It's not a data breach, it's a surprise backup

Fostering cybersecurity

Autor:innen:
Teresa Reiter
Dieter Feierabend

NEOS LAB

elf

#It's not a data breach, it's a surprise backup

Fostering cybersecurity

Graphic design: Andreas Pohancenik

Publisher:
European Liberal Forum EUPF
Rue d'Idalie 11-13, boite 6, 1050 Ixelles, Brussels (BE)
info@liberalforum.eu
www.liberalforum.eu

NEOS Lab
Neubaugasse 64–66, 1070 Vienna (AUT)
lab@neos.eu
lab.neos.eu

Published by the European Liberal Forum in cooperation with NEOS Lab. Co-funded by the European Parliament. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum.

Printed by Printpool, Austria 2022

ISBN: 978-2-39067-041-4

Abstract

Studien zufolge macht Cyberkriminalität die Hälfte aller begangenen Straftaten in einigen Mitgliedstaaten aus und verursacht Schäden in Milliardenhöhe pro Jahr. Dennoch passieren die meisten Hacks über bekannte Exploits, bei denen Hacker die IT-Netzwerke besser kennen als Unternehmen. Ziel dieser Publikation ist es, Maßnahmen zur Stärkung der Cybersicherheitsinfrastruktur auf europäischer und nationaler Ebene aufzuzeigen. Die Minimierung von Cyberkriminalität hängt im Allgemeinen mit der Geschäftsbereitschaft und dem Wissen der Bürger zusammen. Daher werden diese Gruppen in der Analyse und den Politikempfehlungen besonders berücksichtigt.

Teresa Reiter
Autorin

Dieter Feierabend
Autor

Inhalt

Einleitung

Die Hälfte aller Unternehmen wird Opfer von Ransomware-Attacken. Jedes achte Unternehmen wird fast täglich Ziel von Angriffen, die einen Cyber-Aspekt beinhalten, 9 Prozent erfahren solche Angriffe mehrmals im Monat (Deloitte, 2022:4). Besonders Ransomeware-Attacken nehmen zu. Dabei werden oft Daten des Unternehmens verschlüsselt, um Lösegeld zu erpressen. Ein neueres Beispiel aus Österreich ist die Attacke der Hackergruppe „Black Cat" auf das Bundesland Kärnten (Futurezone, 2022). Die Angreifer erbeuteten 250 Gigabyte an Daten und drohten mit der Veröffentlichung dieser, sollte das Land Kärnten nicht schnellstens 5 Millionen US-Dollar Lösegeld bezahlen.

Während solche Angriffe die tagespolitische Dimension haben, dass sie für einzelne oder alle betroffenen Personen, Parteien und Regierungen unangenehm werden können und ihnen politisch schaden, ist das Hauptproblem jedoch die Einschränkung der Handlungsfähigkeit des Ziels einer solchen Attacke. Selbst wenn ein Unternehmen oder eine Institution ordnungsgemäß und regelmäßig Backups gemacht hat, um seine Daten abzusichern, ist eine Wiederherstellung oft mit viel Zeitverlust und hohen Kosten verbunden. Während der Zeit des Wiederherstellens funktionieren möglicherweise für die Bürger:innen/Kund:innen wichtige Services nicht, was zu weiterem Schaden führen kann. Auch physische Sicherheitsbedrohungen sind als Konsequenz eines solchen Angriffs nicht ausgeschlossen. Fällt ein solcher Angriff mit einer anderen Krise zusammen und beeinträchtigt das Krisenmanagement, so kann ein Cyberangriff leicht Konsequenzen für die Sicherheit Einzelner haben. Während die meisten Organisationen bzw. Unternehmen angeben, kein Lösegeld zu bezahlen, gibt es hier wohl eine hohe Dunkelziffer, da die Höhe des Lösegelds oft in keiner Relation zum potenziellen oder tatsächlichen mittel- und langfristigen Schaden steht, den der Cyberangriff verursacht.

Den größten Schaden richten meistens nicht High-Level-Attacks wie oben genannte Beispiele an, sondern Low-Level-, Low-Cost-Angriffe auf zivile Infrastruktur, private Firmen und Einzelpersonen. Dies zeigt, dass Cybersecurity für uns alle ein Thema ist, als Bürger:in, deren Daten durch Angriffe auf Behörden gestohlen wurden, als Unternehmer:in, die mit Ransomware-Attacken zu kämpfen hat, oder als politische:r Entscheidungsträger:in, die im Zuge der Digitalisierung in allen Lebensbereichen vermehrt mit Cybersecurity in Kontakt kommt. Angesichts der oben genannten Dimension ist es nicht verwunderlich, dass die ENISA, die

Agentur der Europäischen Union für Cybersicherheit, kritisiert, dass Cybersecurity weiterhin fälschlich als reines IT-Thema behandelt wird (ENISA 2021). Individuelle Freiheiten, Wohlstand und unsere Sicherheit in Europa können ohne eine digitale Sicherheitsarchitektur nicht mehr gewährleistet werden. Daher ist es nötig, das Thema aus einer anderen Perspektive zu betrachten, die sich nach folgenden beiden Kernaussagen orientiert:

- Cybersecurity ist ein Thema der Organisationskultur, das weit über IT-Fragen hinausgeht
- Der Mensch und nicht die IT steht bei Cybersecurity im Mittelpunkt

Das Ziel dieser Publikation ist es, basierend auf diesen Kernaussagen Maßnahmen zu einer Stärkung der Cybersecurity-Infrastruktur auf europäischer und nationaler Ebene zu liefern. Dieses Paper ist in zwei Abschnitte eingeteilt:

Die Pandemie hat auch in im Bereich Cyberkriminalität zu veränderten Bedrohungsszenarien geführt. Daher werden zu Beginn des ersten Abschnitts aktuelle Bedrohungsszenarien dargestellt und primäre Bedrohungen im Cybersecurity-Bereich definiert. In den vergangenen zehn Jahren schufen die Mitgliedstaaten der Europäischen Union unterschiedliche Einrichtungen und Instrumente, um Verwaltung, Wirtschaft und auch den einzelnen User vor Cyberangriffen unterschiedlicher Art zu schützen. Zusätzlich richteten auch NATO und OSZE sowie alle europäischen Nationalstaaten Stellen und Mechanismen ein, um auf diese nun doch nicht mehr allzu neue Herausforderung zu reagieren. Einen Überblick über deren Zuständigkeiten, Kompetenzen und Funktionsweisen zu gewinnen, ist mitunter nicht einfach. Daher fordern politische Entscheidungsträger:innen oft die Einrichtung weiterer Instrumente, Agenturen und Koordinationsstellen, ohne sich genaue Gedanken dazu zu machen, welche bereits vorhandenen Strukturen man nutzen, ausbauen oder einfach stärker unterstützen könnte, um das Ziel der größeren Cybersicherheit für alle zu erreichen. Dies ist von besonderer Relevanz, da durch den Ausbruch des russischen Aggressionskrieges gegen die Ukraine, die geopolitische Dimension von Cyberangriffen sowie Angriffe von staatlich gesponsorten Gruppen deutlich zugenommen haben (ENISA 2022b).

Dieses Papier zielt daher darauf ab, eine solche Darstellung – eine Art Organigramm der wichtigsten Einrichtungen und Schutzmaßnahmen im Cyberbereich – zu erstellen, inklusive der wichtigsten legistischen Maßnahmen.

Der zweite Abschnitt gliedert sich in vier Themenbereichen, bei denen aus Sicht der Autor:innen Handlungsbedarf besteht:

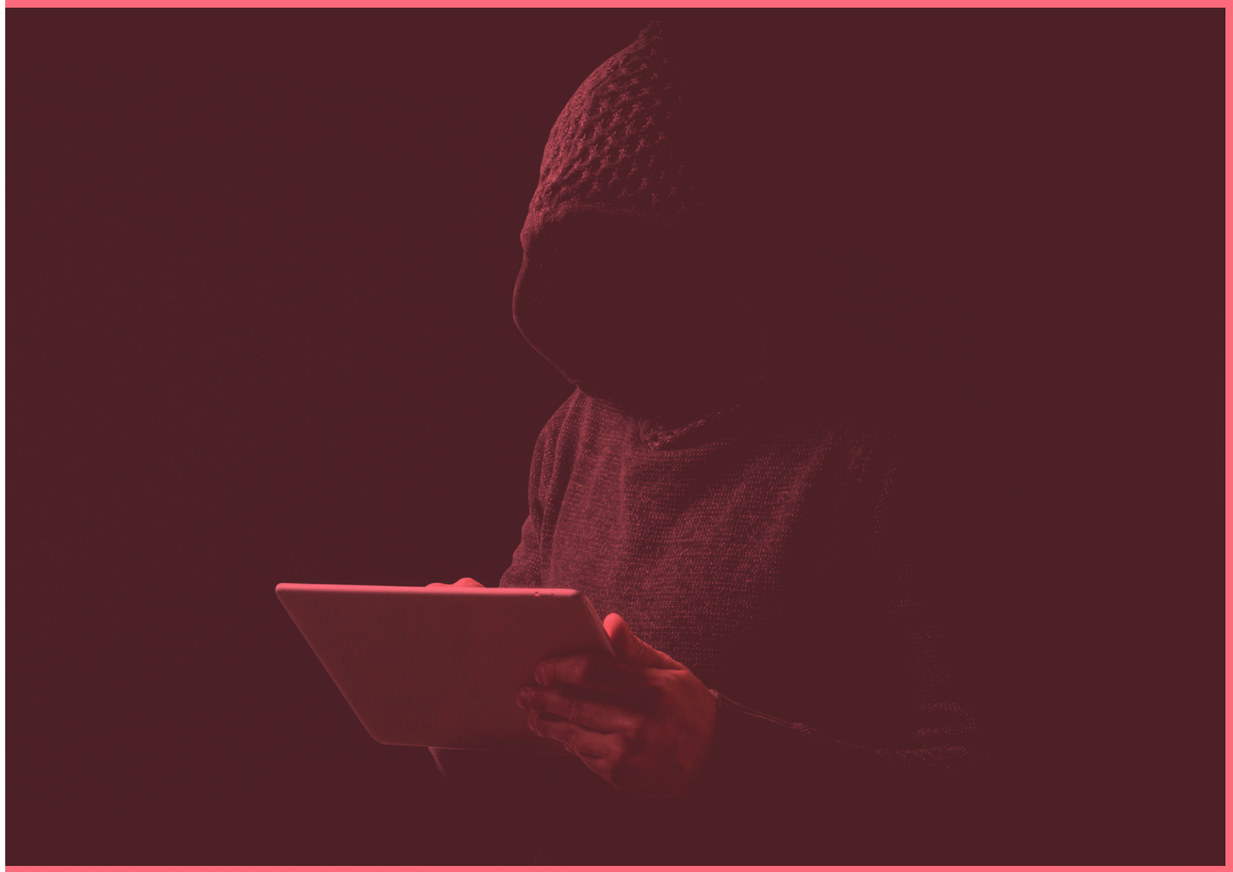
1. Resilienz und strategische Autonomie sind auch im Cybersecurity-Kontext ein wesentliches Thema. Während es in Europa eine Vielzahl an Gesetzen und Verordnungen darüber gibt, fehlt es an konkreten quantitativen Maßzahlen, mit denen wir Effektivität und Erfolg der Maßnahmen messen können.
2. Angesichts sehr unterschiedlicher Zugänge der USA, Russland und China zu Cybersecurity und Cyberdefence, KI und Dateninfrastruktur gilt es, auch die europäische Position im Sicherheits- und Verteidigungsbereich zu schärfen.
3. Wie im gesamten IKT-Bereich sind auch die Beschäftigungszahlen im Cybersecurity-Sektor massiv angestiegen. Angesichts des weiterhin stark steigenden Personenbedarfs stellt sich die Frage, wie der Fachkräftemangel behoben werden kann.
4. Wenn es um Unternehmen und Cybersecurity geht, wird oftmals nur über die kritische Infrastruktur gesprochen. Gleichzeitig sind viele Klein- und Mittelbetriebe (KMU) von europäischen Richtlinien wie NIS 1 und 2 ausgenommen. Da auch sie sehr stark von Cyberangriffen betroffen sind und diese Unternehmen das Rückgrat der europäischen Wirtschaft darstellen, muss auch ihre Cybersicherheit verbessert werden.

