Im Zustand des Unfriedens

Staatliche Cyberoperationen unterhalb der Schwelle bewaffneter Konflikte

JOHANNES WIGGEN
Geboren 1993 in Worms, Referent für Cybersicherheit, Hauptabteilung Analyse und Beratung, Konrad-Adenauer-Stiftung.

In den letzten Jahren haben zahlreiche Länder Cyberfähigkeiten entwickelt. Die Anzahl öffentlich bekannt gewordener Cybervorfälle steigt seit einer Dekade stetig. Cyberoperationen sind „weniger aggressiv als offener Krieg, aber alles andere als pazifistisch".[1] Lucas Kello charakterisiert diesen Zustand als „*Unfrieden* oder Rivalität im mittleren Spektrum, die unterhalb der physisch-destruktiven Schwelle zwischenstaatlicher Gewalt liegt, deren schädliche Auswirkungen aber bei Weitem das tolerierbare Ausmaß an Wettbewerb in Friedenszeiten und möglicherweise sogar auch im Krieg übersteigen".[2] Welche Dynamik liegt dieser Auseinandersetzung zugrunde?

Zu unterscheiden ist zwischen Cyberoperationen, die mit Blick auf ihre Effekte und ihren Umfang in das Spektrum bewaffneter Konflikte fallen, und solchen, die unterhalb dieser Schwelle bleiben. Cyberoperationen, die sich gegenwärtig hauptsächlich beobachten lassen, gehören in letztere Kategorie und dienen der Spionage, Sabotage und Subversion.[3] Solche Operationen werden überwiegend von Geheimdiensten durchgeführt. Für Staaten gibt es zahlreiche Anreize, in strategisch wichtige Netzwerke anderer Länder einzudringen.

Ein solches Eindringen in ein bedeutendes Netzwerk kann der Auftakt zu einem Konflikt oder bewaffneten Angriff sein. Hierfür eignet sich vor allem Cybersabotage mit disruptiven, das heißt temporären Störungen oder zerstörerischen Effekten, die zum Beispiel aus einem Cyberangriff gegen Kritische Infrastrukturen wie Kernkraftwerke oder Stromnetze resultieren können. Wenn von einem „Hackerangriff" keine unmittelbare Gefahr ausgeht, kann das Eindringen in ein fremdes Netzwerk der Errichtung eines Brückenkopfes oder der Sammlung interner Informationen dienen. Hierauf können die den Angriff ausführenden Regierungen zu einem späteren Zeitpunkt, zum Beispiel in einem Spannungsfall, zurückkommen, um schneller weitergehende Operationen realisieren zu können. Aus diesem Grund dringen Staaten gegenseitig in die Netzwerke anderer Staaten ein, um ein „Patt" herzustellen und in einem Spannungsfall nicht mit einer Cyberoperation unter Druck gesetzt zu werden.

CYBEROPERATIONEN UND „COVERT ACTION"

Cyberoperationen können auch zum Zweck der Spionage genutzt werden. Die gewonnenen Informationen dienen der Formulierung von Politiken oder Maßnahmen, die künftige Konflikte oder die wirtschaftliche Entwicklung eines Landes beeinflussen können. Cyberspionage ermöglicht es, Einblicke in politische Entscheidungsprozesse und militärische Fähigkeiten eines Landes sowie in Technologien und Geschäftsgeheimnisse von Firmen zu erhalten. Mit sensiblen Informationen, die in „Hacks" erlangt und veröffentlicht werden, können ferner Einflusskampagnen durchgeführt werden. Solche subversiven Aktivitäten verfolgen das Ziel, die Vertrauenswürdigkeit, Integrität oder Verfassung einer bestehenden Ordnung zu unterminieren.

