Systemen des Angreifenden die Passwörter oder empfangene Daten geändert werden. Die kognitive Ebene des Angreifenden würde so beeinflusst und eventuell fehlgeleitet werden. Dies setzt voraus, dass der Angreifende im Glauben ist, dass die Fehlfunktion in seiner Sphäre oder in seinen Systemen liegt und ohne ein aktives Eingreifen des Verteidigers entstanden ist.

Weiß der Angreifende, dass der Verteidiger in seinen Systemen ist, oder dass er aktiv falsche Daten übermittelt, kann das bei nichtstaatlichen Akteuren eine abschreckende Wirkung erzeugen, auch wenn sich die Grundgedanken der Abschreckung nicht ohne Weiteres auf den Cyberraum – vor allem wegen den Attributions- und Demonstrationsproblemen – übertragen lassen.

Ein gutes Beispiel ist Operation Cronos (2024), eine multinationale polizeiliche Operation unter der Leitung der UK National Crime Agency, an der auch das Landeskriminalamt Schleswig-Holstein und das Bundeskriminalamt teilnahmen. Als Teil der aktiven Cyberabwehr wurden die Server der Ransomware Gruppe Lockbit übernommen und ihre Kunden-Webseite durch ein polizeiliches Banner ersetzt. Diese Kommunikation der Aufdeckung hat zu Abschreckung geführt. Auch zwei Monate nach der Operation Cronos hat Lockbit fast keine neuen Angriffe durchgeführt oder neuen Opfer auf ihre „Leak"-Webseite zur Schau gestellt.

Rechtliche Wirkung: Verantwortungsvolles Rechtsverständnis bekräftigen

Die rechtliche Wirkung aktiver Cyberabwehr zeigt die derzeitigen gesetzlichen Grenzen auf und verdeutlicht die Notwendigkeit zur Schaffung klarer Regeln. Sie befindet sich in einem Spannungsfeld zwischen staatlichem Handlungsanspruch und bestehenden verfassungsrechtlichen sowie völkerrechtlichen Verpflichtungen. Eingriffe in fremde IT-Systeme können als Verletzung staatlicher Souveränität gewertet werden und verfassungsrechtlich bedenklich sein. Selbst technisch begrenzte Eingriffe, etwa das Umleiten von Datenströmen, werfen prozessrechtliche und haftungsrechtliche Fragen auf. Auf nationaler Ebene entsteht dadurch ein Legitimationsproblem, wenn staatliche Stellen ohne klare gesetzliche Grundlage agieren oder ohne ausreichende parlamentarische Kontrolle handeln. Außerdem kann aktive Cyberabwehr zugleich rechtliche Unsicherheit, diplomatische Kontroversen und Vertrauensverlust erzeugen. International bergen solche Maßnahmen das Risiko diplomatischer Spannungen und können als Präzedenzfälle wirken, die bestehendes Völkerrecht infrage stellen.

Sozioökonomische Wirkung: Handlungsfähigkeit demonstrieren und Schäden verhindern

Eine sozioökonomische Wirkung gegenüber der Öffentlichkeit kann vertrauensbildend sein. Wenn über eine erfolgreiche Maßnahme der aktiven Cyberabwehr kommuniziert wird, kann dies mehr Vertrauen in die Sicherheit und Handlungsfähigkeit des Staates aufbauen. Gleichzeitig können aber entstehende (Kollateral-)Schäden oder fehlgeschlagene Abwehrmaßnahmen Misstrauen erzeugen und Haftungsfragen aufwerfen.

Wirtschaftlich betrachtet haben Maßnahmen der aktiven Cyberabwehr unterschiedliche gemischte Wirkungsbilanzen. Für Unternehmen und Behörden ergeben sich Vorteile in Form reduzierter Schadenskosten, da Produktionsausfälle, Datenverluste oder Erpressungszahlungen vermieden werden können. Für Angreifer steigen hingegen die Kosten und Risiken. Sie müssen mehr Ressourcen in Aufklärung, Tool-Entwicklung und Durchführung investieren, während die Rentabilität sinkt. Auf makroökonomischer Ebene können aktive Abwehrmaßnahmen positive Externalitäten erzeugen, indem sie die Resilienz einer Volkswirtschaft erhöhen und neue Märkte für Sicherheitstechnologien fördern. Zugleich profitiert der Versicherungssektor durch sinkende Schadenssummen.