Zielgruppe dieser Publikation sind politische Referent:innen, Entscheidungsträger:innen der europäischen Liberalen, liberal gesinnte Bürger:innen und Policy-Thinktanks. Niemand soll mehr dem Mythos zum Opfer zu fallen, die Verteidigung von Cyberangriffen sei billiger, einfacher, schneller als die Akquise schwerer Waffensysteme für den Kampf gegen Verbrechen und Kriegsführung im analogen Raum. Vielmehr sehen wir einer Zukunft entgegen, in der auf Cyberbedrohungen adaptierte Sicherheitsstrategien und -doktrinen auch auf das gesamtheitliche Denken im Sicherheits- und Verteidigungsbereich Einfluss nehmen könnten. Die Idee der Abschreckung, besonders die nukleare Abschreckung, prägte lange Zeit die sicherheitspolitische Vorgehensweise unterschiedlicher geopolitischer Mächte. Sie lässt sich jedoch nicht eins zu eins auf den Cyberraum anwenden. Die Akkumulation von offensiv einsatzbaren Cyberwaffen verringert nicht das Risiko eines Angriffs. Im Gegenteil: Es gibt prominente Beispiele dafür, dass eben für solche Zwecke von Großmächten entwickelte Cyberwaffen von Angreifern entwendet und direkt oder indirekt gegen den Entwickler eingesetzt wurden. Ein weiteres Thema, das die Liberalen im Kontext von Sicherheitspolitik immer wieder beschäftigt, ist die Waffenexportkontrolle. Wie die Debatte um Waffenlieferungen an die Ukraine 2022 zeigt, sind Positionen dazu auch in der liberalen Familie wandelbar. Vor den vergangenen EU-Parlamentswahlen 2019 zeigten viele Staaten große Unterstützung für die Position, dass keine Waffen an Staaten exportiert werden sollten, die in einen aktiven kriegerischen Konflikt involviert sind. Hier hat sich der Wind durch Russlands Krieg gegen die Ukraine nicht nur gedreht, sondern die Debatte wird auch durch Möglichkeiten der digitalen Kriegsführung verkompliziert. Traditionelle Waffenexportkontrolle stößt im Cyberraum an ihre Grenzen, dennoch werden wir in Europa und auch darüber hinaus nicht umhin kommen, internationale Regeln weiterzuentwickeln bzw. zu überlegen, wie bereits bestehende Regeln auf diesen Aspekt des Cyberraums anwendbar sind.

Schließlich gilt es gerade für die Liberalen, aber auch für alle anderen politischen Kräfte, die Implikationen von Cyber Crime bzw. Cyberattacken auf die Wirtschaft und dabei besonders die kritische Infrastruktur besser zu verstehen und Wege aufzuzeigen, wie man damit umgehen könnte. Die NIS2-Richtlinie der Europäischen Union stellt Wirtschaft und Staat besonders

aufgrund des IKT-Fachkräftemangels in den meisten Staaten Europas vor große Herausforderungen, auf die es zu reagieren gilt.

Das Allheilmittel gibt es bei Bedrohungen, die eine solch komplizierte und diverse Stakeholder und Threat-Actor-Landschaft hat wie diese, nicht. Dennoch gibt es gute Beispiele dafür, wie die Zahl der erfolgreichen Cyberattacken auf einen Staat, seine Verwaltung, Wirtschaft und Individuum verringert werden kann. Bei der Implementierung dieser gilt es für die Liberalen Europas, möglichst eine gemeinsame Vorgehensweise zu finden, die einen Kernwert des Liberalismus nicht außer Acht lässt: die Freiheit des Individuums und dessen Grund- und Menschenrechte. Die Antwort auf Cyberbedrohungen darf niemals ungezügelte, überschießende und rechtswidrige Überwachung der Bürger:innen sein. Die Verantwortung, diesen Aspekt immer wieder hochzuhalten, liegt vorwiegend bei den Liberalen.



Kapitel 1

1.1 Cyberkriminalität und Cybersecurity – Definitionen und Statistiken

Der EU Cybersecurity Act definiert „Cybersecurity“ als „alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen“ (Cybersecurity Act, 2017: Titel 1, Art 2, Zf 1). Diese Definition sollte politische Entscheidungsträger aufhorchen lassen, denn sie ist insofern klug, als sie klar macht, dass die Maßnahmen zur Förderung von Cybersicherheit quasi alles denkbar Notwendige umfassen kann und nicht rein auf den IT-Kontext beschränkt ist.

Spätestens seit der Entdeckung des Stuxnet-Virus 2008 ist jenen, die sich mit der Materie beschäftigen, klar, dass Cybersecurity und auch Cyberdefense keine reinen IT-Angelegenheiten sind. Die Operation „Olympic Games“, wie der Einsatz des Virus bei der Zerstörung iranischer Zentrifugen zur Uran-Anreicherung, nutzte bei der Anwendung der Schadsoftware physische Schwächen der Anlage aus. Sehr vereinfacht gesagt hätte Schadsoftware allein gegen ein System ohne diese physischen Schwächen zu jenem Zeitpunkt viel weniger ausrichten können. Es war also nicht die „Übermacht“ der Cyberwaffe, die die Attacke so gefährlich machte, sondern die Kombination aus Vulnerabilität und einer effektiv auf diese abzielenden Waffe. Die für die Entdeckung des Stuxnet-Virus berühmt gewordene Sicherheitsfirma Langner schließt in ihrer Analyse, dass es unwahrscheinlich ist, dass Stuxnet oder Teile davon für Copycat-Angriffe auf kritische Infrastruktur in den USA angewandt würde. Die größere Gefahr sehen die Langner-Experten darin, dass der taktische Ansatz der Attacke kopiert, weiterentwickelt und auf zivile Infrastruktur „abgefeuert“ werden könnte (Langner, 2013).

High-Level-Attacken wie diese erreichen zwar großes mediales Interesse, jedoch sind sie nicht alltäglich. Angriffe von der Komplexität und Kostspieligkeit der Operation „Olympic Games“ sind vergleichsweise schwierig durchzuführen. Wichtige primäre Bedrohungen sehen anders aus und werden durch die ENISA in ihrem periodisch erscheinenden „threat landscape“ definiert (ENISA, 2022):

Tabelle 1: Wesentliche Bedrohungsszenarien

Art	Beschreibung
Ransomware	Ransomware heißt so viel wie "Erpressersoftware" und ermöglicht dem Angreifer, Daten einer Organisation zu verschlüsseln, also quasi als Geisel zu halten. Dies geht mit einer Zahlungsaufforderung für die Wiederherstellung des Zugangs zu den Daten einher.
Schadprogramme	Ein Schadprogramm ist Software, deren Ziel es ist, dass Unbefugte ungenehmigten Zugriff auf Systeme erlangen. Dieser Zugriff wirkt sich nachteilig auf die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems aus.
Cryptojacking	Bei Cryptojacking (auch verdecktes Crypto-Mining genannt) nutzen Kriminelle die Rechnerleistung ihrer Opfer ohne deren Wissen, um eine Cryptowährung zu generieren.
Bedrohung für Verfügbarkeit und Integrität	Hierbei handelt es sich um eine Bandbreite an Bedrohungen und Angriffen, wobei die Gruppen der Denial-of-Service- (DoS) und Internetangriffe herausstechen. Oftmals ist das Ziel, die Verfügbarkeit von Systemen durch Erschöpfen der Ressourcen zu verhindern, was wiederum zu Leistungsverlust, Datenverlust und Ausfällen führt.
Bedrohung in Verbindung mit Mails	Angriffe im Zusammenhang mit Mails (elektronischer Postverkehr) bestehen aus einem Bündel von Bedrohungen, die die Schwächen der menschlichen Psyche ausnützen. Beispielsweise vermeintliche Mitteilungen der eigenen Bank, dass es Probleme mit dem eigenen Konto gibt oder Nachrichten von Softwarefirmen.
Desinformation – Fehlinformation	Desinformations- und Fehlinformationskampagnen werden häufig bei Hybridangriffen genutzt, um das gesellschaftliche Vertrauen in Organisationen und Systemen, einer wichtigen Voraussetzung für Cybersicherheit, zu mindern. Durch die erhöhte Nutzung von Social-Media-Plattformen und der verstärkten Online-Präsenz seit dem Ausbruch der Pandemie haben sich diese Bedrohungen verstärkt.

Quelle: ENISA 2022

Seit mehreren Jahren stellt Ransomware die häufigste Bedrohung dar, wobei mehrere Vorfälle mit hohem Bekanntheitsgrad auftraten (siehe Kapitel 1). Die Relevanz derartiger Angriffe wurde sowohl in Europäischen Union als auch auf internationaler Ebene nachgewiesen. (ENISA 2021, 2020). Trotz breiter Sensibilisierungsmaßnahmen ist die Gefahr von Schadprogrammen in Verbindung mit E-Mails weiterhin sehr hoch. Neue Formen der Kriminalität, wie Cryptojacking, eine Bedrohung, die in ihrer Häufigkeit in den letzten beiden Jahren signifikant angestiegen ist (ENISA 2020, 2021), ergänzen das Gefahrenbild.

In den letzten zehn Jahren ist die Zahl der Cyberangriffe auf zivile Infrastruktur und auch militärische Einrichtungen gravierend gestiegen. Einer Studie von Accenture (2019) zufolge ist alleine binnen Jahresfrist die Anzahl an erfolgreichen Angriffen um 11 Prozent gestiegen. Der Internet Crime Report 2021 des FBI (2022) zeigt, dass während der COVID-19-Pandemie ein massiver Anstieg an Fällen zu beobachten ist. Die Anzahl an gemeldeten Fällen ist im Vergleich zu 2019 um fast 70 Prozent angestiegen, während sich die Schadenssumme binnen zwei Jahren verdoppelt hat. Laut dem offiziellen jährlichen Cybercrime-Bericht 2019 von CyberSecurity Ventures ist Cyberkriminalität die größte Bedrohung für jedes Unternehmen der Welt (CyberSecurity Ventures, 2020). Ihren Berechnungen zufolge haben sich die Kosten von Cyberkriminalität zwischen 2015 und 2021 auf 6 Billionen Dollar verdoppelt und Prognosen gehen davon aus, dass bis 2025 der Schaden auf 10,5 Billionen ansteigt. Analysen von Proofpoint (2022) zufolge starten Cyberattacken in 90 Prozent aller Fälle mit Mailnachrichten. Ihren Analysen zufolge werden pro Tag 3,1 Milliarden Scam-Mails verschickt. Grundsätzlich ist dieser Anstieg durch mehrere Faktoren erklären. Neben der zunehmenden Online-Präsenz sind der Anstieg von Online- und Cloud-basierten Lösungen oder die Nutzung aufstrebender Technologien wie Künstliche Intelligenz (KI) und die damit einhergehende Komplexität von Systemen und Cyberangriffen ein wesentlicher Faktor (ENISA 2020, 2021, Stealthlabs 2020).

Abbildung 1: The rising cost of cybercrime

Quelle: CyberSecurity Ventures

Vergleicht man auf Basis der Daten von CyberSecurity Ventures die volkswirtschaftlichen Kosten der Cyberkriminalität mit dem BIP von Staaten, wäre Cyberkriminalität nach den USA und China die drittgrößte Volkswirtschaft der Welt. Diese Dimension, gepaart mit dem massiven Anstieg der Schadenssumme in den letzten Jahren, stellt gemäß CyberSecurity Ventures (2021) den größten Transfer von wirtschaftlichem Reichtum in der Geschichte dar. Innerhalb der Kriminalitätsfelder ist Cyberkriminalität damit profitabler als der globale Drogenhandel.

In ihrem jährlichen Bericht zur Cybersecurity-Bedrohungslage bildet die Agentur der Europäischen Union für Cybersicherheit ENISA neben einer grundsätzlichen Einschätzung der Bedrohungslage auch erhebliche böswillige Angriffe ab. Hierbei handelt es sich um größere Vorfälle, wie die eingangs erwähnten erfolgreichen Angriffe auf das Bundesland Kärnten oder private Firmen wie SolarWinds. Auch bei größeren Vorfällen ist ein kontinuierlicher Anstieg zu beobachten. Alleine im ersten Jahr der Pandemie haben sich die schwerwiegenden Attacken verdoppelt, insbesondere im Gesundheitssektor wurde ein Anstieg von 50 Prozent beobachtet ENISA (2020, 2021). Für das letzte Berichtsjahr zeigt sich, dass die öffentliche Verwaltung, Anbieter von digitalen Diensten und der Gesundheitssektor besonders betroffen waren.

