POLICY BRIEF NO. 4

SCHAFFUNG EINER UMFASSENDEN UND KONSISTENTEN EU-CYBER-SICHERHEITSPOLITIK

Die Herausforderung: Aufbau einer kohärenten EU-Cybersicherheitspolitik

In den letzten Jahren wurden auf EU-Ebene zahlreiche Richtlinien und Regulierungsmaßnahmen zur Cybersicherheit verabschiedet. Sie konzentrierten sich hauptsächlich auf die Bereiche des Binnenmarkts und des Strafrechts, um die Sicherheit von Bürgern, Unternehmen und öffentlichen Verwaltungen im digitalen Umfeld zu verbessern. Es fehlt jedoch an Konsistenz in diesen Richtlinien und Vorschriften, was zu einer Vielzahl von Überschneidungen, aber auch zu sich widersprechenden Verpflichtungen führt. Ein aktuelles Beispiel für diese mangelnde Konsistenz ist der Vorschlag der Europäischen Kommission, wonach die Strafverfolgungsbehörden grenzüberschreitenden Zugang zu Daten haben sollen (e-Evidence). Eine Studie, die diesen Vorschlag analysierte, kam aber zum Schluss, dass die verstärkte Kooperationsregelung, die einen raschen Zugang der EU-Mitgliedstaaten zu Providerdaten ermöglicht, die Mitgliedstaaten (MS) hemmen würde, die Verantwortung für einen wirksamen Schutz der Grundrechte in ihrem Hoheitsgebiet zu übernehmen. Ferner würde sie Rechtsunsicherheit sowohl für die Dienstanbieter als auch für die einzelnen Nutzer schaffen.

Strategiedokumente und Legislativmaßnahmen betreffen oft nur bestimmte Aspekte der Cybersicherheit und werden beschlossen, ohne sie in der Gesamtheit des Rechtsrahmens zu berücksichtigen.

Das Konzept „Cybersicherheit“ entwickelt sich weiter

Es wird oft angenommen, dass es schwierig ist, eine einheitliche Politik im Bereich der Cybersicherheit zu erreichen, weil Begriff und Geltungsbereich von Cybersicherheit unterschiedlich verstanden werden können. Zahlreiche Definitionen von „Cybersicherheit“ werden auf europäischer und nationaler Ebene von EU-Institutionen, Interessengruppen und EU-Mitgliedstaaten verwendet. Diese Definitionen von Cybersicherheit variieren und hängen von Adressaten, Kontext und dem Regelungsbereich ab, in dem sie eingesetzt werden. Die Diskussionen um die EU-Cybersicherheit umfassen

Die EU und ihre Mitgliedstaaten definieren Cybersicherheit unterschiedlich

So lautet beispielsweise die Definition der Cybersicherheitsstrategie der Europäischen Union von 2013 wie folgt: „Der Begriff ‚Cybersicherheit' bezeichnet im Allgemeinen die Sicherheitsfunktionen und Maßnahmen, die sowohl im zivilen als auch im militärischen Bereich zum Schutz des Cyberraums vor Bedrohungen eingesetzt werden können, die im Zusammenhang mit seinen voneinander abhängigen Netzen und Informationsstrukturen stehen oder diese beeinträchtigen können. Bei der Cybersicherheit geht es darum, die Verfügbarkeit und Integrität von Netzen und Infrastrukturen sowie die Vertraulichkeit der darin enthaltenen Informationen zu erhalten." Demgegenüber haben die EU-Mitgliedstaaten auf nationaler Ebene Cybersicherheitsdefinitionen entwickelt, die nationale Ansätze zur Bewältigung von Herausforderungen und Bedrohungen der Cybersicherheit erfassen. So besagt beispielsweise die Cybersicherheitsstrategie der Tschechischen Republik für den Zeitraum 2015-2020: 'Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace [...]'. Die Luxemburger Nationale Cybersicherheitsstrategie III 2018 besagt, Cybersicherheit 'is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets.', wobei der Schwerpunkt auf den Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit liegt. Auch in den Strategiedokumenten anderer Länder gibt es sehr unterschiedliche Definitionen, deren Geltungsbereiche sehr begrenzt bis global umfassend sind.

verschiedene Aspekte wie Cyber-Resilienz, Cyberkriminalität, Cyberabwehr, sowie Cybersicherheit im engeren Sinne sowie andere globale Cyberspace-Fragen.

