Cyberkrieg, -kriminalität, -terror? Eine Typologie

Cyberphänomene lassen sich anhand ihrer Handlungslogik kategorisieren. In seinem Beitrag auf der AKSB-Jahrestagung 2018 gab Dr. Matthias Schulze einen Überblick.

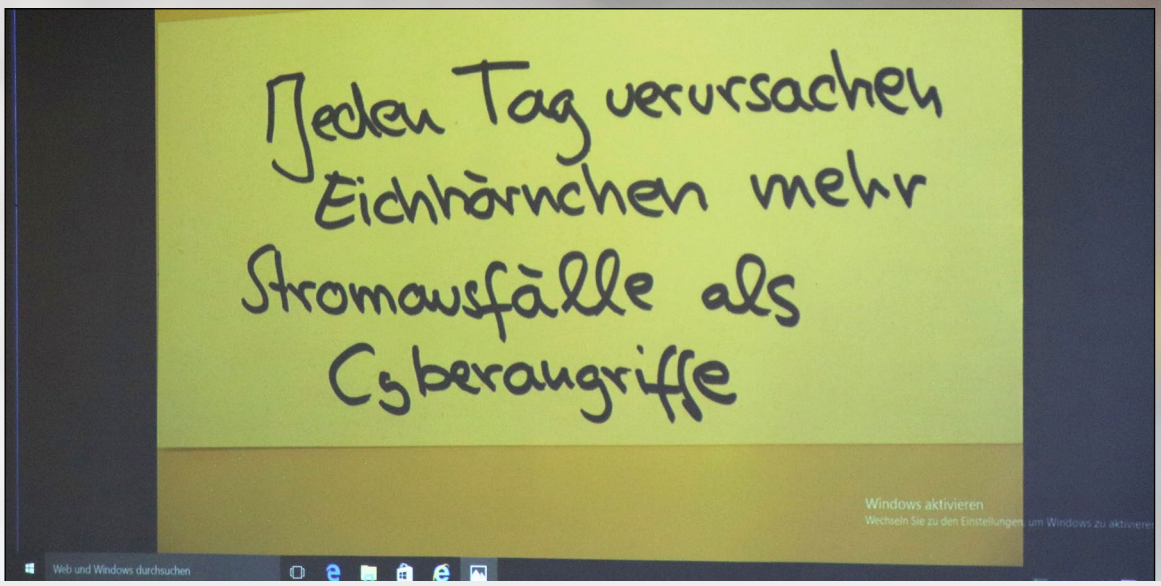
Cyberkrieg ist in den vergangenen Jahren zum Buzzword verkommen (Singer/Friedman 2014: 16). Dabei entsprechen die meisten Cybervorfälle, die durch Medien und Politik bekannt werden, gar nicht den Kriterien von gewaltsamen Konflikten[1] oder gar (zwischenstaatlichen) Kriegen. Rid (2013) argumentiert, dass die meisten Cyberangriffe keine physische Gewalt erzeugen, staatliche Beteiligung schwer nachzuweisen ist und bis zum heutigen Tage kein Mensch durch eine Computerattacke getötet worden ist. Deswegen sei der Begriff des Krieges hier irreführend, da dieser mit Gewalt und Zerstörung mit dem politischen Ziel, den Willen des politischen Gegners zu brechen, einhergeht.

[1] »A contested incompatibility that concerns government and/or territory where the use of armed force between two parties, of which at least one is the government of a state, results in at least 25 battle-related deaths in one calendar year« (Uppsala Conflict Database 2015).

Cybervorfälle kategorisieren

IT-Experte Bruce Schreier (2007) argumentiert, dass nicht jeder Einsatz eines Gewehres ein Akt des Krieges oder ein Angriff ist (Jagd) und somit auch nicht jeder Hack als Cyberangriff gewertet werden sollte. Weil die Intention der Angreifer eine Rolle spielt, ist es sinnvoll, verschiedene Cybervorfälle zu kategorisieren, etwa nach Intensität des Vorfalls (störend, destruktiv), Intention (politisch, sozial, wirtschaftlich), Komplexität & Kosten (je gering bis hoch) und den dominanten Akteuren.

