POLICY BRIEF NR. 4

SCHAFFUNG EINER UMFASSENDEN UND KONSISTENTEN EU-CYBERSICHERHEITSPOLITIK

Die Herausforderung: Aufbau einer kohärenten EU-Cybersicherheitspolitik

Es fehlt an Kohärenz in der Politik und Regulierung der EU-Cybersicherheit, was zu einer Vielzahl von Überschneidungen, aber auch zu widersprüchlichen Anforderungen führt.

In den letzten Jahren wurden auf EU-Ebene zahlreiche Strategien und Regulierungsmaßnahmen zur Cybersicherheit verabschiedet. Bisher konzentrierten sich diese vor allem auf die Bereiche des Binnenmarkts und des Strafrechts, um die Sicherheit von Bürgern, Unternehmen und der öffentlichen Verwaltung im digitalen Umfeld zu erhöhen.

Diesen **politischen Bemühungen mangelt es jedoch oft an Konsistenz und einer hinreichend kohärenten Sichtweise auf Probleme**, die mit der Cybersicherheitspolitik zusammenhängen. Das ist etwas, das behoben werden sollte.

Die direkte Zusammenarbeit zwischen den EU-Mitgliedstaaten kann den Schutz der Grundrechte schwächen

Bei der Gestaltung von Cybersicherheitspolitik muss dafür Sorge getragen werden dass keine unbeabsichtigten und negativen Auswirkungen entstehend, insbesondere im Hinblick auf den Schutz der Grundrechte von europäischen Bürgern. Dies kann unter Umständen eine anspruchsvolle Aufgabe sein. Ein aktuelles Beispiel dafür ist der Vorschlag der Europäischen Kommission, dass die Strafverfolgungsbehörden grenzüberschreitenden Zugang zu Daten erhalten sollen (so genannte e-Evidence).

Eine Studie des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) hat diesen Vorschlag analysiert. Er stellte fest, dass die verstärkte Kooperationsregelung, welche einen schnellen Zugang der EU-Mitgliedstaaten zu den Datenprovidern erlauben würde, die Mitgliedstaaten hemmen würde, „die Verantwortung für einen wirksamen Schutz der Grundrechte in ihrem Hoheitsgebiet zu übernehmen“. Dies würde sowohl für Serviceanbieter als auch für einzelne Nutzer zu Rechtsunsicherheit führen.

Dies ist vor allem auf den Vorschlag zurückzuführen, der eine Neuzuweisung von Schutzfunktionen weg von den EU-Mitgliedstaaten hin zu den Dienstleistern und/oder die zuständige Behörde vorsieht, was den Grundrechtsschutz des Einzelnen wirksam schwächt. Es wäre daher sinnvoll, diese Bedenken im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Das Konzept „Cybersicherheit“ entwickelt sich weiter

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

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

Die unterschiedlichen Bedeutungen des Begriffs „Cybersicherheit“ können sowohl Vor- als auch Nachteile haben

- Der Begriff hat die **Flexibilität**, sich an sich ändernde Umstände anzupassen, aber...
- ...ebenso werden **Spannungen zwischen der EU und der Staatsgewalt der Mitgliedstaaten** verursacht, insbesondere im Bereich der nationalen Sicherheit...
- Wenn sich ein solcher Begriff ständig weiterentwickelt, bleibt der **Umfang zudem unklar.** Er kann übermäßig integrativ oder umfassend werden und eine kohärente Regulierung in diesem Bereich erschwert und behindert.
- **Die Unklarheit des Begriffs „Cybersicherheit“ sollte addressiert werden**, um die regulatorische Fragmentierung sowie die institutionellen Verantwortlichkeiten zu klären.

Cybersicherheit ist vielschichtig und betrifft viele Bereiche

Einige exemplarische Aspekte der Cybersicherheitspolitik sind Cyberkriminalität, Maßnahmen der Netzwerk- und Informationssicherheit sowie elektronische Kommunikation. Viele von ihnen haben auch Auswirkungen auf den europäischen Datenschutzrahmen.