Abbildung 2: Kritische Angriffe auf ausgewählte Sektoren

Kritische Angriffe zwischen April 2020 und Juli 2021

Sektor	Anzahl
Öffentliche Verwaltung	189
Anbieter von digitalen Diensten	151
Gesundheitswesen	137
Breite Öffentlichkeit	117
Finanz/Banken	89
Verkehr	49
Bildung/Wissenschaft	48
Militär	33
Medien/Unterhaltung	32
Energie	25
Bauwesen	24
Lebensmittel	16

Quelle: CENISA 2021

Der Anstieg an Cyberangriffen sowie ein verstärktes Bewusstsein für Cybersecurity sorgt für ein kontinuierliches und robustes Wachstum des weltweiten Markts für Cybersicherheitsprodukte. Während im Jahr 2016 weltweit ein Umsatz von 83 Milliarden Dollar mit Cybersecurity-Lösungen gemacht wurde, ist dies im Jahr 2021 auf 139 Milliarden angestiegen, wobei die jährlichen Wachstumsraten meist über 10 Prozent lagen (Statista 2022a, 2022b, Zdnet 2022). Damit gehört der Cybersecurity-Sektor zu den am stärksten wachsenden Märkten (Statista 2022b). Innerhalb der Europäischen Union wird erwartet, dass der Cybersecurity-Markt 36,3 Milliarden Euro erreicht, wobei Sicherheitsdienstleistungen mit 21,1 Milliarden den größten Anteil ausmachen (Statista 2022a).

Das Ponemon-Institut hat in Zusammenarbeit mit IBM in 17 Staaten und 17 Sektoren untersucht, welche Kosten ein erfolgreicher Cyberangriff verursacht. Ihren Analysen zufolge gaben Unternehmen 2022 im Durchschnitt pro Schadensfall 4,4 Millionen für die Schadensbehebung aus, während 2020 noch 3,9 Millionen ausgegeben wurden (Ponemon/IBM 2022). Gleichzeitig zeigt der Bericht, dass Organisationen, die den Schaden innerhalb von 200 Tagen identifizieren und beheben konnten, ihre Kosten um 1,1 Millionen senken konnten. Zeit ist also ein entscheidender Faktor bei der Entdeckung von Angriffen.

Den größten Schaden richten meistens nicht die High-Level-Attacks an, sondern niederschwellige und für den Angreifer vergleichsweise kostengünstige Angriffe auf zivile Infrastruktur, private Firmen und Einzelpersonen. Ein hoher Grad der Standardisierung, wie ihn die Europäische Union in unterschiedlichen wirtschaftlichen und administrativen Zusammenhängen anstrebt, um etwa das Funktionieren des Binnenmarkts zu gewährleisten, Zusammenarbeit zwischen EU-Staaten zu vereinfachen oder den Endkund:innen das Leben zu erleichtern, sind im Kontext von Cybersecurity manchmal ein Problem, denn er macht Copycat-Attacken sehr kostengünstig für die Angreifer. Digitale Systeme, die eine bestimmte Funktion haben und nie darauf ausgerichtet waren, Angriffen standzuhalten oder diese abzuwehren, werden für Cyberangreifer immer relevanter. Ein Beispiel dafür sind Kontrollsysteme zur Überwachung der Funktion von Industrieanlagen. Physische Schwächen bei z.B. Industrieanlagen etc. werden oft nicht in erster Linie als Schwäche im Kontext eines möglichen Cyberangriffs begriffen. Militär- und kriminalhistorisch ist davon auszugehen, dass Cyberkriminelle und staatliche Akteure Mittel und Wege finden werden, physische und virtuelle Schwächen eines Ziels durch kreative Methoden zu verknüpfen und in immer neuen Kontexten zu nutzen (Langner, 2013: 19f.). Aspekte wie Infokrieg-Methoden verändern sich gemeinsam mit der sich ebenfalls verändernden Kommunikationsarchitektur und dem Kommunikationsverhalten unserer Gesellschaften. Plattformen, Software und digitale Gebrauchsgüter können leicht „weaponised", also als Waffe oder als Manipulationsinstrument eingesetzt werden, wie etwa der Fall des britischen Unternehmens Cambridge Analytica zeigt, der durch seine Rolle im US-Wahlkampf Schlagzeilen machte (Chang, 2018).

Hinzu kommt, dass durch die zunehmende digitale Vernetzung von Privaten und Staat, national und international, die Gefahr von Kettenreaktionen, digitalen Pandemien, wenn man so will, steigt. Das bekannte Beispiel des Angriffs auf die Ukraine mit NotPetya zeigt, dass viele Rechner, die nicht ursprünglich Ziel der Attacke, aber mit der Zielarchitektur auf die eine oder andere Art vernetzt waren, infiziert wurden und Schaden davontrugen. Sind bei solchen High-Level-Attacken meist Staaten oder größere Institutionen bzw. kritische Infrastruktur betroffen, so gibt es heute kaum noch jemanden, der nicht darüber hinaus auch individuell von Cyberbedrohungen betroffen ist, sei er/sie sich dessen bewusst oder nicht (Perlroth, 2021).

Das ist besonders relevant, da nach Erkenntnissen von ENISA (2021b) 84 Prozent aller Cyberattacken auf „Social Engineering" basieren. Hierbei handelt sich um eine Technik, bei der kriminelle Akteure sicherheitstechnisch relevante Daten erhalten, indem sie menschliches Verhalten ausnützen. Menschliche Emotionen und Eigenschaften wie Vertrauen, Hilfsbereitschaft oder Angst werden ausgenutzt, um User zu manipulieren, beispielsweise vertrauliche Informationen weiterzugeben oder Schadsoftware zu installieren (Kaspersky 2022). Je mehr man über Nutzer:innen und ihre Gewohnheiten weiß, desto leichter ist es, diese Gewohnheiten zu instrumentalisieren. Dass die meisten

Menschen auf Social Media ihre Vorlieben, Verwandtschaftsbeziehungen und berufliche Details teilen, macht es Angreifern leichter. Hacker könnten feststellen, dass viele Mitarbeiter:innen eines Unternehmens ein bestimmtes Restaurant auf Facebook leiten und im Menülink des Restaurants ihre Malware verstecken. Social Engineering ist zwar kein neuartiges Phänomen, jedoch ermöglicht die Digitalisierung unserer Gesellschaften es Kriminellen, Millionen von Opfern bei vergleichsweise geringem Aufwand zu erreichen. Besonders schlagend wird dies bei Klein- und Mittelbetrieben (KMU), die oftmals im Gegensatz zu Großunternehmen keine eigene IT-Abteilung besitzen und oftmals nur wenige Angestellte haben. Accentures neunte „Annual Cost of Cybercrime"-Studie (Accenture, 2019) zeigt, dass 43 Prozent aller erfolgreichen Datenlecks in Klein- und Mittelbetrieben stattfinden. In einer ENISA-Analyse (ENISA 2021b) zur Cybersicherheit von KMU zeigt sich, dass neben Social Engineering schwache Passwörter (für 56 Prozent aller KMU war dies ein Problem) und unversperrte Geräte (44 Prozent) zu den größten Sicherheitsrisiken gehören.

1.2 Akteure und wichtige Gesetzgebung

In den vergangenen zehn Jahren hat die EU eine Vielzahl an Cybersicherheitsmaßnahmen verabschiedet. Insbesondere die NIS-1-Direktive im Jahr 2016 führte zu einer Aufwertung der Cybersicherheit in der Europäischen Union. Hierbei wurden Industrie und relevante Institutionen dazu verpflichtet, Schwachstellen aus Sicht der Cybersicherheit zu reduzieren und die Resilienz zu stärken. Aus institutioneller Sicht war der „Cybersecurity Act" von besonderer Relevanz, da er neben zentralen Begriffsdefinitionen wie Cybersicherheit, IKT-Standards und Zertifizierungsprozessen die Etablierung der ENISA, der EU-Agentur für Cybersicherheit, darstellt.

Die gerade in Finalisierung stehende NIS-2-Direktive, die Unterschiede bei den Anforderungen an die Cybersicherheit minimieren und einheitliche Standards bei der Umsetzung von Cybersicherheitsmaßnahmen garantieren soll, ist ein weiterer wesentlicher Meilenstein in der Cybersicherheit. Besonders hervorzuheben ist hierbei die Ausweitung der von der Richtlinie betroffenen Unternehmen. Während auf Basis der aktuellen Richtlinien die Mitgliedstaaten dafür zuständig waren festzulegen, welche Einrichtungen als Betreiber wesentliche Dienste erfüllen, wird mit der neuen NIS-2-Richtlinie ein Schwellenwert für die Größe eingeführt, wodurch deutlich mehr Unternehmen den Richtlinien unterworfen werden. Da oftmals auch öffentliche Verwaltungen Angriffen ausgesetzt sind, gilt NIS 2 auch für öffentliche Verwaltungseinrichtungen auf Bundes- und regionaler Ebene.

Tabelle2: Auswahl von wesentlichen EU-Cybersecurity-Initiativen

Datum	Initiative	Referenz
2013/02	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: 'An Open, Safe and Secure Cyberspace	JOIN/2013/01
2015/04	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The European Agenda on Security	COM/2015/0185
2016/04	European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	Regulation (EU)2016/679
2016/07	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	EU Directive 2016/1148
2017/09	European Commission, Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certifcation ('Cybersecurity Act')	COM(2017) 477 fnal
2018/09	Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres	COM(2018) 630 fnal
2020/02	Shaping Europe's Digital Future White Paper on Artifcial Intelligence A European Data Strategy	COM(2020) 65 fnal COM(2020) 66 fnal
kommend	Network and Information Security (NIS2) Directive	EU Directive

Quelle: European Commission, Joint Research Centre

1.2.0 Akteure

1.2.1 EU

ENISA

Die 2004 gegründete EU Agency for Cyber Security mit Hauptquartier in Athen hat die eher allgemein formulierte Aufgabe, Cybersicherheit in Europa allgemein zu stärken. In der Praxis arbeitet sie mit Wirtschaft und unterschiedlichen Organisationen zusammen, um das Vertrauen in die Digitalwirtschaft und die relevante EU-Infrastruktur zu stärken sowie in der EU lebende Menschen vor Cyberattacken zu schützen. Diese Aufgaben nimmt die Agentur vor allem durch Capacity Building, Vernetzungsinitiativen, Zertifizierungen etc. wahr. Die ENISA ist keine polizeiliche oder militärische Organisation. In Relation zu den diversen Themenfeldern, der sich die ENISA annimmt, hat sie eher wenige Mitarbeiter:innen (ca. 60 bis 100). Darüber hinaus verfügt sie über verschiedene Beratungsgremien, Arbeitsgruppen und ein Netzwerk an nationalen Verbindungsoffizieren (NLOs) in den Mitgliedstaaten.

European Cybercrime Center (EC3)

Das 2013 gegründete EC3 ist eine Einrichtung der europäischen Polizeibehörde EUROPOL. Seine Aufgabe ist die Stärkung der Exekutivorgane im Kampf gegen vor allem transnationale Cybercrimes. Die EC3-Expert:innen geben nationalen Behörden strategische, operative, analytische und forensische Unterstützung bei der Bekämpfung von Online-Zahlungsbetrug, Kinderpornografie und anderen Cyberverbrechen. Dazu gehört auch der Kampf gegen illegale Aktivitäten im sogenannten Dark Web und anderen dunklen Ecken des digitalen Raums.