	Ausführende Akteure	Betroffene Ziele	Motivation
Aktivismus & Desinformation	- Individuen - Gruppen - 'state-sponsored' - patriotische Hacker & Proxies	- Zivile Infrastruktur - Medien - Parteien - religiöse Ziele - NGO	- Stören des politischen Diskurses - Politische Polarisierung - Propaganda - Rekrutierung (ISIS)
Vandalismus	- Individuen - Gruppen - 'state-sponsored' - patriotische Hacker & Proxies	- Zivile Infrastruktur - Medien - Parteien - religiöse Ziele - NGO	- Stören des politischen Diskurses - Propaganda - Politische Kommunikation (signaling) - Doxxing
Cyber Crime	- Individuen - organisierte Kriminalität - Staaten mit Cyber-Crime-Nexus (Russland, China, Nordkorea)	- Opportunität der Ziele - Vorwiegend monetäre Infrastrukturen (Banken, Bitcoin-Wallets, Online-Payment, Online-Games, Gambling)	- monetärer Gewinn - Doxxing - Cyber-Crime as a Service - Cover-up für Spionageoperationen (state-sponsored)
Spionage & Überwachung	- Staaten (Nachrichtendienste, Strafverfolgung, Cyberwarfare-Einheiten) - Advanced-Persistent-Threats	- politische Infrastrukturen (Parteien, Regierung, Militär, Nachrichtendienste) - Wirtschaftliche Hochwertziele - Opposition & Dissidenten	- Intelligence gathering - Diebstahl geistigen Eigentums - Doxxing - Diebstahl politisch relevanter Dokumente - Information-Warfare
Cyber Terror (?)	- Unbekannt	- Unbekannt - vermutlich prestigereiche „soft targets" - Strategische kritische Infrastrukturen (Energie, Wasser, Transport, Finanzen)	- Staatliche Übersturzhandlungen produzieren - Signaling
Cyber War (?) (above the threshold of an armed attack)	- Staaten (Nachrichtendienste, Cyberwarefare-Einheiten)	- Ziele von politischer und militärischer Relevanz, aber auch gesellschaftliche Ziele - Strategische kritische Infrastrukturen	- Coercion - Niederringen des Gegners - „adjunct function to physical war" - dauerhafte Störung bzw. Zerstörung von Assets



Nicht alles, was als Cyberangriff gedeutet werden könnte, ist eine geplante Attacke, wie diese Notiz von Dr. Matthias Schulze verdeutlicht. *Foto: AKSB*

Die meisten Vorfälle bewegen sich dabei am mittleren bis unterem Spektrum zwischen Hacktivismus und Spionage. Sie haben in der Regel eine geringe Intensität, das heißt: sie sind nicht-destruktiv, sondern der Schaden ist meist temporär bzw. symbolisch (Imageverlust). Die Einstiegskosten und Komplexität sind gering, sodass eine Vielzahl von Akteuren diesen Aktivitäten nachgehen kann: Individuen, Gruppen und auch Staaten. Insbesondere Website Defacement und Formen des Hacktivismus (zum Beispiel