Staaten dringen auch aus defensiven Motiven in fremde Netzwerke ein, um mit den gewonnenen Informationen die Fähigkeit anderer Staaten zur Durchführung von Cyberoperationen zu schwächen. Da aufgrund ihrer Spezifika kaum ersichtlich ist, ob das Eindringen in ein Netzwerk einen offensiven oder lediglich einen defensiven Zweck verfolgt, resultiert hieraus ein schweres Cybersicherheitsdilemma, das Eskalationsrisiken birgt.[4]

Spionage, Sabotage und Subversion, die auch als *covert action* beziehungsweise „verdeckte Aktivitäten“ bezeichnet werden, zeichnen sich dadurch aus, dass sie bis zu einem gewissen Zeitpunkt geheim bleiben müssen: Werden sie entdeckt, ergreift der betroffene Staat Gegenmaßnahmen, was die Operation scheitern lässt und im schlimmsten Fall sogar Vergeltungsschläge nach sich ziehen kann.[5] Gleiches gilt für Cyberoperationen unterhalb der Schwelle bewaffneter Konflikte: Sollen sie erfolgreich sein, müssen Staaten mit Geheimhaltung und Täuschung agieren. Auch wenn die Auswirkungen einer Cyberoperation – beispielsweise bei einem Stromausfall – sichtbar sein können, bleibt die Urheberschaft oder der Zweck dem Betroffenen oftmals verborgen. Umgekehrt können verdeckte Aktivitäten bis zu einem gewissen Grad plausibel abgestritten werden.

CHINAS STRATEGISCHE CYBERSPIONAGEKAMPAGNEN

Was können Regierungen folglich mit verdeckten „Hacks“ bezwecken? Cyberoperationen können in einen strategischen Vorteil münden, wenn sie koordiniert über einen Zeitraum in einer Kampagne durchgeführt werden.[6] Cyberfähigkeiten, die typischerweise geheim gehalten werden, und Cyberoperationen, die verdeckt stattfinden, sind weniger gut geeignet, um die Absichten eines Staates zu signalisieren. Dafür eignen sie sich zum *Shaping,* das heißt zur Formung oder Beeinflussung eines Umfelds: „Die Staaten, die am meisten von Hacking profitieren, sind die, die das geopolitische Umfeld aggressiv so gestalten, dass es mehr zu ihren Gunsten ist als für die, die mit dem Zaunpfahl winken, jemanden zu etwas zwingen oder drohen.“[7]

Exemplarisch für strategische Cyberkampagnen sind Chinas Spionageaktivitäten, die sich bis zur Jahrtausendwende zurückverfolgen lassen.[8] Eine bedeutende Komponente chinesischer Cyberaktivitäten ist Wirtschaftsspionage zur Erlangung ziviler und militärischer Technologien sowie sensibler Geschäftsgeheimnisse. Auf Grundlage der Prioritäten des chinesischen Fünf-Jahres-Plans spionierte seit spätestens 2006 die dem chinesischen Militär zugerechnete Gruppe APT1 *(Advanced Persistent Threat)* mit einem Schwerpunkt in den USA weltweit systematisch Firmen aus. Im Fokus der Cyberkampagne standen Produktdesigns, Testergebnisse, Handbücher und sensible Informationen über Produktionsprozesse und Firmenpolitiken. Ein weiteres Beispiel für chinesische Wirtschaftsspionage ist die Operation *CloudHopper* der Gruppe APT10, die über Jahre die Netzwerke führender Informationstechnologiedienstleister infiltrierte. Von dort aus gelang es den Hackern, in die Netzwerke Hunderter Kunden einzudringen und geistiges Eigentum, Geschäftsgeheimnisse sowie sensible Daten von Firmen in 45 Ländern zu entwenden. Selbst wenn Cyberspionage dadurch erschwert wird, in der

großen Menge an Daten die gesuchten identifizieren, sie anschließend verstehen und für die weitere Nutzung aufbereiten zu müssen, ermöglichte chinesische Wirtschaftsspionage dem früheren Chef des US-amerikanischen Geheimdienstes *National Security Agency* (NSA) zufolge den „größten Wohlstandstransfer in der Geschichte".[9]

