KEINE AUSSICHT AUF CYBERFRIEDEN

Im Cyberspace kämpfen alle gegen alle: Armeen, Geheimdienste, Behörden, Konzerne, Mafiagruppierungen, Hackerkollektive und Terroristen. Aber es bilden sich auch Normen und Strategien heraus, um mit der Situation umzugehen

Von Philipp von Wussow

Dr. Philipp von Wussow ist Privatdozent für Religionsphilosophie an der Goethe-Universität Frankfurt am Main und leitet am Institut für Theologie und Frieden in Hamburg ein Forschungsprojekt zum Thema Cyberkrieg.

Auf dem Höhepunkt der medialen Berichterstattung um 2009/2010 schien „Cyberkrieg" die nächste große Bedrohung der Menschheit zu sein, vergleichbar allein mit der Atombombe in der Zeit des Kalten Kriegs oder dem Klimawandel in der Gegenwart. Vorstellungen von einem zukünftigen katastrophischen Cyberkrieg, die oft apokalyptische Züge annahmen, gingen meist von großflächigen Angriffen auf sogenannte kritische Infrastrukturen aus – nichtstaatliche Bereiche wie Energie- und Wasserversorgung, Transport, Gesundheit, Banking und Agrar, die von vitalem Interesse für den Staat, wenn nicht für die Aufrechterhaltung der Zivilisation sind. Solche großflächigen Cyberangriffe auf kritische Infrastrukturen hat es nie gegeben und es wird zunehmend unplausibel, dass es sie je geben wird. Denn sie besitzen für staatliche Akteure keinerlei strategischen Nutzen, während sie für nichtstaatliche Akteure, die sich auch ohne strategischen Grund dazu verleitet sehen könnten, zu hohe operationale Anforderungen stellen.[1] Stattdessen spielt sich Cyberkrieg immer stärker in einem Grenzbereich zu Cyberkriminalität und Cyberspionage ab. Ihn einzudämmen, ist das Alltagsgeschäft von IT-Spezialisten. Ihre Arbeit ähnelt zunehmend den Aufgaben einer Straßenmeisterei, die die Schlaglöcher in veralteten Bundesstraßen auffüllt. Tarah Wheeler schrieb dazu in einem viel beachteten Artikel in *Foreign Policy*: „Wenn Cyber-Arbeit nicht langweilig ist, machen wir es falsch."[2]

Typischerweise werden drei ganz verschiedene Dinge als „Cyberkrieg" bezeichnet:

1. Cyberkrieg im engen Sinn wäre ein Krieg zwischen zwei souveränen Staaten, der wesentlich oder ausschließlich mit Cyberwaffen geführt wird. Im Gegensatz zu Cyberkriminalität und Cyberspionage hat es Cyberkriege *in diesem Sinne* bislang nicht gegeben und es gibt keine Anzeichen, dass es sie in naher Zukunft geben wird.

2. Von Cyberkrieg wird auch dort gesprochen, wo begrenzte Cyberangriffe als Vorbereitung eines sogenannten kinetischen Kriegs vorgenommen werden – etwa indem die IT-Infrastruktur des Gegners temporär lahmgelegt wird. Inzwischen ist Cybertechnologie tief in eine Vielzahl von Waffensystemen integriert und diese Technologie schafft neuartige Sicherheitslücken, die von Angreifern ausgenutzt werden können. Kriege der Zukunft werden somit notwendig *auch* Cyberelemente enthalten, doch es scheint, dass eine solche Integration von Cyberelementen in den Krieg letztlich die Vorstellung vom Cyberkrieg obsolet machen wird.

3. Einer weiteren Auffassung zufolge beschreibt die Allgegenwart von Cyberkriminalität und Cyberspionage eine neue Art von Krieg, die den permanenten Ausnahmezustand zum neuen Normalzustand macht. Es handelt sich hier eher um einen Kriegs*zustand* im Sinne des Hobbes'schen Naturzustands, des Kampfes aller gegen alle. Neben staatlichen Akteuren (Armeen, Geheimdiensten und Behörden) kämpfen hier auch Konzerne, Mafiagruppierungen, Hackerkollektive (die teilweise mit staatlichen Stellen zusammenarbeiten) und Terroristen gegeneinander. Cybersicherheitsunternehmen geraten mitunter selbst in Verdacht. Sogenannte Hacktivisten greifen auch ohne direkten Regierungsauftrag aus patriotischen Gründen im Sinne der eigenen Regierung fremde Staaten an.

2017 zwang das in Nordkorea programmierte Virus *WannaCry* zahllose Anzeigetafeln der Deutschen Bahn in die Knie. Der damals 23-jährige Brite Marcus Hutchins verhinderte Schlimmeres, weil er das Virus zufällig entdeckt hatte

Definitionsfragen

Die unzeitgemäße Wiederkehr dieses Zustands fordert in hohem Maß unsere Vorstellungen von Krieg und Frieden heraus. Das neuartige Phänomen stellt viele Prinzipien und Unterscheidungen des westlichen Denkens infrage. Dazu gehören etwa:

▸ **1. Die Unterscheidung zwischen Kombattanten und Nichtkombattanten:** Armeen können ihre Cyberangriffe bis zu einem bestimmten Komplexitätsgrad an nichtmilitärische Akteure auslagern. Damit wird die Attribution von Angriffen zu konkreten Akteuren erschwert – eine Problematik indes, die angesichts der immer besseren und schnelleren Cyberforensik kaum mehr gegeben ist. Doch auch das Outsourcing von staatlichen IT-Aufgaben an den Privatsektor stellt die Unterscheidung zwischen Kombattanten und Nichtkombattanten vor eine schwere Prüfung.