EU Intelligence and Situation Centre (EU-INTCEN)

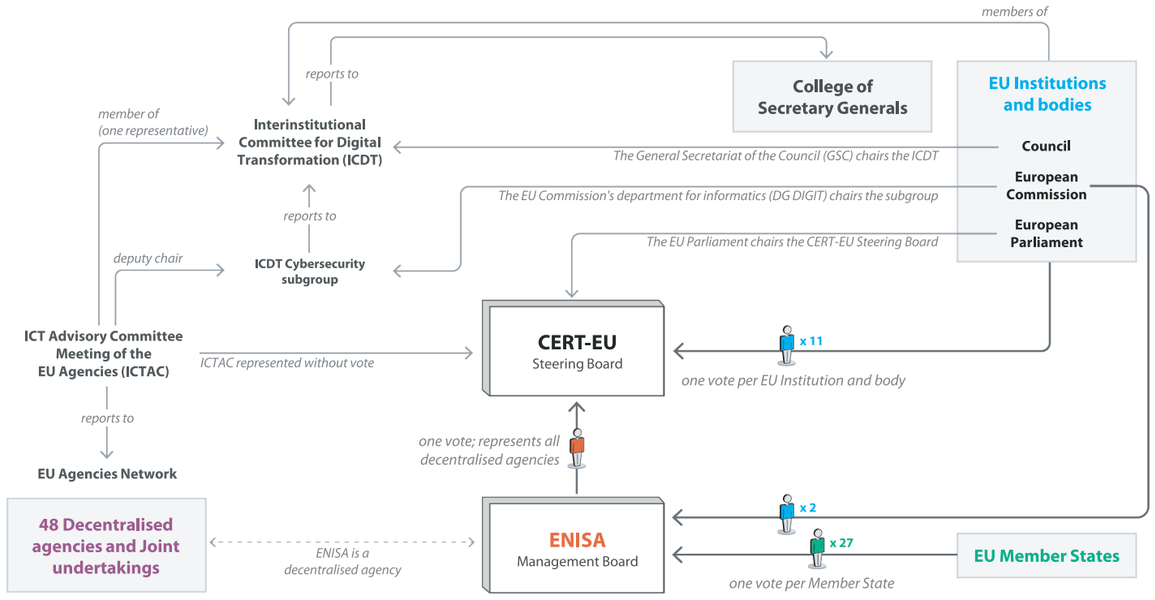
Das EU-INTCEN ist eine Einrichtung des Europäischen Auswärtigen Dienstes (EEAS) und damit direkt dem High Representative for Foreign Affairs and Security Policy der EU untergeordnet. Es ist das, was gemeinsam mit dem EUMSINT (siehe unten) einem europäischen Nachrichtendienst am nächsten kommt. Da Sicherheit weiterhin eine nationalstaatliche Kompetenz ist, beziehen sich seine Analysen auf Informationen, die es von den nationalstaatlichen Nachrichtendiensten erhält. Welche Informationen die Nachrichtendienste mit den europäischen Kollegen teilen, entscheiden die Mitgliedstaaten, sofern nicht anders geregelt (z.B. durch Berichtspflichten nach Cyberangriffen). 2016 wurde innerhalb dieses Diensts die sogenannte „Hybrid Fusion Cell" eingerichtet, die Entscheidungsträger:innen auf EU-Ebene mit Analysen und Lagebild bezüglich hybrider Bedrohungen versorgt. Sie verfügt über ein Netzwerk an nationalen Verbindungsoffizieren, die einander zweimal im Jahr zum Austausch treffen und die Koordinatoren zwischen

verschiedenen Ressorts innerhalb der Mitgliedstaaten sind. Die Hybrid Fusion Cell arbeitet beim Thema Cybersecurity und -defence darüber hinaus eng mit dem Intelligence Directorate des EU-Militärstabs (EUMSINT) zusammen. Beide haben Kompetenzen im Bereich Hybride Bedrohungen.

Computer Emergency Response Team der Europäischen Kommission (CERTEU)

Dabei handelt es sich um ein IT-Notfallteam der Europäischen Kommission, das alle Organe, Einrichtungen und Agenturen der Europäischen Union unterstützt. Ergänzend zu ENISA arbeitet das CERTEU ebenfalls im Bereich Prävention und Aufklärung und unterstützt auch im Bereich „Incident Response". Ist eine EU-Organisation etwa akut von einem Cyberangriff betroffen, so kann das CERTEU die Reaktion darauf koordinieren, verfügbare Informationen auswerten und analysieren bzw. verifizieren. Gleichzeitig ist das CERT dafür verantwortlich, Schwachstellen der technischen Infrastruktur der EU-Institutionen etc. zu identifizieren und zu bekämpfen. Das passiert u.a. durch Penetrationstests und „ethical hacking techniques".

Abbildung 3: Aufbau Computer Emergency Response Team der Europäischen Kommission (CERTEU)



Quelle: European Court of Auditors

1.2.2 NATO

Das Thema Cyberdefense ist bereits seit 2002 auf der politischen Agenda der NATO. Allerdings dauerte es eine Weile, bis das Bündnis in diesem Bereich ausgereifte Policies, Strukturen und Governance etabliert hatte. Hier einige Meilensteine und eine Übersicht über die heutigen Strukturen.

Am NATO-Gipfel im Juli 2016 in Warschau erfolgte die offizielle Anerkennung des Cyberraums als „domain of war"/„domain of operations", als Kriegs- bzw. Einsatzdomäne zusätzlich zu Luft, Land und Meer, welche die bestehenden Domänen waren. Dieser Schritt war insofern ein wesentlicher, als dass er bedeutete, dass die NATO mehr Fokus auf die Entwicklung von Ressourcen, Fähigkeiten und Fertigkeiten in diesem Bereich legen würde. Es ging also um operative Schritte, die die NATO mit dieser Anerkennung setzte. Die NATO bekannte sich darüber hinaus dazu, die NATO-EU-Cyberdefence-Kooperation auszubauen und sich für Transparenz und verantwortungsbewusstes Agieren von Staaten im Cyberraum einzusetzen.

Das vorwiegende Ziel der NATO im Cyberraum ist der Schutz der eigenen Netzwerke und Operationen zur Unterstützung seiner Mitglieder und Partner beim Resilienzaufbau. Die NATO-Alliierten bekennen sich dazu, dass Völkerrecht auch im Cyberraum gilt (NATO, 2022).

Comprehensive Cyber Defence Policy

Die NATO verfügt über eine sogenannte Comprehensive Cyber Defence Policy, welche die grundsätzlichen NATO-Aufgaben der Verteidigung und einer allgemeinen Abschreckungslogik stärken soll, und erklärt, dass Artikel 5 des NATO-Vertrags über „kollektive Selbstverteidigung" auch im Falle eines Cyberangriffs gilt. Darüber hinaus wird darin festgestellt, dass die NATO-Antwort auf einen solchen Angriff nicht notwendigerweise auf den Cyberraum beschränkt sein wird (NATO 2022, NATO 2018).

Cyber Space Operations Centre

Relativ neu ist das manchmal auch „NATO-Cyberkommando" genannte Cyber Space Operations Centre der NATO. Es bietet den NATO-Kommandanten Unterstützung bei der Lagebilderstellung und koordiniert die den Cyberspace betreffenden operativen Aktivitäten der NATO, das betrifft auch Abschreckung. In diesem Zentrum sind bei voller Besetzung 70 Cyberexpert:innen im Einsatz, die durch die Nachrichtendienste der Mitgliedstaaten mit Informationen gefüttert werden, um ein Echtzeit-Lagebild zu erstellen (Emmott, 2018).

Chief Information Officer (CIO)

Der NATO Chief Information Officer (CIO) ist eine neue Position. Der erste CIO wurde 2021 ernannt. Er ist dafür zuständig, Integration und für funktionierende Interoperabilität wesentliche Aspekte der NATO Informations- und Kommunikationstechnologiesysteme und die gemeinsame Entwicklung neuer IKT-Fähigkeiten zu überblicken und koordinieren. Er hat auch eine Single-Point-of-Contact-Funktion innerhalb der NATO für alle Cybersecurity-Angelegenheiten. Dazu gehören auch Incident Management, strategische Investments und NATO-weite Bewusstseinsbildung für strategisch relevante Themen im Cyberbereich (NATO, 2022).

NATO Computer Incident Response Capability (NCIRC)

Das NCIRC ist im Brüssler Hauptquartier der NATO untergebracht und gehört zur NATO-Kommunikations- und Informationsagentur. Es ist für den Schutz der NATO-eigenen Netzwerke zuständig und stellt 24 Stunden am Tag Unterstützung für etwaige Cybervorfälle zur Verfügung.

Centres of Excellence

Die NATO verfügt über eine bedeutende Anzahl an sogenannten Centres of Excellence, die über ihre Mitgliedstaaten verteilt sind. Für den Cyberbereich besonders wichtig ist das **Cooperative Cyber Defence Centre of Excellence (CCDCOE)** in Tallinn. Dessen Mission ist das Zurverfügungstellen von interdisziplinärer Expertise für die Abwehr von Cyberbedrohungen. Das betrifft vor allem die Bereiche Technologie, Strategie, Operations und Recht. Es ist ein Forschungs- und Ausbildungs- und Übungszentrum und bietet auch Staaten, die nicht der NATO angehören, die Möglichkeit, sich einzubringen (CCDCOE, 2022). Für den Cyberbereich außerdem relevant ist das **Strategic Communications (STRATCOM) COE** in Riga, das für die Bekämpfung von Desinformation wesentlich ist und durchaus kreative Ansätze dabei hat. So entwickelte STRATCOM das Online-Game Newshero (LSE, 2018), um Quellenkritik zu schulen, oder gab Studien zum Thema Humor als Waffe gegen Desinformation und Propaganda in Auftrag (Ozolina et.al, 2017). Das Zentrum legt einen Fokus auf Public Diplomacy und Public Affairs und psychologische Operationen (STRATCOM COE, 2022). Auch das **European Centre of Excellence for Countering Hybrid Threats (Hybrid COE)** hat eine Rolle in der Bekämpfung von Cyberbedrohungen. Es arbeitet an der Schnittstelle zwischen NATO und EU und koordiniert gemeinsame Übungen (Hybrid COE, 2022).

Über all diese Einrichtungen hinaus betreibt die NATO noch eine Reihe von anderen Ausbildungsstätten wie die **NATO School** in Oberammergau, Deutschland oder die **NATO Communications and Information Academy** in Oeiras, Portugal, und das **NATO Defence College** in Rom. Auf der **NATO Cyber Range** in Estland finden Übungen und Training im Bereich Cyberabwehr statt. Die NATO betreibt auch

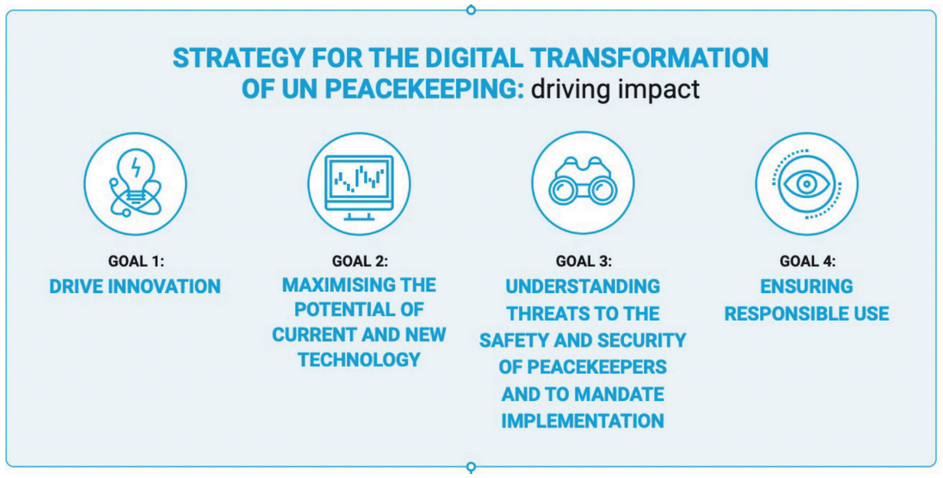
eine **Industry Cyberpartnership,** innerhalb der sie mit privaten Unternehmen kooperiert, um die Gesamtresilienz der NATO-Staaten zu fördern (NATO, 2022).

1.2.3 Vereinte Nationen

Auch innerhalb der Vereinten Nationen gibt es Stellen und Strategien, die dazu dienen sollen, die Cybersecurity zu steigern und Bedrohungen im Cyberraum abzuwenden.

Die **Roadmap for Digital Cooperation** wurde im Juni 2020 vom Büro des UN-Generalsekretärs veröffentlicht. Sie beschäftigt sich damit, wie die Weltgesellschaft besseren Nutzen aus digitalen Technologien ziehen kann und beinhaltet Empfehlungen, die auf Input von Mitgliedstaaten, dem Privatsektor, der Zivlgesellschaft, der Tech Community und anderen basieren. Das Ziel: ein sichererer und gerechterer Digitalraum für alle (UN Office of the Secretary General's Envoy on Technology, 2020). Die **UN Data Strategy** zielt auf einen besseren Datenaustausch bei höherem Schutz zwischen den Mitgliedstaaten ab und dient auch der Förderung einer datengetriebenen Kultur innerhalb der UN. Mit der **Strategy on New Technologies** wollte die UN definieren, wie sie die Nutzung neuer Technologien konkret vorantreibt. Die **Action for Peacekeeping (A4P+)** und die **Strategy for the Digital Transformation of UN Peacekeeping** beinhalten Empfehlungen und Strategien für innovatives, digitalisiertes und datengetriebenes Peacekeeping, und die **ICT Strategy** konzentriert sich auf die Modernisierung, Transformation und Innovation des IKT-Bereichs (UN Peacekeeping, 2021).