Strategiedokumente und Legislativmaßnahmen betreffen oft nur bestimmte Aspekte der Cybersicherheit und werden beschlossen, ohne sie in der Gesamtheit des Rechtsrahmens zu berücksichtigen. Beispiele für solche Aspekte sind Bereiche der Cyberkriminalität, Maßnahmen zur Netz- und Informationssicherheit (für Betreiber grundlegender Dienste oder Betreiber kritischer Infrastrukturen) und der elektronischen Kommunikation, was Fragen des Datenschutzes mit einschließt. Versuche, Cybersicherheit richtig zu konzeptualisieren sind dadurch erschwert, dass die Grenzen zwischen den verschiedenen Cybersicherheitsbereichen verschwimmen.

Die unterschiedlichen Wortbedeutungen des Begriffs „Cybersicherheit" haben sowohl Vor- als auch Nachteile. Der Begriff erlangt so eine gewisse Flexibilität, um an veränderte Bedingungen angepasst werden zu können. Gleichzeitig kann jedoch ein sich ständig wandelnder Begriff übermäßig integrativ oder umfassend werden, was eine kohärente Regulierung in diesem Bereich erschwert oder gar verhindert. Dies verursacht auch Reibung zwischen der EU und der Staatsgewalt der Mitgliedstaaten, insbesondere im Bereich der nationalen Sicherheit. Daher sollte die Unklarheit des Begriffs „Cybersicherheit" in der EU adressiert werden, um regulatorische Unklarheiten und institutionelle Verantwortlichkeiten zu addressieren.

Fehlende EU-Kompetenz für die Regulierung der Cybersicherheit

Die Herausforderung, eine umfassende und kohärente Cybersicherheitspolitik zu schaffen, wird durch unklare Zuständigkeiten der EU für die Gesetzgebung in Fragen der Cybersicherheit noch verstärkt. Die EU hat im Grundsatz nur die Befugnisse, die ihr von den Mitgliedstaaten in den Verträgen übertragen wurden. Sie kann über ausschließliche Zuständigkeit, geteilte Zuständigkeit oder die Kompetenz verfügen, unterstützende, koordinierende oder ergänzende Maßnahmen zu ergreifen. Da die Cybersicherheit nicht als Teil eines bestehenden Bereichs erwähnt wird, strebt die EU nach statthafter juristischer Begründung für ihre Regulierungsmaßnahmen der Cybersicherheit in bestimmten Regulierungsbereichen. So wurde beispiels-

weise im Vorschlag der Europäischen Kommission für die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) festgestellt, dass die Praktiken der verschiedenen Mitgliedstaaten in Bezug auf Cybersicherheitsmaßnahmen dazu führen dass „[...] Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die Sicherheit von Netz- und Informationssystemen in der Union generell untergraben wird." Mit anderen Worten, es wird darauf hingewiesen dass zusätzliche (Cyber-)Sicherheitsmaßnahmen erforderlich sind. Diese nicht eindeutige Verwendung des Begriffs „Cybersicherheit" in mehreren EU-Dokumenten und -Maßnahmen ist kein Zufall. Sie deutet darauf hin, dass es möglicherweise ein „Kompetenzproblem" gibt, das für die Beziehungen zwischen der EU und ihren Mitgliedstaaten von grundlegender Bedeutung ist. Die Anerkennung der internen, externen und auch der verteidigungspolitischen Dimension der Cybersicherheit erfordert eine sorgfältige Prüfung der EU-Kompetenzermächtigung durch die EU-Mitgliedstaaten sowie der Auslegung der EU-Kompetenz durch deren Organe.

Förderung der Zusammenarbeit zwischen den Interessengruppen

Die Bekämpfung von Bedrohungen der Cybersicherheit muss als eine Angelegenheit erkannt werden, die die Expertise und Zusammenarbeit von Interessengruppen (Stakeholder) aus verschiedenen Bereichen wie IT, Psychologie, Recht, Bildung, Wirtschaft und Politik erfordert. Die EU verfolgt bereits einen solchen Multi-Stakeholder-Ansatz mit einer initialen Einbeziehung des öffentlichen und privaten Sektors, einschließlich der nationalen Regierungen, Internet-Provider, Technologie- und Sicherheitsunternehmen, Unternehmen und der Zivilgesellschaft, um die Bedrohungen der Cybersicherheit zu bekämpfen. Eine solche Zusammenarbeit könnte jedoch noch mehr gefördert werden.