▸ **2. Die Abgrenzung von defensiven und offensiven Fähigkeiten:** Im Cyberkrieg kann man sich nur vorwärts verteidigen. Rein defensive Vorgehensweisen (Firewall, Virenscanner) bieten dagegen keinen ausreichenden Schutz.

▸ **3. Die Proportionalität eines Gegenangriffs:** Viele Angreifer lassen sich mit einem streng proportionalen Gegenangriff gar nicht treffen. Westliche Militärdoktrinen sehen deshalb durchweg vor, dass ein Cyberangriff auch mit konventionellen militärischen Mitteln beantwortet werden kann. Diese Auskunft gilt der strategischen Abschreckung. Gleichwohl würde kein Staat wegen Spionage- oder Ransomware-Angriffen in den Krieg ziehen.

Alle diese Aspekte erscheinen in gewisser Weise nachgeordnet gegenüber der prinzipiellen Unklarheit, inwiefern es sich überhaupt um Krieg handelt – dem Schwebezustand zwischen Krieg und Frieden. Die strategische Bedrohung durch Cyberkriege sorgt für eine Permanenz des Kriegs im Frieden. Hobbes beschreibt dies als den Zustand, in dem „die Furcht vor Tod, Armut oder einem anderen Unglück den ganzen Tag über am Herzen des Menschen [nagt], der aus Sorge über die Zukunft zu weit blickt, und er hat vor seiner Angst nur im Schlaf Ruhe."[3]

Bei Hobbes sollte die These vom Kampf aller gegen alle die *Abkehr* vom Naturzustand und die Begründung der Zivilisation motivieren. Es gibt derzeit keine realistischen Aussichten auf die Etablierung umfassender globaler Sicherheitssysteme, die dem Naturzustand des 21. Jahrhunderts ein Ende bereiten könnten. Insbesondere gibt es keine Aussichten auf Cyberfrieden. Die einzige Möglichkeit zur Einhegung des Cyberkriegs besteht darin, dass sich mit der Zeit Normen herausbilden, die dafür sorgen, dass Cyberangriffe weiterhin unterhalb der Schwelle zum Krieg bleiben. Dies geschieht insbesondere durch Prozesse der Dialog- und Vertrauensbildung zwischen den Cybermächten. Idealerweise führt der diplomatische Dialog zu Vereinbarungen unterhalb der Schwelle des Rechts, die mit der Zeit quasi Gesetzeskraft erlangen.

Auch Cyberabwehr hat viele Akteure

Zugleich bilden sich Verhaltensregeln durch die Klärung der Zuständigkeiten unter den beteiligten Stellen. Das Militär ist einer von vielen Playern im Bereich der staatlichen Cyberabwehr. Gerade im föderalen Deutschland teilt sich die Bundeswehr ihre Aufgaben mit den verschiedenen Landeskriminalämtern, dem BND, dem BSI und verschiedenen Ministerien. International ist die staatliche Cyberabwehr in die NATO und die EU eingebunden. Ferner ergeben sich immer wieder begrenzte Allianzen von hoher Durchschlagskraft, darunter Five Eyes (Australien, Großbritannien, Kanada, Neuseeland, USA) mitsamt ihren diversen Erweiterungen, zu denen teilweise auch Deutschland gehört. Zugleich haben auch Unternehmen, private IT-Sicherheitsfirmen und Cyberversicherungen einen immer größeren Anteil an der Cybersicherheit. Eine funktionierende Cybersicherheit muss letztlich als eine gesamtgesellschaftliche Aufgabe verstanden werden, bei der es unabdingbar ist, auch das alltägliche Nutzerverhalten zu verändern.

Die militärische Komponente ist in der Multipolarität von Kompetenzen und Zuständigkeiten ein wichtiges Element. Es wird vor allem dann bedeutsam sein, wenn ein Angriff militärischer Natur ist. Dies betrifft nicht allein die Ziele, sondern vor allem die Angriffsart, das heißt: den Grad

DIE STRATEGISCHE BEDROHUNG DURCH CYBER-KRIEGE SORGT FÜR EINE PERMANENZ DES KRIEGS IM FRIEDEN.

der Komplexität und strategischen Tiefe. Im Bereich der alltäglichen Cyberkriminalität übernehmen staatliche Stellen nur in geringem Maß selbst Abwehraufgaben und sind weitgehend koordinierend tätig.

Die Aufgaben der militärischen Cyberabwehr liegen also vornehmlich in einem Bereich, der von anderen Beteiligten nicht bedient werden kann. Die Diskussionen über die notwendigen Kapazitäten und Befugnisse des Cyberkommandos der Bundeswehr haben sich stark auf die Frage konzentriert, ob es im Angriffsfall allein seinem defensiven Mandat treu bleiben kann oder gegebenenfalls auch „zurück-hacken" darf, etwa um den Server eines Angreifers abzuschalten. In Wirklichkeit müsste man sich in dieser Situation bereits in den Systemen der Gegner befinden, um tatsächlich etwas ausrichten zu können, anstatt lediglich zu reagieren. Cyberkrieg fordert damit die klassische Abgrenzung von Abwehr und Angriff heraus und die Bundeswehr könnte erst mit der Hinzunahme offensiver Komponenten überhaupt erst ein ernsthafter Player im Cyberkrieg werden. ◢

[1] James Andrew Lewis, Rethinking Cybersecurity. Strategy, Mass Effect, and States, CSIS Technology Policy Program (2018), www.tinyurl.com/zsbw-csis

[2] Tarah Wheeler, In Cyberwar, There Are No Rules. Why the World Desperately Needs Digital Geneva Conventions, in: Foreign Policy (Herbst 2018), S. 34–41: 39.

[3] Thomas Hobbes, Leviathan, übers. Walter Euchner, Berlin 2011, S. 106.