Abbildung 4: Wesentliche Ziele der Strategy for the Digital Transformation of UN Peacekeeping



Quelle: UN Peacekeeping

Stand 2022 verhandeln die Mitgliedstaaten der UN eine neue Konvention über die Nutzung von Informations- und Kommunikationstechnologien für illegale Zwecke. Ein Entwurf soll vom „Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes" der UN Generalversammlung bei ihrer 78. Sitzung vorgelegt werden (UNODC, 2022).

Unter den UN-Institutionen, die sich mit einem oder mehreren Aspekten der Cybersicherheit beschäftigen, verdienen Folgende besonderes Augenmerk:

UN Office on Drugs and Crime (UNODC)

Die meisten operativen Aktivitäten der UN im Bereich der Bekämpfung von Cyberbedrohungen liegen beim UN Office on Drugs and Crime (UNODC). Mit dem UNODC Cybercrime Repository ist in dieser Institution auch ein umfangreiches Archiv relevanter Daten von Cybercrime vorhanden. Die Ziele des UNODC sind etwa im Cyberbereich gut ausgebildete Polizeibeamt:innen, Strafverfolger:innen und Richter:innen, internationale Kooperation und Informationsaustausch bei der Bekämpfung von Cybercrime. Diese Ziele fördert sie etwa durch Trainings, Workshops und auch einem Monitoring der Maßnahmen gegen Cybercrime, die Mitgliedstaaten setzen. In der UNODC sind auch oft Arbeitsgruppen für die Erarbeitung neuer Strategien oder Policies angesiedelt.

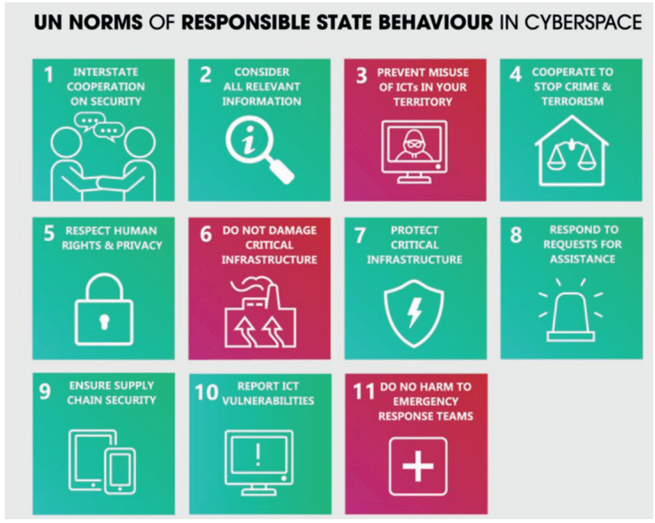
UN Office of Disarmament Affairs (UNODA)

Auch UNODA hat Kompetenzen im Cyberraum. Diese haben aber weniger mit der zivilen Komponente zu tun, sondern vielmehr mit Fragen von globaler Sicherheit und digitaler Abrüstung. In diesem Kontext legte die von diesem Büro eingesetzte UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE) 2021 einen Katalog von 11 Normen für verantwortungsbewusstes staatliches Agieren im Cyberraum vor (Australian Strategic Policy Institute, 2021). Diese sind quasi die Handlungsanleitung zur Selbstregulierung der UN-Mitgliedstaaten.

Office of Information and Communications Technology (OICT)

Das UN Office of Information and Communications Technology (OICT) ist dem Büro des zuständigen Assistant Secretary General der UN unterstellt und soll sich um eine „bessere, sichere, nachhaltigere Zukunft durch innovative Technologie" kümmern. Analyse neuer Technologien, Technikfolgenabschätzung und strategische Aufgaben gehören zu den Kernaufgaben des OICT (Unite, 2022).

Abbildung 5: Normen für verantwortungsbewusstes staatliches Agieren im Cyberraum



Grafik: Australian Strategic Policy Institute, ASPI, 2021

Kapitel 2

Vier Themenfelder zur Stärkung der Cyberinfrastruktur in Europa

Wie Kapitel 1 gezeigt hat, wurde auf die steigende Cyberbedrohungslage weltweit mit Investitionen in die Cybersicherheit, neuen Gesetzen und neuen Organisationen reagiert. Durch neue technologische Möglichkeiten und die De-facto-Dominanz von Informations- und Telekommunikationstechnologien in unserem gesellschaftlichen Alltag ist eine Weiterentwicklung der Cybersicherheit weiterhin eine zentrale Aufgabe politischer Entscheidungsträger:innen.

Während Resilienz in den letzten Jahren zu einem Modewort geworden ist, zeigt sich, dass es in vielen Fällen für einen effektiven Resilienzaufbau zu spät ist bzw. unsere Gesellschaft sehr weit vom Resilienzideal entfernt ist. Welche Hürden für die europäische Souveränität im digitalen Raum noch bestehen und wie diese gelöst werden können, wird in Kapitel 3.1 erläutert. Auch wenn Cybersecurity nicht mit Cyberdefense verwechselt werden sollte, gehört beides zusammen. Kapitel 3.2 widmet sich wesentlichen Themenfeldern, auf deren Basis Cyberdefense die Cybersecurity-Politik in Europa verbessert. Nicht zuletzt aufgrund des demografischen Wandels wird seit Jahren von einem Fachkräftemangel im IKT-Bereich gesprochen. In kaum einer Branche ist er so evident wie bei der Cybersicherheit. Nicht zuletzt aufgrund des starken Wachstums in wenigen Jahren gibt es weltweit personelle Kapazitätsprobleme. Wie dieser Fachkräftemangel gelöst werden kann, wird in Kapitel 3.3 beschrieben. Kritische Infrastruktur wie beispielsweise Energiebetreiber stehen seit dem Aufkommen von Cyberangriffen nach und nach immer mehr im Fokus einer effektiven Cybersecurity-Policy. Das ist aus gutem Grund so, zeigt doch etwa das Beispiel des US-Pipelinebetreibers Colonial Pipeline, dass aufgrund eines Cyberangriffs fast die Hälfte der Kraftstoffversorgung der US-Ostküste temporär gezwungenermaßen eingestellt werden kann. Dennoch zeigt sich empirisch, dass über 40 Prozent aller erfolgreichen Cybersecurityangriffe Klein- und Mittelbetriebe betreffen. Gerade für Mitgliedstaaten der Europäischen Union ist die Sicherheit von Klein- und Mittelbetrieben von elementarem Interesse, da diese 99 Prozent aller Unternehmen in der EU ausmachen und über 100 Millionen Menschen beschäftigen (Europäische Kommission 2022a). Kapitel 3.4 zeigt Maßnahmen auf, um die Cybersicherheit von Klein- und Mittelbetriebe zu stärken.

2.1 Resilienz, Souveränität und strategische Autonomie im Digitalbereich

Im europäischen Sprachgebrauch herrscht beim Thema Handlungsfähigkeit im Sicherheitsbereich manchmal ein wenig Unordnung. Semantisch auf unterschiedlichen Hierarchie-Ebenen stehende Begriffe werden oft synonym verwendet, bzw. erschwert es die Übersetzung in so manche Sprache eines Mitgliedstaats eine klare Unterscheidung unterschiedlicher Begriffe und Konzepte.

Der Strategische Kompass der Europäischen Union ist die Strategie, die die EU zu einer *souverän/autonom* planenden und handelnden Akteurin machen soll. Das bedeutet einerseits, dass die EU sicher vor ungebetener Einmischung von außen sein muss, um die Sicherheit ihrer Bürger:innen zu gewährleisten. Andererseits muss die Union möglichst unabhängig von anderen – möglicherweise andere strategische Ziele verfolgenden – Mächten sein. In Zeiten globaler Produktions- und Lieferketten ist das ein schwieriges Unterfangen, und es sei festgestellt, dass Unabhängigkeit nicht mit Protektionismus und Isolation gleichzusetzen ist. Das Beispiel der Gasabhängigkeit von Russland und den Folgen für die Europäische Union seit Beginn des russischen Angriffskriegs in der Ukraine im Februar 2022 zeigt jedoch gut, welche Situation es zu vermeiden gilt. Betrachtet man die Aktivitäten, die etwa der US-Konzern Apple setzt, um seine durch die langen Lockdowns für die Produktion problematisch gewordene Abhängigkeit von China zu reduzieren (Jennings, 2020), so könnte eine gewisse Diversifizierung, also eine Aufteilung der wesentlichen Produktion auf unterschiedliche Länder, idealerweise solche Länder, die z.B. Allianzpartner in der NATO sind, oder sonst ein enges Naheverhältnis zum eigenen Staat haben, ein Lösungsweg sein.

Gemäß ENISA (2021c) basiert digitale Souveränität, also Handlungsfreiheit, auf drei Komponenten: der individuellen Datensouveränität, der politischen Souveränität, um Normen und Standards zu beeinflussen, und der Souveränität der datengetriebenen Industrie. Demzufolge definiert sie digitale strategische Autonomie als die Fähigkeit Europas, Produkte und Dienstleistungen zu beziehen, die ihren Bedürfnissen und Werten entsprechen, ohne ungebührlichen Einfluss von externen Akteuren (siehe ENISA 2021c).

Das Erreichen der beiden Ziele Unabhängigkeit und Widerstandsfähigkeit gegen Einfluss von außen, um strategische Autonomie im Digitalbereich

herzustellen, beruht auf unterschiedlichen Aspekten. Wesentlich für Europa sind dabei einerseits die Implementierung von an europäischen Werten und den Gegebenheiten des europäischem Binnenmarkts orientierten Cyber Policies. Beides ist nicht immer leicht unter einen Hut zu bekommen und erfordert einen aktiven Interessenausgleich.

Möglichst europäische Produktion digitaler Produkte (Software und Hardware) und Services, die wichtig für Sicherheit und Funktionalität der europäischen Demokratien und Volkswirtschaften sind, steigern unsere Widerstandsfähigkeit, ebenso wie eigene europäische Digitalinfrastruktur für Wirtschaft und Verwaltung.

Darüber hinaus braucht es fortwährend auch Bewusstseinsbildung bei und Vertrauensarbeit mit den Einwohner:innen Europas, um eine Beeinflussung von außen zu minimieren.

Und schließlich sind auch die Ausbildung von Fachkräften und die Fähigkeit, diese anschließend am Standort zu halten, ein wichtiger Grundpfeiler europäischer Handlungsfähigkeit im Digitalbereich. Dazu gehört auch lebensnahes Capacity Building bei nicht im IKT-Sektor tätigen Personen aller Altersgruppen. Mit diesem Aspekt befassen sich die Kapitel 3.3 und 3.4.

„Resilienz" ist das Modewort der Sicherheitspolitik in den 2020er Jahren. Die Idee, dass es effektiver und effizienter ist, einen Staat, eine Organisation und auch Einzelpersonen so weit gegen Cyberbedrohungen aller Art zu immunisieren, dass sie durch etwaige Angriffe etc. gar nicht erst Schaden nehmen können, ist eine hervorragende. Leider hat die westliche Welt das Konzept erst jetzt für sich entdeckt. In vielen für die Sicherheit relevanten Bereichen ist es entweder zu spät für einen lückenlosen effektiven Resilienzaufbau, oder ein solcher ist mit hohen wirtschaftlichen Kosten bzw. mitunter auch mit hohen politischen Kosten verbunden (Erhardt, 2019).

Infrastruktur

Ein Beispiel dafür ist die Debatte um die besonders unter Jugendlichen weltweit beliebte Smartphone-App TikTok. Die App gehört der chinesischen Firma *ByteDance,* die in ihren Statements stets darauf besteht, nicht von der chinesischen Regierung kontrolliert zu werden (BBC, 2020). Das Unternehmen steht unter dem Verdacht, User-Daten an die chinesische Regierung weiterzugeben, was ByteDance-Sprecher stets abstreiten. Eine Buzzfeed-Recherche im Juni 2022 zeigte jedoch, dass es legitimen Grund gibt, an den Beteuerungen des Unternehmens zu zweifeln. Geleakte Audio-Aufzeichnungen von über 80 internen TikTok-Meetings der Mutterfirma ByteDance weisen darauf hin, dass sogenannte Master User, die sich innerhalb Chinas befinden, auf nichtöffentliche Daten von US-TikTok-Usern zugegriffen haben, was Zugriffsrechte impliziert, die nicht einmal die US-Angestellten von ByteDance haben. In die Zeit von September 2021 bis Jänner 2022, in der der Datenzugriff stattgefunden haben soll, fällt die Zeugenaussage eines hohen TikTok-Executives vor dem US-Senat. Darin schwor er, dass ein Team von weltweit anerkannten, in den USA ansässigen Experten entscheide, wer Zugriff zu den Daten erhält. In einer der geleakten Audioaufzeichnung von TikTok-Mitarbeitern sagt offenbar jemand: „Everything is seen in China" (Buzzfeed, 2022). Um das Unternehmen vor größerem Schaden zu bewahren, kündigte ByteDance kurz darauf an, alle Daten von US-Usern ab diesem Zeitpunkt in den USA zu lagern, indem alle Daten an das US-Unternehmen Oracle übergeben werden. Auch wenn viele Experten das als klugen Schachzug bezeichneten, ist das Misstrauen westlicher Regierungen dadurch nicht erloschen.