Gesundheitswesen

Wirtschaft

Polizei und nationale Sicherheit

Versuche, Cybersicherheit richtig zu konzeptualisieren sind dadurch erschwert, dass die **Grenzen zwischen den verschiedenen Cybersicherheitsbereichen verschwimmen**, während diese jeweils spezifisches Fachwissen erfordern, wie z.B. Sicherheitstechnik, operationelles Sicherheits- und Schwachstellen Management oder IT-Sicherheitsrahmenwerke und Standards.

Die EU und ihre Mitgliedstaaten definieren „Cybersicherheit“ unterschiedlich

In den jeweiligen Ländern gibt es sehr unterschiedliche Definitionen, deren Geltungsbereiche ein Spektrum von sehr begrenzt bis global umfassend abdecken.

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 […]’.

Ein weiteres nationales Beispiel ist die **Luxemburger Nationale Cybersicherheitsstrategie III 2018**, die 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.

Unsicherheit hinsichtlich der EU-Zuständigkeit 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 ausschließlich einem spezifischen Regulierungsbereich zugeordnet werden, sollte die EU kontinuierlich danach streben, **statthafte juristische Begründung für Regulierungsmaßnahmen der Cybersicherheit** in festgelegten Regulierungsbereichen zu erreichen.

Wer regelt alles Fragen der Cybersicherheit?

Eine sorgfältige Prüfung von Kompetenzfragen ist erforderlich, um die interne, externe und auch die verteidigungspolitische Dimension der Cybersicherheit wirksam anzugehen.

Die EU verwendet den Begriff „Cybersicherheit“ sehr vorsichtig. Ein Beispiel dafür war der 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). In diesem Vorschlag wurde argumentiert, dass die Praktiken der verschiedenen Mitgliedstaaten in Bezug auf Cybersicherheitsmaßnahmen dazu führen dass „[...] Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die Sicherheit von Netzwerk- und Informationssystemen in der Union generell untergraben wird.“ Mit diesen Worten wies die EU faktisch darauf hin dass zusätzliche (Cyber)Sicherheitsmaßnahmen erforderlich sind.

Dies deutet darauf hin, dass es möglicherweise ein **„Kompetenzproblem“** gibt, das für die Beziehungen zwischen der EU und ihren Mitgliedstaaten von grundlegender Bedeutung ist.

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 Fachbereichen 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.

Dies schließt nationale Regierungen, Internet-Provider, Technologie- und Sicherheitsfirmen, Unternehmen und die Zivilgesellschaft ein, um 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, und DG Joint Research Centre).

Aufgrund der ständig zunehmenden Bedeutung und Abhängigkeit der Gesellschaften von ICT ist zu erwarten, dass die Zahl der mit Cybersicherheitsfragen befassten DGs kontinuierlich zunehmen wird.

Während bereits einige Anstrengungen unternommen wurden, um eine Zusammenarbeit zwischen diesen Generaldirektionen und ihrer verschiedenen internen Abteilungen herzustellen, handelt es sich jedoch bei einigen davon nur um informelle Verfahren. **Es fehlt an einer formalen Governance-Struktur für die Regelung der Zusammenarbeit und des Austausches** zwischen diesen Institutionen.

Beispiele für aktuelle Versuche, die Zusammenarbeit auf formellem und informellem Weg zu pflegen, sind Netzwerke von Fachexperten, Konferenzen und Treffen mit mehreren Interessengruppen. Was jedoch den Aufbau einer besseren institutionellen Zusammenarbeit betrifft, so waren die Bemühungen bisher uneinheitlich, unvollständig und nicht effizient genug.

Künftige **politische Initiativen sollten zwischen Rollen, Kompetenzen und Missionszielen der beteiligten Bereiche und Akteure klar unterscheiden.** Dies ist besonders wichtig bei der Entscheidung, ob eher offensive oder eher defensive Cybersicherheitsstrategien verfolgt werden sollen.

