(Un)Sicherheitsproduktion im Cyberspace: Cybersecurity-Architekturen in Deutschland und der Schweiz

Hälterlein, Jens

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

BERICHT

(Un)Sicherheits-produktion im Cyberspace

Cybersecurity-Architekturen in Deutschland und der Schweiz

Jens Hälterlein, *Centre for Security and Society (CSS), Albert-Ludwigs-Universität Freiburg, Werthmannstr. 15, 79098 Freiburg (jens.haelterlein@css.uni-freiburg.de)*

Durch die zunehmende IT-Vernetzung von Unternehmen, staatlichen Einrichtungen und kritischen Infrastrukturen ist Cybersecurity seit den 1990er-Jahren zu einem sicherheitspolitischen Thema geworden. Sicherheitspolitik nimmt hierbei die Rolle einer institutionalisierten Technikfolgenabschätzung ein, die bemüht ist, Risiken, die durch Cybercrime und Cyberspionage für Staat, Wirtschaft und Bevölkerung entstehen, zu erkennen, zu bewerten und abzuwehren. Die staatlichen Architekturen und Institutionen der Cybersecurity und Cyberabwehr in Deutschland und der Schweiz standen im Zentrum der Veranstaltung „Cyber-Sicherheit. Architektur und institutionelle Kooperation in Deutschland und der Schweiz“, die vom Centre for Security and Society der Albert-Ludwigs-Universität Freiburg organisiert wurde und am 3. Juni 2019 in Berlin stattfand.

Ausgehend von der These, dass der Auf- und Ausbau institutioneller Vernetzungen und Kooperationen von staatlichen Agenturen einen oder vielleicht sogar den Kern der staatlichen Reaktion auf die neue Bedrohungslage darstellt, sollten im Rahmen von zwei Impulsvorträgen sowie einer Podiumsdiskussion die wesentlichen Unterschiede und Gemeinsamkeiten in den Herangehensweisen in beiden föderalen Staaten herausgearbeitet und die jeweiligen politisch-strategischen oder auch verfassungsrechtlichen Hintergründe thematisiert werden. Das von den Veranstaltern ausgegebene Ziel einer kritischen Reflexion zu den praktischen Grenzen und den strategischen Orientierungen der nationalen Strategien wurde von den Vortragenden und Diskutanten durchaus erfüllt. Wünschenswert wäre es allerdings gewesen, wenn auch der konstitutive Zusammenhang zwischen einer politischen Rhetorik des Cyberterrorismus und Cyberkriegs einerseits und des politisch beabsichtigten Aufbaus von Kapazitäten für eine aktive Cyberabwehr (das sogenannte Hackback) andererseits stärker thematisiert worden wäre. Auch die Frage, inwiefern der wachsende Markt für IT-Sicherheitslösungen aus der Erzeugung von Unsicherheit im Cyberraum profitiert und welche Schlüsse sich daraus ziehen lassen, wurde nicht gestellt.

Widersprüchliche Interessen in nationalen Cybersecurity-Strategien

In seiner Darstellung der staatlichen Cybersicherheitsarchitektur in Deutschland verwies Sven Herpig (Leiter Transatlantisches Cyber-Forum und Mitarbeiter der Stiftung Neue Verantwortung) zunächst auf eine zentrale Entwicklung: Zwar gelte weiterhin der Primat des Zivilen, d. h. defensive, zivile Organisationen waren und sind in Deutschland für die Cybersicherheit verantwortlich. Jedoch werde der militärische Bereich kontinuierlich aufgebaut und aktiver. Auch gäbe es bereits Diskussionen, ob das Militär – analog zum Katastrophenschutz – im Angriffsfall kritische Infrastrukturen verteidigen solle. Dies führe zu der kuriosen Entwicklung, dass das Innenministerium Maßnahmen zur Förderung der Cybersicherheit ankündigt (erstmals geschehen in der Cybersicherheitsstrategie der Bundesregierung von 2016), die zugleich die IT-Sicherheit einschränken. Dies sei beispielsweise der Fall, wenn es dem Verfassungsschutz technisch und rechtlich ermöglicht werden soll, IT-Sicherheitsbarrieren zu überwinden, um an bestimmte Daten zu kommen. Es ergebe sich daraus ein Interessengegensatz zwischen offensiven und defensiven Strategien der Cyberabwehr, der sich auch in unterschiedlichen Interessenlagen der zuständigen Behörden wiederspiegelt. Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) generell daran interessiert ist, dass Sicherheitslücken in einer Software geschlossen werden, möchten die Strafverfolgungsbehörden und Nachrichtendienste diese Sicherheitslücken ggf. ausnutzen oder haben sogar den Wunsch, dass Sicherheitslücken gezielt in Informations- und Kommunikationstechnologien (IKT) eingebaut werden. Das zeige z. B. die aktuelle Diskussion um den neuen Mobilfunkstandard 5G. Solche Sicherheitslücken könnten natürlich wiederum für kriminelle Absichten ausgenutzt werden.

IT-Sicherheit als zentrales Problem

Die Unterscheidung von defensiver und offensiver Cyberabwehr sowie deren zuweilen widersprüchliche Effekte bildeten auch einen Schwerpunkt der Podiumsdiskussion. Bei der Analyse aktueller defensiver Strategien standen Probleme bei der Einschätzung der Bedrohungslage, das fehlende Vertrauen in die Arbeit der staatlichen Behörden, eine Meldepflicht von betroffenen Unternehmen sowie ausstehende gesetzliche Vorgaben für sicherheitskritische IT-Produkte im Zentrum.