Institutionelle Zusammenarbeit auf EU-Ebene

Auf EU-Ebene konzentrieren sich bereits eine Reihe von EU-Institutionen, -Agenturen und -Dienststellen auf Fragen der Cybersicherheit, wie beispielsweise die EC Directorate Generals (zum Beispiel die DG CONNECT, DG for Mobility and Transport, and DG Joint Research Centre). Während bereits einige Anstrengungen unternommen wurden, um eine Zusammenarbeit zwischen diesen Generaldirektionen und verschiedenen Abteilungen innerhalb diesen herzustellen, handelt es sich jedoch bei einigen davon nur um informelle Verfahren. Derweil haben jene Kooperationen, die bereits durch formale Regeln gesteuert werden noch nicht ihr volles Potenzial entfaltet. Darüber hinaus ist aufgrund der ständig zunehmenden Bedeutung und Abhängigkeit der Gesellschaften von ICT zu erwarten, dass die Zahl der mit Cybersicherheitsfragen befassten DGs zunehmen wird. Die Organe und Einrichtungen der EU, welche an verschiedenen Aspekten der Cybersicherheitspolitik arbeiten, sind bereits bestrebt, ihre Zusammenarbeit sowohl auf formelle als auch auf informelle Weise zu pflegen, wie z. B. durch Netzwerke von Fachexperten, Konferenzen und Treffen mit mehreren Interessengruppen. Für den Erfolg eines jeden Multi-Stakeholder-Ansatzes ist jedoch eine umfassendere Governance-Struktur Voraussetzung. Bisher waren die Bemühungen um den Aufbau einer institutionellen Zusammenarbeit meist inkonsistent, unvollständig und nicht effizient genug. Daher sollten zukünftige politische Initiativen die Rollen, Kompetenzen und Missionsziele der beteiligten Bereiche und Akteure klar voneinander unterscheiden. Dies ist besonders wichtig bei der Entscheidung, ob eine eher offensive oder eher defensive Cybersicherheitsstrategie verfolgt werden sollen. Ein Beispiel für eine solche Entscheidung wären die Debatten um die Nutzung des sogenannten rechtmäßigen Zugangs durch Sicherheitsbehörden, wirksame Verschlüsselung ohne Hintertüren oder die Nutzung von Zero-Day-Exploits.

Dabei sollte die Europäische Union versuchen, ernsthaft auf Bedenken im Hinblick auf eine mögliche Schwächung der gesamten IT-Sicherheitslandschaft, der Privatsphäre und des Datenschutzes sowie der

Menschenrechte im Allgemeinen einzugehen. Die Empfehlung ist, Sicherheitsexperten, Datenschutzbehörden, Menschenrechtsaktivisten und die breite Öffentlichkeit einzubeziehen, wenn es darum geht, ein ausgewogeneres Verhältnis zwischen den Bedürfnissen der Strafverfolgung und den Bürgerrechten herzustellen. Der kürzlich verabschiedete Rechtsakt zum Cybersicherheitsgesetz ist eine positive Entwicklung, da er zumindest die Governance-Struktur besser klärt, indem er die verschiedenen Rollen der ENISA festlegt. Sie soll die EU zu Fragen der Cybersicherheit beraten, einen zentralen Anlaufpunkt für Fachwissen bieten und soll auf diese Weise die Zusammenarbeit und Koordination zwischen den verschiedenen Interessengruppen erleichtern.

