Die EU im Cyberspace

Zwischen Aufrüstungszwang und Wirtschaftsförderung

von Thomas Gruber

Der Begriff „Cyberspace" ist sehr unscharf abgegrenzt: Er bezeichnet die virtuelle Welt, also alle computerbasierten Realitäten und Erlebnisräume. Im allgemeinen Sprachgebrauch sind damit meist Computernetzwerke gemeint, in denen sich Nutzer_innen mittels Ein- und Ausgabegeräten bewegen können. Konkrete Beispiele für solche Netzwerke gibt es viele: die Steuerung eines Kraftwerkes, die Kommunikationsstruktur eines Satellitensystems, die Vernetzung von Truppen im Kriegseinsatz oder das Internet. Der Cyberspace setzt sich also aus Netzwerken zusammen, die sich sowohl in ihrer Reichweite (lokal oder global) als auch in ihrer Exklusivität (privat oder öffentlich) unterscheiden. In Größe und Vielfalt hat dabei der zivil genutzte virtuelle Raum eine weit größere Bedeutung als der militärisch und polizeilich besetzte. Und dennoch ist die öffentliche Darstellung genau umgekehrt: Cyberkrieg, Cyberterrorismus und Cyberverbrechen dominieren die mediale Debatte. Diese Schwerpunktsetzung geht vorwiegend von militärischen Bündnissen wie der NATO und den einzelnen Mitgliedsstaaten aus, die den Cyberraum als militärisches und polizeiliches Operationsgebiet begreifen. Ein völlig neues Schlachtfeld also, für das neue Waffen entwickelt, Infrastruktur aufgestellt und Strategien erdacht werden müssen und das sich damit auch als Gelddruckmaschine für Wehrforschung, Militär und Industrie erweist.

Seit Jahrzehnten soll die Diskussion um die „europäische Sicherheits- und Verteidigungspolitik" dabei helfen, auch Kriegseinsätze der EU schrittweise salonfähig zu machen. Doch das Thema Cyberkrieg steht in der Öffentlichkeit bisher noch nicht in Verbindung mit militärischen Strukturen der Union. Die Aufstellung für das fünfte Schlachtfeld verläuft aus europäischer Perspektive also noch etwas holprig, doch wäre es verwunderlich, würde die EU nicht längst mit entsprechenden Strategiepapieren und Organisationsformen aufwarten. Wie also positioniert sich ein Staaten- und Wirtschaftsbündnis mit großen militärischen Ambitionen auf dem neuen, dem virtuellen Schlachtfeld? Welche Strategien und Handlungen gehen daraus hervor?

Die Position der EU im Cyberspace

Parallel zur politischen Struktur der Union besitzt auch das Thema Cyberspace innerhalb der EU eine staatliche, eine wirtschaftliche sowie eine militärische Komponente. Die wichtigsten Eckpunkte für die Cyber-Politik finden sich dabei in der EU-Globalstrategie vom Juni 2016 sowie in entsprechenden Beschlüssen des Parlamentes und der Kommission. Ein zentraler Aspekt der Agenda ist die IT-Sicherheit: Sowohl staatliche Institutionen als auch Unternehmen in der EU sollen in Zukunft besser gegen Cyberangriffe geschützt werden – eine „Kultur der Cybersicherheit" soll entstehen.[1] Diese Aufgabe soll vorrangig von IT-Sicherheitsunternehmen mit Sitz in der EU bewältigt werden. Zum einen ist so gewährleistet, dass das Hintergrundwissen über die Sicherheitsmaßnahmen in der EU verbleibt, zum anderen kann so massiv Wirtschaftsförderung betrieben werden. Günther Oettinger dazu in seiner Position als Kommissar für die Digitale Gesellschaft und Wirtschaft: „Das ist eine großartige Gelegenheit dafür, unsere Cyber-Sicherheitsindustrie auf einem schnell wachsenden Weltmarkt konkurrenzfähig zu machen."[2] Auf militärischer Ebene sind dagegen zwei Strategien offenkundig: Erstens sollen die Cyber-Komponenten in den Einsätzen der Gemeinsamen Sicherheits- und Verteidigungspolitik (kurz: GSVP) gestärkt und die Mitgliedsstaaten so zur Aufrüstung ihrer militärischen Cyber-Kapazitäten gedrängt werden.[3] Zweitens wird politisch der Weg bereitet, um im Falle eines Cyberangriffes auf europäische Institutionen ggf. auch militärisch antworten zu können.[4]