Einer Analyse von netzpolitik.org zufolge (Meineck und Fanta, 2022) ist das Neue an der Buzzfeed-Recherche nicht, dass dieser Datenzugang existiert – das war zuvor von TikTok selbst angesprochen worden – sondern wie umfassend der Zugang ist. Die Autoren weisen auch darauf hin, dass der Konzern Bytedance nicht automatisch mit der chinesischen Regierung gleichzusetzen ist, jedoch das chinesische Regime Unternehmensanteile besitze und „Regimetreue für chinesische Unternehmen Pflicht ist". Gemäß einer Recherche des *Wired*-Magazins sammelt TikTok eine Menge Daten, ohne den Usern konkret mitzuteilen, welche davon mit Dritten geteilt werden. *Wired* zitiert die Vizepräsidentin für Threat Research bei Proofpoint, die sagt, das Ausmaß der Berechtigungen, die TikTok von seinen Usern verlangt, sei größer als bei anderen Plattformen. Zwar könne man diesen Zugriff ablehnen, das schränke jedoch die Funktionalität der App ein (O'Flaherty, 2021). TikTok hat über 1,5 Milliarden aktive User, über die die chinesische Regierung möglicherweise bestens Bescheid weiß, egal ob in diesem Jahr die US-Daten zur Firma Oracle übersiedelt wurden (Bloomberg, 2022). Ungeachtet dessen, wie viel ein Staat in die Resilienz gegen solche Datenzugriffe investiert, wird das Wissen über die bis hierhin aktiven User nicht mehr löschbar sein.

Noch weitreichendere Konsequenzen von Entscheidungen, die zum Teil bereits vor Jahren getroffen wurden, gibt es im Bereich Infrastruktur. Das betrifft einerseits 5G-Infrastruktur, aber auch chinesische Direktinvestitionen in Europa. Im Strategischen Kompass der Europäischen Union (2022) heißt es, es brauche „einen konkreten und realistischen Plan für Europa, damit es alle wesentliche Cyberinfrastruktur selbst entwickelt, besitzt und kontrolliert, damit die strategische Autonomie im Cyberraum so gut gesichert werden kann wie möglich". Die Entscheidung, gemeinsam mit China 5G-Infrastruktur zu erforschen, fiel im Jahr 2015 (Europäische Kommission, 2015). Bis heute haben mehrere EU-Länder gemeinsam hohes Risikopotenzial identifiziert, dass manche 5G-Anbieter möglicherweise von ausländischen Geheimdiensten für Manipulation verwendet werden. Auch vor einem versteckten „Schalter" in dieser Infrastruktur, mit dem China dem Westen das Netz abdrehen könnte, fürchtet man sich. Aus diesem Grund haben manche Regierungen (Australien, Neuseeland, Israel, Südkorea, Japan, Vietnam) China aus den Produktionsketten für ihre 5G-Infrastruktur ausgeschlossen (Gorman, L., 2020). Realistisch betrachtet, müssen sowohl die USA als auch Europa der Tatsache ins Auge sehen, dass China sein 5G-Netz wesentlich schneller ausbaut als der Westen, wenn auch nicht ganz ohne Probleme. Will man mit dem technologischen Fortschritt in China mithalten, so wird man in den nächsten Jahren große Sprünge machen müssen, um diese Infrastruktur – strategisch autonom – selbst zu erschaffen (Strumpf, 2020).

Auch andere Versäumnisse der Vergangenheit beeinflussen heute die Resilienz unserer Gesellschaft gegenüber Cyberangriffen. Ein weiteres Beispiel dafür ist, dass bei der Digitalisierung von z.B. Schulen nicht ausreichend Wert darauf gelegt wurde, diese gegen Cyberangriffe zu schützen, erschien doch eine Schule als wenig lohnendes Ziel für Hacker. Als Vehikel für Botnet-Attacken auf wiederum andere Institutionen eigenen sich jedoch schlecht abgesicherte Schulen sehr wohl. Das betrifft genauso jeden Kleinbetrieb, in dem Computer stehen und Angestellte im besten Fall Grundkenntnisse von Bedrohungen im Netz haben. In den meisten Betrieben, deren Kerngeschäft nicht IT ist, gibt es keine verpflichtenden, regelmäßigen Cybertrainings.

Die europäische Datenlage

Während in den letzten zehn Jahren eine Vielzahl an Richtlinien und Gesetzen auf europäischer und nationaler Ebene beschlossen wurde, zeigen sich in der Praxis oftmals noch sehr heterogene Herangehensweisen bei zentralen Themenfeldern wie beispielsweise der Bewusstseinsbildung für Cybersecurity. Da über 80 Prozent aller Cyberattacken auf Social Engineering beruhen, ist Bewusstseins- und Wissensvermittlung von zentraler Bedeutung. Wie ENISA in einer ländervergleichenden Studie (2021d) zeigt, sind sowohl die Zielsetzungen als auch die Bevölkerungsgruppen, die angesprochen werden sollen, von Land zu Land sehr unterschiedlich definiert. Während das Ziel in Luxemburg der Aufbau von Vertrauen in die digitale Welt und den Schutz der Menschenrechte im Internet ist, setzt sich die lettische Cybersecurity-Strategie den Aufbau einer Informationsgesellschaft zum Ziel (ENISA 2021d). Zwar wird in allen Strategien ein Ausbau des Bewusstseins für die Allgemeinbevölkerung angegeben, konkrete Maßnahmen finden sich jedoch oftmals nur für bestimmte Zielgruppen. Während die Slowakei Maßnahmen zur Verbesserung des Cyberverständnisses von öffentlich Bediensteten und IT-Fachkräften definiert, inkludiert die finnische Cyberstrategie auch den NGO-Sektor, und Lettland legt einen Fokus auf Studierende und Lehrkräfte (ENISA 2021d). Dies bedeutet in der Praxis, dass in jedem Mitgliedsland unterschiedliche Ziele und Zielgruppen im operativen Alltag angesprochen werden und somit die Messbarkeit und Vergleichbarkeit erschwert wird. Dadurch ist es für die EU schwieriger, potenzielle Schwachstellen bei der Bewusstseinsbildung zu adressieren.

Grundsätzlich ist eine Heterogenität bei Zielgruppen nachvollziehbar, unter anderem aufgrund der geopolitischen Lage und damit einhergehenden unterschiedlichen Bedrohungswahrnehmungen. Auch unterschiedliche Wirtschaftsstrukturen in den einzelnen Mitgliedstaaten spielen eine Rolle. Dennoch muss sichergestellt sein, dass grundsätzliche Ziele und Maßnahmen, insbesondere wenn es um die Gesamtbevölkerung geht, harmonisiert werden. Als Fallbeispiel für eine niederschwellige Information und Sensibilisierung dient der „Cyber Weather Report" des finnischen National Cyber Security Center (NCSC 2022). Der Cyber Weather Report bietet ein Update zu den wichtigsten Informationssicherheitsvorfällen und Bedrohungslagen des Monats. An einen Wetterbericht angelehnt, werden alle Bereiche einer von drei Kategorien zugeordnet: ruhig, besorgniserregend oder ernst. Die Regelmäßigkeit des Formats erhöht seinen Bekanntheitsgrad in der Bevölkerung, und die klare Kategorisierung hilft den Einwohner:innen bei der Beurteilung von Risiken. Die Maßnahme ist darüber hinaus vergleichsweise kostengünstig und kann leicht über den öffentlichen Rundfunk implementiert werden.

Wie in allen Bereichen gilt auch für die Cybersicherheit, dass effektive Maßnahmen nicht ohne Evidenz gesetzt werden können. Im Falle der Bewusstseins- und Wissensvermittlung von Cybersicherheit, werden über Eurobarometer regelmäßig Daten für alle Mitgliedstaaten erhoben. Diese werden oftmals durch nationalstaatliche Umfragen ergänzt. Während etwa Estland jährlich Fragen zum Bewusstsein um Cyberkriminalität erhebt, werden in Belgien Daten zu Cybersicherheitspraktiken erhoben (ENISA 2021c). Nicht zuletzt wegen der Gefahr durch Social Engineering ist es ratsam, auch Daten zu Einstellungen und Verhaltensweisen zu erheben, dennoch fehlt es in Europa oftmals an grundlegenden Daten. Das Fehlen einer gemeinsamen Messmethodik der EU-27 sorgt laut ENISA für Unsicherheiten darüber, was die relevanten Indikatoren für die Cybersicherheitskultur wirklich sind (ENISA 2021c).

Ein weiteres Beispiel dafür, was in einer Taxonomie für Cybersicherheit enthalten sein sollte, sind bessere Daten zu Direktinvestitionen aus dem Ausland (Foreign direct incvestment, FDI). Diese Investitionen haben in den letzten Jahrzehnten weltweit für Wachstum und Entwicklung gesorgt, Arbeitsplätze geschaffen und den Wohlstand verbessert. Die Beseitigung von Hindernissen für Kapitalzuflüsse führt dazu, dass Empfängerländer das potenzielle Risiko für die nationale Sicherheit oder die öffentliche Ordnung managen müssen (OECD 2009). China ist nicht nur auf Basis seiner Cyberkapazitäten für Europa von Relevanz. Gerade in den Bereichen Wirtschafts- und Konkurrenzspionage oder Spionage aus politischen Gründen ist es zentral, aus europäischer Sicht Investitionen aus China zu screenen (Herpig 2021) und gegebenenfalls einzuschränken. Welche Auswirkungen dies in der Praxis hat, zeigt ein Bericht des German Marshall Fund (Christiani, D. et. al 2021).

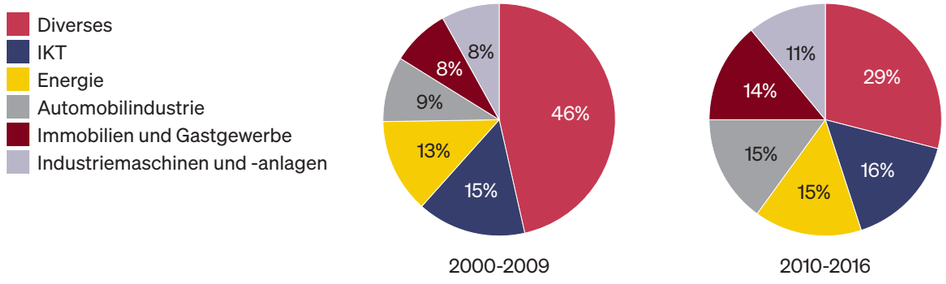
In den letzten Jahren hat China im Rahmen der „Belt and Road Initiative" unter anderem massive Investitionen in die Bahninfrastruktur Ungarns oder die Hafeninfrastruktur in Griechenland getätigt. Beide Länder haben die EU daran gehindert, China wegen Menschenrechtsverletzungen, einschließlich der angeblichen Folter von Menschenrechtsanwält:innen, zu verurteilen. Sowohl Ungarn als auch Griechenland lehnten 2016 eine gemeinsame Position der EU zum Konflikt im Südchinesischen Meer ab (Christiani, D. et. al 2021). Gerade wenn es um zentrale digitale Infrastruktur geht, ist es für die digitale Souveränität von vitalem Interesse, Investitionen aus dem Ausland zu screenen. Wie ein Bericht des European Think-tank Network on China (ETNC) zeigt, besteht insbesondere im 5G-Sektor eine massive Abhängigkeit von China in einigen Mitgliedstaaten, was dazu führte, dass Österreich, Ungarn und Griechenland Maßnahmen gegen den chinesischen Konzern Huawei blockierten (Seaman, J. et. al 2022).