Aus der Perspektive von André Duvillard (Delegierter des Sicherheitsverbundes Schweiz) sei es ein zentrales Problem für die nationale Cyberabwehr, dass es keine aussagekräftige Übersicht über Cyberdelikte gibt. Zwar wurde in der zweiten Cybersicher-

https://doi.org/10.14512/tatup.29.1.58

heits-Strategie der Schweiz von 2018 Cybersecurity als nationale Sicherheitsaufgabe definiert und ein Cyberradar zur Identifikation und Analyse von Bedrohungen eingerichtet. Es fehle jedoch an Vertrauen in die Arbeit der Behörden, sodass viele Firmen Vorfälle nicht melden würden. Sie fürchten um ihre Reputation, wenn Cyberangriffe in der Folge einer Meldung publik werden würden. In der Schweiz gibt es keine Meldepflicht und nur ein kleiner Teil der Cyberdelikte werde bei der Polizei zur Anzeige gebracht. Bei den kritischen Infrastrukturen funktioniere das Meldewesen gegenüber den Strafverfolgungsbehörden hingegen recht gut. Auf die Frage hin, ob die von professionellen Hackern durchgeführten Angriffe gar nicht bemerkt werden und gesetzliche Regelungen Anreize für Investitionen in die IT-Sicherheit ihrer Produkte erhielten. Rieger wies zudem darauf hin, dass die Software-Branche die einzige Branche sei, für die nach wie vor keine angemessenen Haftungsregeln und Gewährleistungsansprüche gelten. Der State of the Art in der Entwicklung von sicherer Software habe sich zwar in den letzten Jahren signifikant weiterentwickelt. Dadurch ließen sich nach seiner Schätzung vermutlich 80 % der Cyberangriffe abwehren. Dieser State of the Art komme aber nicht in der Breite zur Anwendung, weil die Unternehmen keine entsprechenden ökonomischen Anreize hätten. Das ausschlaggebende Kriterium bei der Produktentwicklung sei weiterhin *time-to-market*.

Die Dunkelziffer von Cyberangriffen, vor allem von nachrichtendienstlichen Cyberaktivitäten im Wirtschaftsspionagebereich, ist hoch.

bei Cybercrime mithin mit einem großen Dunkelfeld zu rechnen sei, betonte Frank Rieger (Sprecher des Chaos Computer Club), dass es zwar generell schwierig sei, über das Dunkelfeld Aussagen zu treffen, es aber dennoch anzunehmen sei, dass viele, vor allem nachrichtendienstliche Cyberaktivitäten im Wirtschaftsspionagebereich gar nicht sichtbar werden.

Sichtbar werden solche Aktivitäten häufig erst, wenn Probleme mit der Funktionalität eines betroffenen IT-Systems festgestellt werden oder wenn gestohlene Daten im Netz auftauchen. Eine Meldepflicht sei daher prinzipiell sinnvoll, da nur so überhaupt die Chance entstehe, einen Überblick über die Bedrohungslage zu bekommen. Wenn es aber darum gehe, die IT-Sicherheit zu erhöhen und Prävention von Cybercrime zu betreiben, sei das eigentliche Problem die Definition und Durchsetzung von branchenspezifischen Sicherheitsanforderungen. Es gäbe zwar Ansätze in diese Richtung. Dabei gehe es aber vor allem um Audit-Prozesse und weniger um konkrete technische Sicherheit. Auch gibt es durchaus Zertifizierungsprozesse für die IT-Sicherheit von Produkten, z. B. medizinischen Geräten. Diese Prozesse dauern aber zuweilen so lange, dass ein Gerät, das ursprünglich den Sicherheitsstandards entsprach, zum Zeitpunkt seiner erfolgten Zertifizierung nicht mehr sicher ist. Verkompliziert werde die Situation dadurch, dass ein Patch – also die Aktualisierung eines Computerprogramms oder seiner unterstützenden Daten – die Zertifizierung außer Kraft setzen würde. Die Dynamisierung des technischen Sicherheitsprozesses stecke insofern noch in den Kinderschuhen.

Manuel Bach (Leiter Nationales Cyber-Abwehrzentrum, BSI) fügte hinzu, dass sich die Bedrohungslage im Bereich Cybercrime durch das Internet der Dinge verändert habe, da dort viel „IT-Unsicherheit“ eingebaut sei. Einig waren sich die Diskutierenden weitestgehend darin, dass der Staat an diesem Punkt aktiv werden müsse, da die Hersteller nur durch entsprechende

Aktive Cyberabwehr nicht zielführend

Bei der anschließenden Bewertung der gegenwärtig diskutierten offensiven Maßnahmen und Strategien der Cyberabwehr standen Fragen der Effektivität und Angemessenheit im Vordergrund. Matthias Schulze (Mitarbeiter im Bereich Cyber-Sicherheitspolitik der Stiftung Wissenschaft und Politik) verwies zunächst auf die völkerrechtliche Problematik solcher Maßnahmen. Darüber hinaus stellte er deren Wirksamkeit infrage. Ob das Löschen von gestohlenen Daten oder das Zerstören der zum Angriff genutzten IT-Systeme eine präventive Wirkung habe, sei anzuzweifeln. Frank Rieger fügt hinzu, dass das Risiko von Kollateralschäden bei diesen Gegenangriffen mittlerweile immens sei, wenn etwa Cloud-Dienste betroffen sind. Auch gebe es ein generelles Attributionsproblem, da die Verursacher von Cyberangriffen nicht verlässlich identifizierbar sind.

Weitere Informationen

Konferenzprogramm und zusätzliche Informationen:
https://www.css.uni-freiburg.de/fileadmin/primary/Public/user_uploads/Aktuelles-News/CSS_Cyber-Sicherheit_-_Berlin_3._Juni2019.pdf