Eigenschaften	Komplexität und Kosten	Tools	Beispiele
- In der Regel nur störend - nicht invasiv und destruktiv	- Kostenlos bis geringe Kosten - Geringe Komplexität	- Legale Boardmittel von Online-Plattformen - Fake-Accounts	- z. B. Facebook-Initiativen, Gruppen, sponsored Ads - Kreml Internet Research Agency im US-Wahlkampf 2016
- störend - teils invasiv und mit illegalen Mitteln	- geringe Kosten (Botnet for hire (24h/400$) - Geringe Komplexität	- Übernahme von Social-Media-Accounts mit gestohlenen Passwörtern - credential theft & abuse	- Estland DDoS-Angriffe 2007 - Übernahme CDU-Website 2010
- in der Regel nicht störend - Ransomware = störend und disruptiv - automatisiert - n-Day Sicherheitslücken - ca. 600 Mrd. $ an wirtschaftlichen Verlusten jährlich	- Kosten & Nutzen abwägend bzw. Pareto-Prinzip - Kosten Banking-Malware (ca. 900$) - Komplexität: gering bis hoch	- diverse Malware, Ransomware - credential theft & abuse - Phishing - Spam - Bot-Netze - COTS-Trojaner von Schwarzmärkten	- Phone-Phreaking 1970s - Mafiaboy 2000 - Sony-Hack 2011 - Yahoo-Hack 2013 - Ransomware-Welle seit 2014 - Emotet 2019
- im Idealfall unbemerkt - gezielte Angriffe - Hochkomplexe, maßgeschneiderte teure Operationen über lange Zeiträume - Langwierige Planungszeit, Forschung und Entwicklung	- Kosten: je höher der Tarnaufwand, desto kostenintensiver - Komplexität: mittel bis hoch - Marktpreise staatliche Spyware zwischen 10.000 - 1.000.000€)	- professionelle Spyware mit 0-Days - Bundestrojaner - Schadsoftware mit 0-Days - Phishing & Credential-Theft - N-Day Schadsoftware	- Snowden-Dokumente 2013 - Angriff auf den Bundestag 2015 - Hack des Auswärtigen Amtes 2018
- im Idealfall: spektakuläre Schadenswirkung mit eindrucksvollen Bildern	- Kosten & Komplexität müssen hoch sein, um kinetische Wirkung zu erzeugen - Problem: „Bang for the buck"	- Schadsoftware mit 0-Days	- Bisher kein Beispiel! - Cyber-Aktivitäten von Terroristen nur im Bereich Propaganda und Recruiting
- physische Schadenswirkung & „loss of life" - Strategischer Angriff („Black-Scenario") - Hochkomplexe, maßgeschneiderte, teure Operationen über längere Zeiträume - Langwierige Planungszeit, Forschung und Entwicklung	- Kosten: sehr hoch, da vermutlich mehrere simultane Operationen in kurzer Zeitfolge stattfinden müssen, um strategisch wirksam zu sein	- Full-spectrum-Nutzung aller verfügbaren Mittel - Schadsoftware mit 0-Days und Payload mit kinetischem Effekt	- Bisher kein Beispiel!

Foto: Markus Spiske/unsplash.com

DDoS-Angriffe, die zum Ausfall von Websites führen) werden auch zunehmend von staatlichen bzw. staats-nahen Hackern durchgeführt, etwa zum Stören der politischen Opposition (Mansfield-Devine 2015). Zu unterscheiden ist auch die Intention: Politische Vorfälle (etwa von Hacktivisten) zielen auf eine hohe Sichtbarkeit ab (zum Beispiel Website Defacement und Trolling von Nachrichtenseiten) und sind dadurch häufig attribuierbar.

Cybercrime am häufigsten

Die statistisch am häufigsten auftretenden Vorfälle sind ökonomischer Natur: Cybercrime. Es wird in Computer von Unternehmen eingedrungen, um Daten zu extrahieren, etwa geistiges Eigentum (Patente) oder Kundendaten (Kreditkartendaten) zu stehlen (etwa der Sony-Hack 2014, Ashley-Madison-Hack 2015). Beliebte Ziele sind Bezahldienste, zum Beispiel Online-Gambling, Online-Gaming oder Software-Services (Mansfield-Devine 2015, 16). Die Intention ist meist wirtschaftlich, die Steigerung von Profit, zum Beispiel durch den Weiterverkauf von Daten auf dem Schwarzmarkt, Erpressung (Ransomware) oder andere Formen der Monetarisierung, wie etwa Bitcoin-Mining. Zahlreiche Akteure haben ein Interesse an gestohlenen Daten, etwa die organisierte Kriminalität und Hackergruppen. Weil Cybercrime sehr lukrativ bei relativ geringer Einstiegshürde ist, gut skaliert und somit automatisierbar ist und das Entdeckungsrisiko durch Strafverfolgungsbehörden als gering wahrgenommen wird, tummeln sich in diesem Bereich quantitativ betrachtet die meisten bösartigen Hacker.

