Digitale Sicherheit

Kenneth Geers: Alliance Power for Cyber Security. Washington, D.C.: The Atlantic Council, August 2020

Besprochen von **Oberst i.G. Sönke Marahrens**: German Institute for Defence and Strategic Studies (GIDS), Hamburg, Deutschland; E-Mail: Soenke.marahrens@gids-hamburg.de

https://doi.org/10.1515/sirius-2020-4020

Der Autor Kenneth Geers fordert in seiner Studie die Bildung einer *Cyber Superpower*. Seine Empfehlungen an die EU und NATO hierzu lauten: 1. Teilen von Geheimdienstinformationen und Transparenz, 2. gemeinsame Nachforschungen und Falluntersuchungen, 3. gemeinsames Benennen von Tätern und 4. Begrenzung der Cyberspionage zwischen NATO- und EU-Partnern.

Er sieht die Notwendigkeit einer gemeinsamen internationalen, wertebezogenen Antwort westlicher Nationen auf die Herausforderungen und Möglichkeiten des Internets, da sich nach seiner Auffassung nur so das Paradoxon zwischen der Notwendigkeit der Nutzung des Internets und den damit einhergehenden Risiken von Kriminalität, Spionage, Terrorismus und Krieg auf der staatlichen Ebene auflösen lasse.

Die moderne Gesellschaft gewinnt durch IT mehr als sie verliert. Damit stellt Cybersicherheit eine neue Herausforderung dar – digitale Informationen sind anfällig für Diebstahl, Entzug oder Manipulation. Jeder vernetzte Rechner, egal wie sensitiv seine Inhalte auch sein mögen, ist mit dem Internet verbunden. Aufgrund der Globalität des Internets gehöre Cybersicherheit, wie die globale Erwärmung oder die Corona-Pandemie, zu den internationalen Risiken, die auch nur international gelöst werden können. Aus Sicht von Geers ist jeder nationale Versuch, die eigene Souveränität im Cyberspace zu verteidigen, zum Scheitern verurteilt. Wenn Staaten, wie China oder Russland, versuchten, sich vom Internet abzukoppeln, so werden auch sie durch die Vernetzung der Märkte und den damit verbundenen Vorteilen immer wieder mit der Singularität des Internet konfrontiert. Er untermauert seinen Appell zum gemeinsamen Handeln an die NATO- und EU-Staaten *zum einen* durch die Beschreibung der russischen Anwendungen von Cyberkriegselementen in vergangenen Konflikten und *zum anderen* durch die konkrete historische Entwicklung von Cyberangriffen auf die NATO und ihre Partnerstaaten. Darüber hinaus führt er Reaktionen der NATO an, wie die Gründung des *Cooperative Cyber Defense Centre of Excellence* in Lettland und die Gleichstellung von Cyberattacken mit terroristischen Aktionen und Angriffen mit ballistischen Raketen in der NATO-Strategie von 2010.

Als Antwort auf diese Bedrohungen schlägt der Autor eine *Collective Defense as Collaboration in Chaos* vor. Zur Wahrung der Ideale der Atlantik Charter von 1941 (Selbstbestimmung, zwischenstaatliche Kooperation, Abrüstung und Steigerung der Lebensqualität) gelte es, die mit der Nutzung von IT verbundenen Herausforderungen gemeinsam zu meistern. Cyberspace, Cyberverteidigung und -attacken verlangten nach Sicherheitsnormen, die bislang aufgrund der technischen Eigenschaften nur schwer greifbar seien und deren Kodifizierung durch Cyberaktionen wie *Stuxnet* oder *NotPetya* immer wieder in Frage gestellt werden. Geltendes Recht, welches Konflikte regelt, basiere auf Ländergrenzen oder kinetischen Angriffen. Cyberattacken würden sich aufgrund ihrer (bis dato) *Non*-Lethalität und aufgrund der fehlenden Attribution jeder auf Ländergrenzen bezogenen Zuordnung entziehen und ließen sich

mit traditionellen Vorstellungen von Abschreckung und Vergeltung nicht bekämpfen. Bisherige Versuche nationaler Regelung, wie Chinas *Golden Shield*-Projekt, Russlands SORM (System für Operative Untersuchungsaktivitäten) oder der *US Patriot Act*, hätten bisher mehr zu Befürchtungen der Einschränkung von Menschenrechten geführt, als zu einem wirksamen Schutz gegen Cyberattacken. Denn eine wirksame nationale Strategie finde dort ihre Grenzen, wo zu viel Kontrolle über das Internet ausgeübt werde. So gingen die Vorteile der IT verloren, die Wirtschaft würde einbrechen und die Bevölkerung sich widersetzen. Somit müsste die Unfähigkeit der Abwehr von Cyberattacken eigentlich zu Waffenkontrollregimen, vergleichbar dem Chemiewaffenkontrollabkommen, führen. Jedoch „widersetze" sich hier die IT einer rechtlichen Fassung, weil Begriffsbestimmungen – wie beispielsweise *Malicious Code* – schwierig und konventionelle Inspektionen – aufgrund der Transferierbarkeit und Verschlüsselungsmöglichkeiten von Daten – zum Scheitern verurteilt seien.

Aufgrund dieser Probleme sieht Kenneth Geers die Zukunft eher in digitalen Nichtaggressionspakten, ähnlich der von Russland 1998 gesponserten UN-Resolution 53/70 zur Verurteilung des Missbrauchs von ICT *(Information and Communication Technologies)* durch Kriminelle und Terroristen. Die EU sei mit ihren Regelungen zur Informationssicherheit am weitesten, und die *Council of Europe's Convention on Cybercrime* sei derzeit die einzige international bindende Vereinbarung mit mittlerweile 50 Vertragsstaaten. Da Herausforderungen der Cybersicherheit weder allein durch politische Maßnahmen noch durch eine militärische Allianz gelöst werden können, wäre ein Zusammengehen von EU und NATO die logische Antwort. Die Notwendigkeit eines *Comprehensive Approach* wird anhand einer Fallstudie am Beispiel der russischen Cyberangriffe auf die Ukraine vertieft.

Das Votum des Autors für eine robuste internationale Allianz als einzige *glaubwürdige Cyber Superpower*, in der auch kleinere Staaten aufgrund ihrer höheren Innovationsfähigkeit ihre Bedeutung haben, ist stringent und prinzipiell methodisch sauber hergeleitet. Was Kenneth Geers in seiner Studie aber völlig außen vorlässt, sind die Aktivitäten der jetzigen US-Regierung im Kontext ihrer *America First*-Strategie, die eine Bildung dieser "Cyber Superpower" gemeinsam mit der NATO und der EU in Frage stellt. Das Verprellen von Verbündeten und das Bevorzugen, bzw. Nichtverurteilen von Aktionen von autoritären Regimen, wie Russland und China, führt dazu, dass für die eingangs ausgesprochenen Empfehlungen eine unabdingbare Voraussetzung fehlt – nämlich das Vertrauen.

https://www.atlanticcouncil.org/in-depth-research-reports/report/alliance-power-for-cybersecurity/