Die militärische Cyber-Agenda wird vornehmlich von EU-Institutionen mithilfe entsprechender Richtlinien und Verträge vorangetrieben. So bildet beispielsweise die 2009 in Kraft getretene „Solidaritätsklausel" des *Vertrages über die Arbeitsweise der Europäischen Union* die Basis für einen Militäreinsatz innerhalb der EU, sollte ein Mitgliedsstaat von einem „Terroranschlag, einer Naturkatastrophe oder einer vom Menschen verursachten Katastrophe betroffen" sein.[5] Auch ein Cyberangriff auf einen europäischen Staat soll dabei explizit von der Solidaritätsklausel abgedeckt werden, was eine militärische Antwort auf eine nicht-militärische Aktion bedeuten könnte: „Das Europäische Parlament […] fordert, […] dass [bei der Solidaritätsklausel] keine bedeutenden Gefahren, wie Cyberangriffe, Pandemien oder Energieengpässe übersehen werden."[6] Das vom Europäischen Rat beschlossene „Cyber Defence Policy Framework"[7] formuliert dagegen Forderungen an die Mitgliedsstaaten und europäischen Institutionen mit dem Ziel, das Thema Cybersicherheit stärker militärisch einzubetten. Die Cyberfähigkeiten der Mitgliedsstaaten in Einsätzen der GSVP sollen verbessert, die zivil-militärische Kooperation sowie die Zusammenarbeit mit der Privatwirtschaft soll gefördert, es sollen verstärkt gemeinsame militärische Manöver durchgeführt und die Vernetzung mit der NATO soll vorangetrieben werden.[8] Als eine wichtige Impulsgeberin für die militärische Cyber-Agenda dient die *Europäische Verteidigungsagentur*[9]: Sie ist verantwortlich für die Entwicklung von Verteidigungsfähigkeiten und damit bedeutend für die GSVP-Missionen. Eines ihrer Themen ist auch die militärische Nutzung des Cyberraums und so war die EDA beispielsweise auch maßgeblich an der Entwicklung des Cyber Defence Policy Framework beteiligt.

Strategien und Manöver

Eine weitere Institution, welche ihren Fokus auf staatliche und wirtschaftliche Aspekte der Cybersicherheit legt, ist die *Europäische Agentur für Netz- und Informationssicherheit*[10], die seit 2005 auf Kreta sitzt. Die ENISA ist

mit Maßnahmen und Empfehlungen zur Cybersicherheit innerhalb der EU – sowohl privater, als auch öffentlicher Institutionen – betraut. In diesem Rahmen findet auch regelmäßig die Großübung „Cyber Europe" statt, an der Behörden und Unternehmen teilnehmen können und während derer das Szenario einer Cyberkrise behandelt wird. Im Jahr 2014 handelte diese Übung beispielsweise von einer energiepolitischen Krise: Während die EU eine Steuer auf fossile Brennstoffe einführt, um die Entwicklung und Implementierung regenerativer Energien zu fördern, greifen Staaten, die „potentiell von jenen Regularien betroffen sind"[11] in breiten Cyberangriffen zunächst EU-Institutionen und dann auch Kraftwerke an. Neben einer stärkeren Vernetzung zwischen dem öffentlichen und dem privaten Sektor sowie einer Steigerung der Wettbewerbsfähigkeit von EU-Unternehmen arbeitet die ENISA damit auch noch einem klaren Feindbild zu: Länder wie Russland, Saudi-Arabien oder Katar wären wohl am ehesten von einer Benachteiligung fossiler Energieträger betroffen.

Noch weiträumiger angelegt ist die vom *Europäischen Auswärtigen Dienst* (kurz: EAD) alle zwei Jahre organisierte „Multi-Layer"-Krisenübung (kurz: ML). Der EAD verfolgt dabei das Ziel, die volle Bandbreite einer GSVP-Mission zu beüben: „Die Übung wird die verschiedenen Schichten des EAD-Krisenreaktionssystems – sowohl zivil, als auch militärisch – und ihre Zusammenarbeit mit anderen EU-Strukturen zur Krisenreaktion behandeln."[12] Dass die aktuellen Übungen eine starke Cyber-Komponente besitzen, ist bei einem medial und militärisch so stark gehypten Thema kaum verwunderlich. Die Übung ML14 handelte beispielsweise von einem Grenzkonflikt in einem fiktiven Staat, in den eine EU-Militärmission eingreift. Während des „Peacebuilding"-Einsatzes werden die EU-Kommunikationsnetze Ziel eines Cyber-Angriffes, den die Truppen abwehren sollen.

Die Übungen machen nur noch offensichtlicher, was der Trend in den Verträgen, Richtlinien und Pressemitteilungen der EU vorgibt: Die Cyber-Komponente in den EU-Militärmissionen sowie die dementsprechenden Fähigkeiten der Streitkräfte sollen gestärkt und die zivil-militärische Zusammenarbeit in diesem Bereich soll stark ausgebaut werden.