Cyberaktivitäten von Staaten

Politische und wirtschaftliche Spionage ist die dominante Cyberaktivität von Staaten. Staatliche Daten, wie Sozialversicherungs- oder Steuerdaten, gespeicherte Vorratsdaten oder Listen über Behördenpersonal mit Sicherheitsfreigabe (wie 2015 beim US Office of Personnel Management) sind attraktiv für Nachrichtendienste. Dabei ist das Ziel, möglichst lange, unbemerkt von fremden Systemen, Daten zu extrahieren, was gleichzeitig den Verschleierungsaufwand erhöht und die Operation komplexer werden lässt.

Dr. Matthias Schulze ist wissenschaftlicher Mitarbeiter der Forschungsgruppe Sicherheitspolitik bei der Stiftung Wissenschaft und Politik (SWP) in Berlin. https://www.swp-berlin.org *Foto: SWP*

Cybervorfälle mit Kalkül entwickelt

Zusammenfassend gilt folgende logische Hypothese: Je intensiver die geplante Wirkung (etwa physische Zerstörung), desto komplexer wird Cyberoperation, desto mehr Budget, Know-how und Professionalisierung ist nötig. Dies führt zu Selektion der Akteure. Es ist also keinesfalls so, dass jeder beliebige Hacker komplexe Cyberwaroperationen mit physischen Schäden ausführen kann. Für Cyberterroristen stellt sich die Frage, ob der enorme Kosten- und Personalaufwand am Ende sinnvoll ist oder ob nicht traditionelle terroristische Mittel wie Autobomben »more bang for the buck« generieren (Lewis 2002).

Cyberterrorangriffe hat es bisher noch keine gegeben. Der Großteil terroristischer Aktivität im Internet konzentriert sich auf Propaganda und Rekrutierung. Komplexe, offensive Cyberoperationen wie Stuxnet oder das Abschalten des feindlichen Radars können (bisher) nur mit nachrichtendienstlicher Beteiligung und den finanziellen Reserven von Staaten oder großen Firmen entwickelt werden (Langner 2013). Zudem hat sich weltweit die inoffizielle Norm herausgebildet, dass ein Cyberangriff mit kinetischen Effekten wahrscheinlich nach dem Völkerrecht als bewaffneter Angriff gewertet werden könnte, welcher das Recht zur Selbstverteidigung auslösen könne. Um diese Eskalation zu verhindern, sind die meisten Cybervorfälle bewusst so entwickelt, dass sie unter dieser Eskalationsschwelle (schwarze Linie) bleiben. All diese Gründe sind Teil der Erklärung, warum ein zwischenstaatlicher Cyberwar bisher ausgeblieben ist.

Literatur

Lewis, James A. (2002): Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic & International Studies.

Langner, Ralph (2013): To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve, in: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf; 14.12.2015.

Mansfield-Devine, Steve (2015): The Growth and Evolution of DDoS, in: Network Security 2015:10, 13-20.

Rid, Thomas (2013): Cyber War Will Not Take Place, Oxford.

Schneier, Bruce (2007): Cyberwar, in:https://www.schneier.com/blog/archives/2007/06/cyberwar.html; 14.12.2015..

Singer, P.W./Friedman, Allan (2014): Cybersecurity and Cyberwar. What Everyone Needs to Know, New York.