Dem stehen jedoch erhebliche Investitions- und Betriebskosten für Verteidiger gegenüber. Eine Eskalation mit dem Angreifenden ist möglich, was Reputations- oder Folgekosten verursachen kann.

HANDLUNGS-EMPFEHLUNGEN:

Maßnahmen erfassen, Wirkungen systematisieren, Reaktionstoolbox erstellen

Nicht jede Maßnahme der aktiven Cyberabwehr erfüllt alle Wirkungen und schon gar nicht in einheitlichem Maße. Der Einzelfall entscheidet über die Reichweite. Dennoch sollten stets alle Wirkungen berücksichtigt werden. Dafür muss jede Maßnahme der aktiven Cyberabwehr einer Kosten-Nutzen-Analyse unterzogen werden. Hierbei kann eine Reaktionstoolbox unterstützend sein.

Diese Toolbox ist ein digitaler Instrumentenkasten in Form einer Matrix, der die Maßnahmen, deren Wirkungskategorie sowie Chancen und Risiken abbildet. Er kann als Werkzeugkasten dienen, der Entscheidungsträgerinnen und -trägern im Cyberraum hilft, situationsgerecht und unter Abwägung der relevanten Kriterien vorzugehen. Die Handlungsoptionen stehen bereit und politisch Verantwortliche können auswählen, welche Kombination von Maßnahmen sinnvoll ist. Die Chancen und Risiken sind systematisch dokumentiert und ermöglichen eine schnelle vorläufige Kosten-Nutzen-Rechnung. Zugleich schafft sie durch ein festgelegtes Verfahren Legitimation. Kommt es zu einem Cyberangriff auf kritische Energieinfrastruktur, könnten verschiedene Maßnahmen aus der Reaktionstoolbox greifen: **Technisch** beispielsweise die Abschaltung gegnerischer Command-and-Control-Server, um den Angriff sofort zu stoppen – wirksam, aber mit Risiko von Kollateralschäden. **Kognitiv** könnte durch Warnungen und irreführende Daten Verunsicherung und Abschreckung erzeugt werden, wobei Eskalationsgefahr besteht. **Rechtlich** schaffen internationale Konsultationen Legitimität, sind jedoch oft langsamer. **Sozioökonomisch** stärkt transparente Krisenkommunikation das Vertrauen der Bevölkerung, kann aber bei anhaltenden Angriffen ins Gegenteil umschlagen.

Die Bundesregierung hat nun ein günstiges Momentum, um die aktive Cyberabwehr faktenbasiert auf- und auszubauen. Vieles ist technisch möglich, aber nicht alles zielführend. Daher ist der Fokus auf die Wirkung von Maßnahmen der aktiven Cyberabwehr im Rahmen einer Reaktionstoolbox entscheidend. Gleichzeitig erscheint es geboten, auf dieser Basis eine Diskussion darüber zu führen, welche Behörden innerhalb der staatlichen Cybersicherheitsarchitektur welche Befugnisse der aktiven Cyberabwehr erhalten sollten oder auch nicht.

Die Reaktionstoolbox sollte in der überarbeiteten Cybersicherheitsstrategie sowie in der Nationalen Sicherheitsstrategie integriert werden. In diesem Zusammenhang könnte es auch gelingen, das Nationale Cyberabwehrzentrum (Cyber-AZ) zu einer Einrichtung aufzuwerten, die ihren Namen verdient. Das Cyber-AZ könnte als zentraler Ort der Cyberabwehr und Hüter der Reaktionstoolbox das passende Forum für die aktive Cyberabwehr Deutschlands sein. Damit dies verwirklicht werden kann, muss sich die Bundesregierung dringend und prioritär der Sache annehmen, um das entscheidende Momentum für sich zu nutzen.

Advancing foreign policy. Since 1955.

Rauchstraße 17/18
10787 Berlin
Tel. +49 30 254231-0
info@dgap.org
www.dgap.org
𝕏 @dgapev

Die Deutsche Gesellschaft für Auswärtige Politik e.V. (DGAP) forscht und berät zu aktuellen Themen der deutschen und europäischen Außenpolitik. Dieser Text spiegelt die Meinung der Autorinnen und Autoren wider, nicht die der DGAP.

Die DGAP ist gefördert vom Auswärtigen Amt aufgrund eines Beschlusses des Deutschen Bundestages.

Herausgeber
Deutsche Gesellschaft für
Auswärtige Politik e.V.

ISSN 2749-5542

Redaktion Jana Idris

Layout Marie Bauer