Institutionelle Zusammenarbeit auf nationaler Ebene

Die EU-Cybersicherheitsstrategien 2013 und 2017 fordern einen umfassenden Ansatz für den Schutz der Cybersicherheit. Dies betrifft auch nationale Ansätze zur Cybersicherheit. Die Kooperationsmechanismen, die sich von der EU-Ebene bis zu den Institutionen der Mitgliedstaaten erstrecken, könnten weiter verbessert werden. Obwohl es verschiedene Kooperationsgruppen wie den Europäischen Datenschutzausschuss und das Gremium der Europäischen Regulierungsstellen für elektronische Kommunikation (GEREK) gibt, sind einige von ihnen stark unterbesetzt oder verfügen nicht über ihr volles Effizienzpotential, da es schwierig ist, alle relevanten Akteure ausreichend einzubeziehen. In einigen Fällen verfügen Entitäten und Regulierungsbehörden, welche für verschiedene Bereiche der Cybersicherheit innerhalb eines Landes zuständig sind, derzeit noch nicht über eine effektive Kommunikationspraxis. So könnte beispielsweise auf nationaler Ebene das Fachwissen und der Informationsaustausch zwischen den CERTs und Strafverfolgungsbehörden noch verbessert werden. Bei der Behandlung dieses Themas sollten die Mitgliedstaaten ermutigt werden, kohärentere Regeln und Mechanismen für den Informationsaustausch im Einklang mit den EU-Werten und den Grundrechten der Bürger festzulegen. Während die meisten Mitgliedstaaten ihre ersten Cybersicherheitsstrategien vor der Verabschiedung der NIS-Richtlinie entwickelt haben, kann diese zu einer weiteren Detaillierung des Regulierungsrahmens auf nationaler Ebene beitragen, indem sie die Rollen und Verantwortlichkeiten der Interessengruppen im öffentlichen und privaten Sektor definiert. Bei der Erwägung von Änderungen, die erforderlich sind, um eine wirksame Zusammenarbeit in Fragen der Cybersicherheit zu erleichtern, sollten die höchsten Standards der Rechtsstaatlichkeit und des Schutzes der Grundrechte eingehalten werden. Dies ist besonders wichtig für die Bereiche der Strafverfolgung und des Strafverfahrens, in denen ein sorgfältiger Ausgleich zwischen den Interessen von Staaten, Gesellschaften und Einzelpersonen gefunden werden muss. Konsequenterweise sollten die politischen Entscheidungsträger ein klares Verständnis für die Grenzen der Zusammenarbeit im Bereich der Cybersicherheit auf der Grundlage von Rechtmäßigkeits- und Rechtsgrundsätzen entwickeln und versuchen, entsprechende Kohärenz über eine Vielzahl von Rechtsvorschriften hinweg zu erhalten.

Mehr Informationen

Dieser Policy Brief basiert auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity). Detaillierte Berichte über diese Arbeit wurden in vier wichtigen Whitepapers in englischer Sprache veröffentlicht:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Opinions Regarding Cybersecurity
4. Technological Challenges in Cybersecurity

Alle Whitepapers finden Sie auf unserer Website, zusammen mit allen unseren (herunterladbaren und druckbaren) Policy Briefs, kurze Online-Erklärungen zu den wichtigsten Fragen der Cybersicherheit und kommentierte Literaturlisten zur vertieften Lektüre:

canvas-project.eu

Darüber hinaus finden Sie auf unserer Website noch mehr CANVAS Projektmaterial:

CANVAS Reference Curriculum
(Integration der Werteperspektive in die Aus- und Weiterbildung im Bereich Cybersicherheit)

CANVAS MOOC
(Massive Open Online Kurs)

Open Access Buch
“The Ethics of Cybersecurity”

Kofinanziert durch das Programm „Horizont 2020“ der Europäischen Union

Das Projekt CANVAS (Constructing an Alliance for Value-driven Cybersecurity) wurde im Rahmen der Fördervereinbarung Nr. 700540 aus dem Forschungs- und Innovationsprogramm Horizon 2020 der Europäischen Union finanziert. Diese Arbeit wurde (teilweise) vom Staatssekretariat für Bildung, Forschung und Innovation (SERI) unter der Vertragsnummer 16.0052-1 unterstützt. Die darin geäußerten Meinungen und Argumente spiegeln nicht unbedingt die offizielle Meinung der Schweizer Regierung wider.

Projektdauer:
September 2016 – Oktober 2019

Ziel von CANVAS:
Die Zusammenführung von Interessengruppen aus Schlüsselbereichen der Europäischen Digitalen Agenda, um der Herausforderung zu begegnen, wie die Cybersicherheit mit den europäischen Werten und Grundrechten in Einklang gebracht werden kann.

Partner:
Das CANVAS-Konsortium besteht aus 11 Partnern (9 akademische Institutionen und 2 Partner außerhalb der akademischen Welt) in 7 europäischen Ländern.

Förderung:
1,57 Mio. €, wovon 1 Mio. € von der Europäischen Kommission finanziert wird und der verbleibende Teil aus dem Staatssekretariat für Bildung, Forschung und Innovation stammt.

Projektkoordination und Kontakt:
PD Dr. sc. ETH Markus Christen
Universität Zürich (UZH), Digital Society Initiative, Rämistrasse 66, 8001 Zürich

Version und Veröffentlichungsdatum:
Version 2.0, Oktober 2019