Doch abseits derartiger Meldungen wissen wir oftmals wenig über ausländische

Direktinvestitionen. Von 2000 bis 2016 wurden laut RHG FDI.Monitor mehr als 1.400 einzelne FDI-Transaktionen chinesischer Investoren in der EU im Wert von insgesamt 101 Milliarden Euro registriert, während Eurostat 58 Milliarden Euro auflistet (Seaman, J. et. al 2022). Sowohl in der Zeitspanne 2000–2009 als auch 2010–2016 gingen jeweils 15 Prozent der chinesischen Direktinvestitionen in den europäischen IKT-Sektor, während insbesondere in den letzten Jahren ein Anstieg im Transport- und Infrastruktursektor zu beobachten ist (ENTC 2017).

Abbildung 6: China investiert stark in Europas IKT-Sektor

Chinesische Direktinvestitionen in Europa



Quelle: RHG FDI Monitor

Derartige Daten sind oftmals geschätzt und granulare Daten, insbesondere auf Ebene der Mitgliedstaaten sind sie oft nicht vorhanden (ENTC 2017, 2022). Zuverlässige Informationen über ausländische Direktinvestitionen aus China werden für die Lösung eines breiten Spektrums politischer Herausforderungen in den EU-Mitgliedstaaten von entscheidender Bedeutung sein. Für zukünftige Handels- und Investitionsabkommen könnten in jenen Bereichen, in denen von China stark investiert wird, im Gegenzug eine Ausweitung des Marktzugangs für europäische Unternehmen in China erfolgen und Rechtssicherheiten für Investoren gestärkt werden, um Abhängigkeiten zu minimieren.

Wie dieses Beispiel zeigt, braucht es einen Mix aus strukturellen Indikationen (beispielsweise FDI in Schlüsseltechnologien), Daten zu Einstellungen und Verhaltensweisen im Cybersecurity-Bereich und sicherheitspolitisch relevante Indikatoren wie Statistiken zu Zero-Day-Incidents. Waldron (2019) führt aus, dass ein System von Metriken erforderlich ist, die Entscheidungsträger nutzen können und die innerhalb der relevanten Stakeholdergruppen akzeptiert sind. Hierzu benötigt es eine Taxonomie sowie ein gemeinsames Verständnis davon, was wir unter „digitaler europäischer Souveränität" verstehen und welchen Beitrag Cybersecurity-Akteure hier leisten müssen. Nicht zuletzt müssen quantitative und qualitative Indikatoren entwickelt werden, die eine Evaluation ermöglichen, wie gut Richtlinien und Verordnungen in den Mitgliedstaaten umgesetzt wurden.

Ein weiterer wesentlicher Faktor für eine europäische strategische Autonomie im Digitalbereich ist Cloud Computing. Dieses ermöglicht die Bereitstellung von Computerdiensten über das Internet. Das bedeutet, Unternehmen kaufen Lizenzen, um bestimmte Programme online nutzen zu können, ohne sie onsite abspeichern zu müssen. Dadurch können Organisationen und Unternehmen flexibler (orts- und verbrauchsabhängig) auf Ressourcen zugreifen und Skalierungseffekte nutzen. Ebenso können ihre Daten zu niedrigeren Kosten gespeichert werden. Gartner (2019) prognostiziert, dass bis 2025 etwa 80 Prozent der Unternehmen ihre traditionellen Rechenzentren zugunsten von Cloud Computing schließen werden. Diese Entwicklung geht mit einem signifikanten Wertanstieg des europäischen Datenmarkts einher. Darunter versteht man jenen Markt, auf dem digitale Daten als Produkte oder Dienstleistungen aus Rohdaten ausgetauscht werden. Schätzungen der Europäischen Kommission zufolge wird der Datenmarkt in den EU-27 bis 2027 voraussichtlich 82,5 Milliarden Euro erreichen, mit einer durchschnittlichen jährlichen Wachstumsrate von 5,8 Prozent (Europäische Kommission 2020). In welcher Infrastruktur diese Daten also gespeichert und verwendet werden, ist also sehr wichtig.

Die Vereinigten Staaten und China sind dabei von zentraler Bedeutung. Wie Daten des UN Digital Economy Reports (UNCTAD 2021) zeigen, besitzen beide Länder zusammen 50 Prozent der globalen Hyperscale-Rechenzentren, haben die höchste 5G-Implementierung weltweit, besitzen 90 Prozent der Marktkapitalisierung der wichtigsten digitalen Plattformern und sind für 94 Prozent der Finanzierung von KI-Startups verantwortlich. Wie das Europäische Liberale Forum (ELF) in seiner Publikation „Cybersecurity in Context" zeigt, dominieren amerikanische Cloud-Service-Provider die europäischen Mitbewerber sowohl hinsichtlich des Geschäftsvolumens als auch bei technologischen Innovationen (Gamal, N., Martino, L., Nestoras, A. 2022).

Um diesen Rückstand zu minimieren und eine Dateninfrastruktur nach europäischen Maßstäben zu entwickeln, wurde 2019 GAIA-X ins Leben gerufen. GAIA-X ist eine internationale NPO mit Sitz im Belgien, die – gemäß ihrer Selbstdarstellung – auf Basis „europäischer Werte" Cloudanbieter in Europa vernetzen will. Derzeit nehmen 1.800 Teilnehmer von über 500 Institutionen an GAIA-X teil (GAIA-X 2022). GAIA-X wurde 2019 von den Regierungen Deutschlands und Frankreichs massiv vorangetrieben, um eine Cloud-Infrastruktur für den europäischen Markt zu schaffen, der den Datenaustausch innerhalb der EU auf Basis ihrer Gesetze erleichtert. Ziel sei es, eine „leistungsfähige, wettbewerbsfähige, sichere und vertrauenswürdige Dateninfrastruktur für Europa" aufzubauen, die die „höchsten Bestrebungen in Bezug auf digitale Souveränität bei gleichzeitiger Förderung von Innovationen" erfüllt (UNCTAD 2021). Dies solle auch einen einheitlichen Datenmarkt in der Europäischen Union erleichtern, was wiederum europäische Cloud-Anbieter befähigt, die Monetarisierung von Daten – und damit ihre internationale Wettbewerbsfähigkeit – zu stärken.

Europa steht hier vor einem Scheideweg, wenn es darum geht, die strategische Autonomie auch im Kontext des Bereichs Cloud-Computing weiterzuentwickeln. Entweder ist Europas Reaktion auf die massive Dominanz von China und den USA das Festschreiben von Standards, die innerhalb der EU gelten, dann muss GAIA-X zu einem EU-weiten Standard ausgebaut werden, der auch von globalen

Cloud-Anbietern genutzt werden muss, was derzeit nicht der Fall ist (UNCTAD 2021). Dies wird insbesondere mit den USA und ihren Cloud-Anbietern zu massiven politischen Spannungen führen. Alternativ kann GAIA-X dahingehend weiterentwickelt werden, dass sie europäischen Cloud-Anbietern kostenfrei zur Verfügung gestellt wird, damit diese sie in ihre Geschäftsmodelle implementieren und international wettbewerbsfähiger werden.

Das Beispiel Cloud-Infrastruktur ist nur eines von vielen dafür, dass weltweit ein deutlich unterschiedlicher Zugang zwischen den großen globalen Märkten in Europa, den USA und China beobachtet werden kann. Wie UNCTAD (2021) zeigt, sind in den Vereinigten Staaten marktbasierende Zugänge prioritär. Datenschutz und Privacy-Fragen werden aus Marktperspektive betrachtet, und Wettbewerbspolitik spielt eine geringe Rolle. In China ist die Dominanz von staatlichen Interventionen zu sehen, der Zugriff auf Daten für den Staat ist essenziell. Innerhalb der EU wird eine Regulierung auf Basis von individuellen Rechten der Marktteilnehmer präferiert und Wettbewerbsrecht als elementar betrachtet. Individuelle Rechte, die beispielsweise innerhalb der EU zentral sind, vertragen sich somit wenig mit US-Unternehmen, deren Geschäftsmodell und Regularien auf freiem Datenaustausch basieren, und chinesischen Social-Media-Applikationen, bei denen der Staat einen starken Zugriff auf Daten und Inhalte hat. Im Umkehrschluss sind europäische Unternehmen, die mit starken Regulierungen konfrontiert sind, global oftmals nicht wettbewerbsfähig. Ebenso ist der Zugriff von nationalen Sicherheitsbehörden sehr unterschiedlich. Da es sich um grundlegend unterschiedliche Zugänge handelt, sind somit Wirtschafts-, Außen und Sicherheitspolitik nicht voneinander zu trennen.

Dass derartige Zugänge nicht nur Daten und ihre Infrastruktur betreffen, sondern ein grundsätzlicher Zugang zu digitalen Themen sind, lässt sich am Beispiel künstliche Intelligenz aufzeigen, die massiv von digitaler Infrastruktur und guter Datenbasis lebt (Paschunder und Feierabend 2019). Dies hat zur Folge, dass Europa aus geopolitischer Perspektive die Abstimmung von Außen-, Sicherheits- und Wirtschaftspolitik verbessern muss, da eine europäische strategische digitale Autonomie zwangsweise Spannungen mit den derzeitigen Technologie- und Marktführern in den USA und China mit sich bringt. Gerade aus Sicherheitsperspektive ist dies von großer Relevanz, da im Zusammenhang mit Wirtschaftsspionage international etablierte Regeln und Normen darüber, welche Cyberaktivitäten legitimes oder illegitimes Verhalten darstellen, größtenteils fehlen (Hoffman & Maurer, 2019).

Tabelle 3: Internationale Zugänge zu datenbezogenen Regelungen

	USA	China	Europäische Union
Wachstum und Entwicklung der Digitalwirtschaft	hauptsächlich Marktbasiert	starke staatliche Eingriffe	Regulierungen und Unterstützung im Rahmen des "recovery plans" nach COVID 19
Datenschutz und Privatsphäre	Nicht historisch priorisiert; keine umfassenden Bundesgesetze, aber in einigen Bundesstaaten (Kalifornien, Virginia) umfassende Gesetze	Regulierung fokussiert auf Unternehmen	GDPR auf Basis von individuellen Grundrechten
Nationale Sicherheit	Daten für die nationale Sicherheit haben eine klare Priorität	Umfassender Zugang und Kontrolle durch die den Staat	Grundsätzlich Kompetenz der jeweiligen Mitgliedsstaaten
Wettbewerbspolitik	Daten werden in der Regel nicht als Wettbewerbsthema gesehen, jedoch derzeit kartellrechtliche Ermittlungen und Gerichtsverfahren	Unklare Regeln ob Daten unter Regelungen der Wettbewerbsregeln fallen	Daten sind teil der Wettbewerbspolitik
Grenzüberschreitender Datenaustausch	Förderung des freien Datenaustausches	Umfrangreiche Einschrenkungen	Frei innerhalb der EU und mit manchen Staaten; Handelspolitik fördert Datenaustausch, aber derzeit Inititativen die Beschränkungen fördern

Quelle: UNCTAD

Tabelle 4: Vergleichender Überblick über KI-Fokus in Nordamerika, China und der EUropäischen Union

Nordamerika	China	Europäische Union
starker öffentlicher F&E Techniksektor	Ambition KI-Weltmarktführer zu werden	Fokus auf verantwortungsvolle, vertrauenswürdige KI
Big-Data-Sammelmonopole	Social Credit Score	Legale, soziale und ethische Standards im Fokus
Kommerzielles Interesse und Seed-Finanzierung im Fokus	Staatlich standardisierte Bewertung des wirtschaftlichen und sozialen "Schutzes" der Bürger	GDPR auf Basis von individuellen Grundrechten
(Federal Communications Commission) & FTC (Federal Trade Commission) als Aufsichtsbehörden	Big Data wird für Disziplinarzwecke (u.a. public shaming) verwendet	Transparenz und nachvollziehbarkeit im Fokus
Kanada: Personal Information Protection and Electronic Documents Act (PIPEDA)	massiver technologischer Wandel in kurzem Zeitraum	Zivilrechtliche Regeln für Robotik

Source: Puaschunder & Feierabend / ELF 2019

Empfehlungen

Resilienz war jahrelang das Buzzword in der Sicherheitspolitik, jedoch wurden in Europa Maßnahmen oftmals zu spät gesetzt, wodurch eine Verbesserung der Resilienz nicht möglich war. Damit dies im Kontext der strategischen digitalen Autonomie nicht passiert, sind folgende Maßnahmen notwendig:

- Eine gemeinsame Verständigung von zentralen Zielen und Maßnahmen zur Stärkung der Bewusstseins- und Wissensvermittlung für Cybersecurity in Europa. Insbesondere niederschwellige Angebote, wie der „Cyber Weather Report" des finnischen National Cyber Security Center sind zu etablieren.
- Die European Cybersecurity Taxonomie muss um messbare Indikatoren für Cybersicherheit ergänzt werden. Dies gelingt mit einem Mix aus strukturellen Indikatoren, Daten zu Einstellungen und Verhaltensweisen im Cybersecurity-Bereich und sicherheitspolitisch relevanten Indikatoren.
- Im Bereich des Cloud-Computing muss entschieden werden, ob GAIA-X jener Standard sein soll, der auch von globalen Cloud-Anbietern in Europa genutzt werden muss, oder ob GAIA-X eine Infrastruktur zur Verbesserung der Wettbewerbsfähigkeit von europäischen Cloud-Anbietern sein soll.
- Die Abstimmung von Außen-, Sicherheits- und Wirtschaftspolitik muss verbessert werden, um die europäische digitale Souveränität zu stärken. Insbesondere auf internationaler Ebene muss das vorrangige Ziel sein, Normen und Verhaltensweisen zu etablieren, die illegitimes Verhalten im Kontext der Wirtschaftsspionage darstellen.
- Europa muss massiv in seine eigene Netzanbindung investieren, um eigene Infrastruktur im 5G- und Glasfaserbereich zu erschaffen und zu kontrollieren und sicherer vor etwaiger Manipulation durch China zu sein.