Institutionelle Zusammen-arbeit auf nationaler Ebene

Es gibt verschiedene Kooperationsgruppen, wie z.B. den Europäischen Datenschutzausschuss oder das Gremium der Europäischen Regulierungsbehörden für elektronische Kommunikation (GEREK). Es besteht eine Wissens- und Informationsaustauschpraxis zwischen CERTs und Strafverfolgungsbehörden auf nationaler und internationaler Ebene, die jedoch noch nicht optimal etabliert ist. Daher sind **Maßnahmen zur Behebung von mangelnden institutionellen Ressourcen und sowie von Ineffizienz erforderlich**, damit alle relevanten Akteure ausreichend einbezogen werden können.

Die EU-Cybersicherheitsstrategien 2013 und 2017 haben beide einen umfassenden Ansatz für den Schutz der Cybersicherheit gefordert. Dazu gehören auch nationale Ansätze zur Cybersicherheit, die sich nicht nur auf die reine Länderebene, sondern auch auf Interaktionen zwischen der EU und ihren Mitgliedstaaten beziehen.

Abgewogene strategische Entscheidungen sind gefordert

Einige Beispiele für die oft sehr kontroversen Diskussionsthemen im Kontext von offensiven vs. defensiven Cybersicherheitsstrategien sind die Debatten um die Nutzung des sogenannten rechtmäßigen Zugangs von Sicherheitsbehörden, wirksame Verschlüsselung ohne Hintertüren oder die Nutzung von Zero-Day-Lücken.

Während diese Maßnahmen und Instrumente von den Sicherheitsbehörden zur Verbrechensbekämpfung eingesetzt werden können, können sie auch **schwerwiegende Kollateralschäden** auslösen, wie z.B. eine allgemeine Schwächung der Sicherheit von IKT-Systemen für alle.

Bei der Behandlung dieser Fragen sollte die Europäische Union versuchen, ernsthaft auf die Bedenken im Hinblick auf eine mögliche Schwächung der gesamten IT-Sicherheitslandschaft, der Privatsphäre und des Datenschutzes sowie der Menschenrechte im Allgemeinen einzugehen.

Um eine kohärente und werteorientierte Cybersicherheitspolitik zu ermöglichen sollten Sicherheitsexperten, Datenschutzbehörden, Menschenrechtsaktivisten sowie die breite Öffentlichkeit beteiligt werden. Es besteht die **Notwendigkeit, ein ausgewogeneres Verhältnis zwischen den Bedürfnissen der Strafverfolgung und den Bürgerrechten herzustellen.**

Ein positives Beispiel ist der kürzlich verabschiedete Rechtsakt zum Cybersicherheitsgesetz, da er zumindest die Governance-Struktur klärt, indem er die verschiedenen Rollen der ENISA festlegt. Die ENISA berät die Europäische Kommission in Fragen der Cybersicherheit, bietet einen zentralen Anlaufpunkt für Fachwissen und erleichtert so die Zusammenarbeit und Koordination zwischen den verschiedenen Interessengruppen.

Das Ziel ist eine wertorientierte Cybersicherheit

Die höchsten Standards der Rechtsstaatlichkeit und des Schutzes der Grundrechte sollten eingehalten werden.

Dies ist besonders wichtig für die Bereiche der Strafverfolgung und des Strafverfahrens sowie für Fälle der Zusammenarbeit und des Informationsaustauschs, in denen ein **sorgfältiger Ausgleich zwischen den Interessen der Bürger, Gesellschaften und Mitgliedstaaten erforderlich** ist.

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. Daher sollte sorgfältig darauf geachtet werden, wie gut solche Gesetzesmaßnahmen in das Gesamtbild passen.

Konsequenterweise sollten die politischen Entscheidungsträger ein **klares Verständnis für die Grenzen der Zusammenarbeit auf der Grundlage von Rechtmäßigkeits- und Rechtsgrundsätzen** entwickeln und versuchen, entsprechende Kohärenz über eine Vielzahl von Rechtsvorschriften hinweg zu erhalten.