Um seinen militärischen Nachteil gegenüber den USA auszugleichen, spionierte China die Hersteller des Transportflugzeugs C-17, des Kampfjets F-35 oder des Flugabwehrraketensystems „Patriot" aus. Diese Informationen ermöglichten China Einblicke in die Funktionsweise der US-Systeme und erleichterten die Entwicklung eigener Waffensysteme. Das Wissen über mögliche Schwachstellen von Waffensystemen könnte ein Staat, zum Beispiel auch mit Cyberoperationen, in einem Konflikt ausnutzen. Neben dem US-Verteidigungsministerium wurde das US-Pazifik-Kommando, das bei einer Auseinandersetzung mit China unmittelbar betroffen wäre, das Ziel chinesischer Cyberspionage. Im Einklang mit Chinas Militärdoktrin wurden auch zivile Logistikdienstleister des US-Transportkommandos ausspioniert, um Erkenntnisse über mögliche Mobilisierungsprozesse zu erlangen. China steht darüber hinaus im Verdacht, große Mengen personenbezogener Daten zu sammeln. Informationen über US-Bundesangestellte von Nachrichtendiensten und dem Militär, wie sie in großem Ausmaß zwischen 2014 und 2015 dem *Office of Personal Management* gestohlen worden sind, können für künftige Anwerbungsversuche genutzt werden oder die Gegenspionage informieren und damit US-Spionageaktivitäten erschweren.

Die Beispiele illustrieren, dass Cyberoperationen die relative Position eines Staates im internationalen System verbessern können, indem sie dazu beitragen, dessen nationale Machtressourcen auszubauen oder die eines anderen Staates zu verringern. Strategische Akteure wägen dabei potenzielle Gewinne einer Cyberoperation gegen die zu erwartenden politischen Kosten – wie einen Reputationsverlust oder einen militärischen Vergeltungsschlag – ab.

ESKALATIONSPRÄVENTION IM CYBERRAUM

Im Gegensatz zu den analogen Versionen von Sabotage, Spionage und Subversion, bei denen zum Beispiel ein Agent erst in ein anderes Land eingeschleust werden muss, stehen die Akteure im Cyberraum in ständigem Kontakt. Während Cyberoperationen gegen komplexe oder gut gesicherte Ziele umfangreichen Know-hows, hochwertiger Geheimdienstinformationen, Zeit und Ressourcen bedürfen, liegen die Einstiegshürden für einfachere Operationen vergleichsweise niedrig. Dadurch bietet der Cyberraum Akteuren mit Blick auf Zeit und Geografie mehr Möglichkeiten, die Initiative zu ergreifen.

Konnten Staaten Spionage, Sabotage und Subversion in der analogen Welt nur in begrenztem Umfang durchführen, können sie mit Informations- und Kommunikationstechnik (IKT) abgestuft vorgehen. Folglich befähigen Cyberoperationen Staaten dazu, verdeckte Aktivitäten in einem – bislang nicht möglichen – Ausmaß anzuwenden, die zusammengenommen strategische Effekte haben können.[10] Welche Folgen ergeben sich aus dieser Entwicklung?

Es lässt sich festhalten, dass Geheimdienst- und Cyberfähigkeiten an Bedeutung gewinnen werden: Der Schutz und die Sammlung von Informationen rückt weiter in den Fokus staatlichen Handelns. So überlegt etwa Großbritannien, die Anzahl seiner Kampfpanzer zu reduzieren und dafür unter anderem seine Cyberfähigkeiten auszubauen. Da in der Wahrnehmung von Staaten die aus niederschwelligen Cyberoperationen resultierenden Vorteile zu verlockend sind, werden sie diese zusehends in ihr außenpolitisches Instrumentarium aufnehmen, was wiederum die Gefahr der Eskalation birgt.

Gegenwärtig sind Staaten auf der Suche nach dem richtigen Umgang mit Cyberoperationen unterhalb der Schwelle bewaffneter Konflikte. In dieser Grauzone ist Abschreckung schwierig, da sie hier unzuverlässig und nicht glaubwürdig ist. Cyberfähigkeiten müssen geheim gehalten werden, um möglichst effektiv zu sein. Im Gegensatz zu anderen Waffen und Kampfstoffen, die abschreckend wirken können, werden offensive Cyberfähigkeiten aufgebaut, um eingesetzt zu werden. Vermutlich werden sich Staaten deshalb auch künftig auf Ebene der Vereinten Nationen nicht ernsthaft auf restriktive Regeln beim Einsatz von Informations- und Kommunikationstechnik einigen können.