Neben der strategischen Ausarbeitung im Krisenfall nimmt der Bereich der Forschung und Entwicklung eine weitere zentrale Rolle in der Cyber-Agenda der EU ein. Innovationen und Gelder sollen wenn möglich in der EU verbleiben – europäische Forschungseinrichtungen und Unternehmen sollen gefördert werden. Auf diesen Zug springt die Gemeinsame Forschungsstelle[13] auf: Die JRC ist eine Großforschungseinrichtung der EU, die beispielsweise Themen der Nuklearforschung, des Verbraucherschutzes sowie der inneren Sicherheit behandelt. Ihre Arbeit im Bereich der Cyber-Bedrohungen konzentriert sich vor allem auf die technische und organisatorische Unterstützung von Trainings und Manövern sowie die Klassifizierung kritischer Infrastruktur und der Schwere von Cyberangriffen.[14] Das größte Förderprogramm für die europäische IT-Sicherheitsindustrie ist die im Juli 2016 beschlossene öffentlich-private Partnerschaft zur Cybersicherheit[15]. Die Cyber-PPP soll der Vernetzung von IT-Sicherheitskonzernen mit öffentlichen Stellen dienen und so explizit mithilfe von Staatsgeldern Wirtschaftsförderung betreiben.[16]

Zusammenfassung und Fazit

Die Rolle, die die EU im Cyberraum einnimmt, ist also weitaus breiter gefächert und unbestimmter, als dies bei Nationalstaaten wie der BRD oder reinen Militärbündnissen wie der NATO der Fall ist. Die Entscheidungsträger_innen der Union scheinen ihre Agenda für den virtuellen Raum an jeder Stelle anbringen zu wollen: Bei der IT-Sicherheit von Behörden und nationalstaatlichen Strukturen, als Ansatz zur Förderung europäischer Unternehmen und – im Kontext von Cyberattacken und -verteidigung – in den Missionen der Gemeinsamen Sicherheits- und Verteidigungspolitik. Der Eindruck, der dabei entsteht, schwankt zwischen einer kalkulierten Platzierung des Themas in allen Arbeitsbereichen des Bündnisses und einem wirren Rundumschlag, der inflationär einen aktuellen Begriff nutzt, um Modernität zu suggerieren.

Aber auch unabhängig von der wahren Intention sind die Auswirkungen der EU-Cyberpolitik offensichtlich: Erstens wird die zivil-militärische Zusammenarbeit unter dem Schlagwort „Cybersicherheit" immer weiter vorangetrieben und selbstverständlicher (siehe z. B. die Multi-Layer-Übungen). Zweitens wird die angebliche Bedrohung durch den „Cyberterrorismus" und den „Cyberwar" genutzt, um Militäreinsätze leichter rechtfertigen zu können (siehe z. B. die sog. „Solidaritätsklausel"). Und drittens werden nicht nur für militärische Zwecke enorme Finanzmittel aus dem EU-Haushalt abgezweigt, sondern auch für die Förderung von Sicherheitsforschung (siehe z. B. die JRC) und Unternehmen (siehe z. B. die Cyber-PPP). Damit ist klar, dass die Cyber-Politik der EU keineswegs der Sicherheit von privater Kommunikation oder ähnlich hehren Zielen dient, sondern nur noch mehr Nährboden für Ökonomisierung und Militarisierung des Bündnisses bieten soll.

Anmerkungen

1 Shared Vision, Common Action: A Stronger Europe, pdf, 16.02.2017, S. 22.
2 Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats, europa.eu, 16.2.2017. Vom Autor aus dem Englischen übersetzt.
3 Shared Vision, Common Action: A Stronger Europe, S. 22.
4 Üben, üben, üben: Wie die EU sich auf den Cyber-Ernstfall vorbereitet, netzpolitik.org, 16.2.2017.
5 Artikel 222 AEUV sowie Gemeinsamer Vorschlag für einen Beschluss des Rates über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union, pdf, 16.02.2017.
6 Entschließung des Europäischen Parlaments vom 22. November 2012 zu den EU-Klauseln über die gegenseitige Verteidigung und Solidarität: politische und operationelle Dimensionen, europarl.europa.eu, 22.02.2017.
7 Z. Dt. etwa: Richtlinien zur Cyberverteidigung.
8 EU Cyber Defence Policy Framework Presents More Than 40 Action Measures, ccdcoe.org, 22.02.2017.
9 EDA: European Defence Agency.
10 ENISA: EU Agency for Network and Information Security.
11 ENISA CE2014 After Action Report, pdf, 22.02.2017, S. 15.
12 EU runs new crisis management exercise, pdf
13 JRC: Joint Research Centre
14 Cybersecurity, ec.europa.eu, 22.02.2017.
15 PPP: Public-Private-Partnership
16 Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats, europa.eu.