Ansatzpunkte für eine verbesserte Cybersicherheitspolitik

Empfohlene Schritte um Inkonsistenzen in der europäischen Cybersicherheitspolitik zu begegnen:

Gewährleistung eines ausreichenden Schutzes der Grundrechte des Einzelnen durch die EU Mitgliedstaaten, insbesondere im Hinblick auf die Balance zwischen Sicherheit und dem Schutz personenbezogener Daten.

EU-weite Einigung auf ein klar definiertes gemeinsames Verständnis dessen, was Cybersicherheit bedeutet und welche Fachgebiete bei der Initiierung neuer Gesetzesvorhaben berücksichtigt werden sollten.

Unmissverständliche Auflösung von Unklarheiten in Bezug auf Gesetzgebungskompetenzen.

Soweit Institutionen Aufgaben und Verpflichtungen durch Regulierung zugeteilt werden, sollten die Rollen, Kompetenzen und Missionsziele der involvierten Bereiche und Akteure deutlich unterschieden werden.

Evaluierung und Verbesserung der Verfahrensweisen zum Informationsaustausch.

Klärung der wechselseitigen Beziehung von staatlichen und privaten CERTs sowie Sicherstellung, dass diese die geltenden Datenschutzgesetze und ethischen Richtlinien befolgen.

Weitere Informationen finden Sie hier

Die Folien basieren auf der Forschungsarbeit des CANVAS-Projekts (Constructing an Alliance for Value-driven Cybersecurity).

Ziel von CANVAS ist es, Stakeholder aus Schlüsselbereichen der Europäischen Digitalen Agenda zusammenzubringen, um der Herausforderung zu begegnen, wie Cybersicherheit mit europäischen Werten und Grundrechten in Einklang gebracht werden kann.

Insbesondere stellen wir die folgenden CANVAS-Ressourcen zur Verfügung:

- Briefing packages
- CANVAS Reference Curriculum
- CANVAS MOOC
- Open Access Book
  ‘The Ethics of Cybersecurity’

Die Folgefolie verweist direkt auf jene unserer White Paper, die sich ausführlich mit den Herausforderungen der Cybersicherheit befassen.

Bibliographie: Herausforderungen der Cybersicherheit (CANVAS White Papers)

Ethische Herausforderungen

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Rechtliche Herausforderungen

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technische Herausforderungen

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Bibliographie

Vertrauen – generell – philosophisch

- Held, Virginia. 1968. “On the Meaning of Trust.” Ethics 78 (2): 156–59.
- Baier, Annette. 1986. “Trust and Antitrust.” Ethics 96 (2): 231–60.
- Pettit, Philip. 1995. “The Cunning of Trust.” Philosophy & Public Affairs 24 (3): 202–25.
- Becker, Lawrence C. 1996. “Trust as Noncognitive Security about Motives.” Ethics 107 (1): 43–61.

Vertrauen – generell – Sozialwissenschaften

- Frey, Bruno S. 1994. “How Intrinsic Motivation Is Crowded out and In.” Rationality and Society 6 (3): 334–52.
- Ostrom, Elinor. 2000. “Collective Action and the Evolution of Social Norms.” The Journal of Economic Perspectives 14 (3): 137–58.
- Frohlich, Norman, and Joe A. Oppenheimer. 1996. “Experiencing Impartiality to Invoke Fairness in the N-PD: Some Experimental Results.” Public Choice 86 (1): 117–35. https://doi.org/10.1007/BF00114878.

Vertrauen – online – digital

- Erlich, Yaniv, et al. 2014. “Redefining Genomic Privacy: Trust and Empowerment.” PLOS Biology 12 (11): e1001983.
- Etzioni, Amitai. 2017. “Cyber Trust.” Journal of Business Ethics, July. https://doi.org/10.1007/s10551-017-3627-y.
- Chakravorti, B., Bhalla, A., Chaturvedi, R.S., 2018. The 4 Dimensions of Digital Trust, Charted Across 42 Countries. Harvard Business Review.

Fakten zum Projekt

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

Slidedocs-Version:
Version 2.0 Oktober 2019

Projektdauer:
Sept. 2016 - Okt. 2019

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

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