VERTRAUENSBILDENDE MASSNAHMEN

Ob Sanktionen oder Ausweisungen von Diplomaten, wie sie die Europäische Union und die USA als Reaktion bereits auf niederschwellige Cyberoperationen eingesetzt haben, das Mittel der Wahl sind, um einen Verhaltenswandel herbeizuführen, kann nicht abschließend beurteilt, darf aber bezweifelt werden. Gegenwärtig dienen solche Maßnahmen und öffentlichkeitswirksame Anklagen mehr dem *naming and shaming.* Bei der Verhängung von Sanktionen oder der Bekanntmachung von Anklagen sollten Staaten deutlich darauf verweisen, gegen welche Prinzipien internationalen Rechts ein Staat mit seinen Cyberoperationen verstoßen hat. Dies kann praktisch zur Einhaltung von Völkerrecht und zur Etablierung von Normen verantwortungsvollen Staatsverhaltens im Cyberraum beitragen. Dabei sollte bedacht werden, dass Geheimdienste aufgrund der Zunahme der von ihnen durchgeführten Operationen Cybernormen mitprägen und damit Einfluss auf das künftige Verhalten von Staaten in Konflikten im Cyberraum haben.[11] Weitere Ansatzpunkte zur

Eskalationsprävention verdeckter Aktivitäten im Cyberraum könnten vertrauensbildende Maßnahmen wie der Dialog über Strategien, der Aufbau von Krisenkommunikationskanälen oder die Kooperation bei gemeinsamen Herausforderungen sein.[12]

Die gegenwärtige Situation im Cyberraum ähnelt einem Zustand „einvernehmlicher" niedrigschwelliger Auseinandersetzung: Staaten nehmen die meisten Cyberoperationen unterhalb einer gewissen Schwelle stillschweigend hin, um innenpolitisch größeren Handlungsspielraum zu haben und die Kommunikation über Interessen in der Grauzone zu erleichtern.[13] Maßnahmen zur Erhöhung des Schutzes von IT-Systemen und zur Steigerung ihrer Resilienz wären die effektivste und am wenigsten Eskalationspotenzial bergende Abwehrstrategie.

[1] Eric Gartzke / Jon R. Lindsay: „Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", in: Security Studies Nr. 2, 2015, S. 316–348, hier S. 346 (Übersetzung S. 346: Johannes Wingen).

[2] Lucas Kello: „The Virtual Weapon and International Order", Yale University Press, New Haven 2017, S. 78 (Übersetzung: Johannes Wingen).

[3] Thomas Rid: „Cyber War Will Not Take Place", in: Journal of Strategic Studies Nr. 1, 2012, S. 5–32.

[4] Ben Buchanan: „The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations", Oxford University Press, Oxford 2017.

[5] Jon R. Lindsay: „Stuxnet and the Limits of Cyber Warfare", in: Security Studies Nr. 3, 2013, S. 365–404, hier S. 387 ff.

[6] Richard J. Harknett / Max Smeets: „Cyber campaigns and strategic outcomes", in: Journal of Strategic Studies 2020, S. 11.

[7] Ben Buchanan: „The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics", Harvard University Press, Cambridge 2020, S. 8 (Übersetzung: Johannes Wingen).

[8] Vgl. Ben Buchanan: 2020, S. 86–107; Harknett / Smeets: 2020, S. 17–23.

[9] Josh Rogin: „NSA Chief: Cybercrime constitutes the ‚greatest transfer of wealth in history'", in: foreignypolicy.com, 09.07.2012, https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history [letzter Zugriff: 24.09.2020].

[10] Michael Warner: „A Matter of Trust: Covert Action Reconsidered", in: Studies in Intelligence Nr. 4, 2019, S. 33–41, hier S. 39.

[11] Alexandra Paulus / Sven Herpig: „Covid-19: Why states now need to consider self-restraint in the cyber domain", in: aboutintel.eu o. A., https://aboutintel.eu/covid-cyber-china [letzter Zugriff: 24.09.2020].

[12] Johannes Wiggen: „Chancen und Grenzen europäischer Cybersicherheitspolitik", Discussion Paper C 261 2020, Zentrum für Europäische Integrationsforschung, Bonn 2020.

[13] Austin Carson: „Secret Wars. Covert Conflict in International Relations", Princeton University Press, Princeton 2018.