2.2 Verteidigung und Sicherheit

Während vor einigen Jahren unter Sicherheitsexperten noch die Rede von einer Verwischung der Grenze zwischen Krieg und Frieden war, stellt sich nunmehr das „Zeitalter des fortwährenden Konflikts" ein (Kolbe, 2020). Während es autokratischen Regierungen ein Leichtes ist, das offene, globale System und die enge Vernetzung liberaler Demokratien auszunutzen, fesselt eben die Freiheit des globalen Westens und anderer Demokratien ihnen oft die Hände auf den Rücken, wenn es darum geht, sich gegen Angreifer zu wehren (Bunde, 2022; Cooley und Nexon, 2022). Eine liberale Demokratie hat gute Gründe, keine Maßnahmen zur Massenüberwachung von Internetusern und Filterung von Netzcontent zu setzen, doch sie bezahlt für die Wahrung der Grundrechte und Freiheiten ihrer Bürger:innen einen Preis.

Demokratien sind leichter angreifbar, gilt es sie doch gegen leicht über digitale Massenmedien schürbare Ängste und Verschwörungstheorien zu verteidigen. Ein großer Anteil der Desinformationskampagnen, die auf Beeinflussung freier Wahlen abzielen, kann ganz klar nach Russland zurückverfolgt werden (Nakashima und Timberg, 2020). Diese Tatsache ist mittlerweile auch der breiten Öffentlichkeit bekannt. Doch das Wissen davon immunisiert nicht gegen diese Angriffe. Als etwa in Österreich Ende August 2022 die Zustimmungswerte für Sanktionen gegen Russland langsam zu sinken begannen, war das zum Teil die Folge visueller russischer Propaganda, die ein vereistes Europa zeigte. Spielend gelang es Russland, die Verbindung zwischen den Sanktionen gegen Russland und der angeblich unmittelbaren Folge des Erfrierens in einem Winter völlig ohne Gas zu verankern (Metzger et. al., 2022).

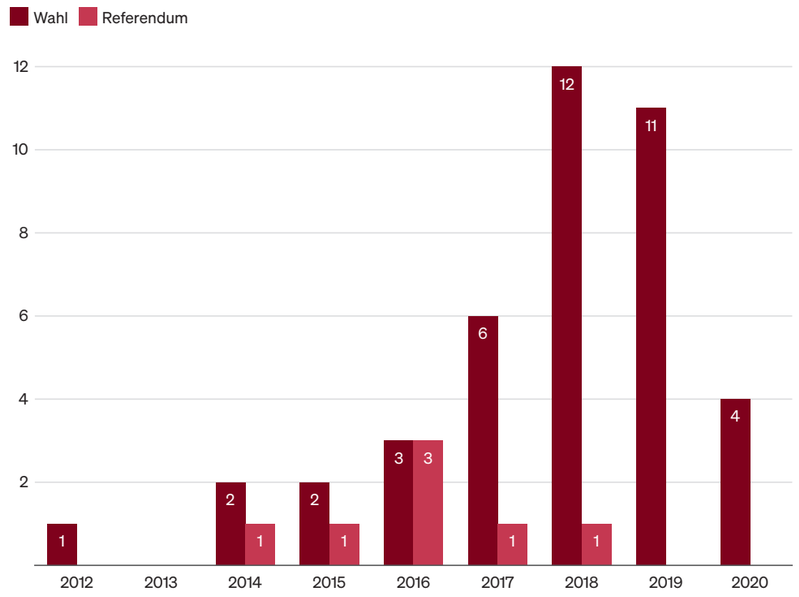
Cyberattacken, wozu im weitesten Sinne auch Desinformationskampagnen gehören, können als eine Methode hybrider Kriegsführung eingesetzt werden, wenn auch die meisten Cyberattacken nicht das Niveau erreichen, auf dem man von einer kriegerischen Handlung sprechen würde. Besteht jedoch in einem kriegerischen Konflikt eine Cyber-Komponente, so zeigen besonders Beispiele der jüngeren Vergangenheit, dass nicht notwendigerweise nur die Konfliktstaaten selbst davon betroffen sind, sondern einerseits Spillover-Effekte möglich sind (Cerulus, 2022) und andererseits auch Partnerstaaten, die eine Konfliktpartei unterstützen, ohne selbst direkt am Konflikt teilzunehmen, im Rahmen einer solchen gewaltsamen Auseinandersetzung Ziel von Cyberattacken sein können. Am Beispiel westlicher Unterstützung der Ukraine durch Waffenlieferungen ist leicht erklärbar, dass Netzwerke industrieller Produzenten von für die Ukraine wichtigen Ausrüstungsgegenständen ein lohnendes Ziel für Cyberangriffe Russlands wären. Hier überschneiden sich nun verteidigungspolitische und sicherheitspolitische Überlegungen zur Abwehr und Abschreckung von Cyberangriffen durch andere Staaten oder nichtstaatliche Akteure. Cybersicherheit ist nicht dasselbe wie Cyberdefense, doch hängen beide eng zusammen.

Verschiedene europäische Staaten machten in den letzten Jahren publik, dass es Cyberangriffe auf ihre Netzwerke gegeben hat, die offensichtlich dem Ziel dienen sollten, Wahlen zu manipulieren. Die angewandten Methoden unterscheiden sich dabei und reichen von Spear Phishing über Datendiebstahl, Malware, DDoS-Attacken bis hin zu jener Bedrohung, die am häufigsten genannt wird: über das Netz verbreitete Desinformation (ENISA, 2019:6).

Das internationale Cyber Policy Centre des Think Tanks Australian Strategic Policy Institute (ASPI) hat 41 Wahlen und sieben Referenden zwischen Jänner 2010 und Oktober 2020 identifiziert, die von Cyberattacken im weitesten Sinne (also inklusive Desinformationskampagnen, etc.) betroffen waren. Die Mehrheit dieser Attacken fand in stark digitalisierten Staaten des globalen Westens, besonders in europäischen Staaten und den USA statt. Soweit die Angreifer identifiziert wurden, zeigen die ASPI-Daten, dass die Welt, was Attacken mit einer Cyberkomponente angeht, in Cybereinflusszonen aufgeteilt ist. Die größte Bedrohung für Europa ist demnach Russland, viele asiatische Staaten – besonders Taiwan – kämpfen mit Cyberattacken, die vermutlich aus China kommen. Attacken aus dem Iran trafen die USA, Großbritannien und Israel. Die USA ist auch Ziel von China, Russland

Abbildung 7: Wahlen und Referenden werden immer häufiger Ziele von Cyberattacken

Fälle von ausländischer Einmischung mittels Cyberangriffen nach Jahr und Art des politischen Prozesses



Quelle: Australian Strategic Policy Institute

Abbildung 8: Regionale Verteilung von politisch motivierten Cyberangriffen auf Wahlen und Referenden

Quelle: Australian Strategic Policy Institute

und Nordkorea (ASPI: 13f). Eine große Rolle spielen bei den Attacken militärische Geheimdienste der Angreifer.

Wie verwundbar unterschiedliche Staaten durch Cyberangriffe auf Wahlen und Referenden sind, hängt nicht nur von ihren Cyberkapazitäten ab. Wie zu Beginn dieses Papiers erläutert, steht beim Thema Cyber der Mensch im Mittelpunkt. Wesentlich ist also das Vertrauen des Individuums in die Institutionen des Staates und in die Informationsarchitektur (staatlich und durch privat geführte Medienunternehmen). Darüber hinaus zählt auch der allgemeine Gesundheitszustand eines politischen Systems. Besonders politisch stark gespaltene Gesellschaften sind oft vulnerabler (Lim und Hansen, 2018). Darüber hinaus spielt der Digitalisierungsgrad eines Staates, wie oben erwähnt, ebenfalls eine Rolle (Conley et. al., 2020).

Während bei traditionellen kriegerischen Auseinandersetzungen trotz oftmals großen Kollateralschadens bei der Zivilgesellschaft ein großer Teil der Auseinandersetzung zwischen Militärs verfeindeter Staaten stattfand, stehen by Cyberattacken zivile Ziele im Mittelpunkt. Demokratische Prozesse, Verwaltung und alle möglichen Branchen der Wirtschaft werden direkt ins Visier genommen. Auch bei der Abwehr solcher Angriffe spielen vorwiegend nichtmilitärische Akteure die Hauptrolle. Vielmehr ist eine erfolgreiche Verteidigung kleinteilig und erfordert eine Immunisierung unterschiedlicher Akteure in einem Staat. Wirksam sind neben gesamtgesellschaftlichen Maßnahmen und militärischer Abwehr auch außenpolitische Instrumente, wenn sie effektiv eingesetzt werden.

Besonders das Thema Attribution, also öffentliche Identifikation des Angreifers, spielt dabei eine große Rolle, sowie (Cyber-)Sanktionen als Folge dieser. Die Europäische Union – außenpolitisch oft nicht der wichtige Akteur, der sie gerne wäre – könnte eine wesentliche Rolle im Kampf gegen Cyberbedrohungen in der Welt spielen. Als – zumindest auf dem Papier – auf Werten eines friedlichen Zusammenlebens und des Respekts der Rechte anderer aufgebaute Staatengemeinschaft könnte die EU weltweit als Advokat der Deeskalation im Cyberbereich auftreten. Friedliche Konfliktlösung, Dialog, Capacity Building im Defensivbereich und verschiedene Präventionsmaßnahmen könnten das Markenzeichen der Union im Cyberbereich werden. Es ist ein Reflex politischer Entscheidungsträger, auch im Cyberbereich auf Aufrüstung zum Zweck der Abschreckung zu setzen. Die Antwort der EU muss jedoch Deeskalation sein. Je mehr Schadsoftware durch digitale Aufrüstung in die Welt gerät, desto mehr davon unterliegt dem Risiko, gestohlen und von den Falschen eingesetzt zu werden. Abschreckung funktioniert im digitalen Raum nicht durch Aufrüstung, sondern durch starke Bündnisse, attraktive Standorte für IT-Fachkräfte, dadurch, dass ein Angriff durch die starken defensiven Komponenten möglichst kostspielig und zeitaufwendig gemacht wird. Das mag sich politisch nicht gut verkaufen, ist jedoch der einzige Weg, wie Europa cybersicherer werden kann.

Weiters könnte die EU Cyberkriminelle dadurch von einem Angriff abschrecken, dass sie geeint auftritt und demonstriert, dass sie bereit dazu ist, Angreifer für ihre Taten zu bestrafen bzw. die Kosten eines solchen Angriffs für die Angreifer in die Höhe zu treiben. Der erste Einsatz des EU Cyber Rapid Response Team in der Ukraine gemeinsam mit den US-Partnern war ein erster Schritt in diese Richtung (Liedekerke und Laudrain, 2022). Auch weitere Kooperation mit der NATO, die ebenfalls über 24-Stunden-Rapid-Response-Teams verfügt, ist sinnvoll.

Während sich die überwältigende Mehrheit internationaler Rechtsexperten einig ist, dass Völkerrecht auch auf den Cyberraum anwendbar ist, gibt es, falls das denn möglich ist, oft noch weniger Konsequenzen für virtuelle Rechtsbrüche. Eine Schwierigkeit dabei ist die sogenannte Attribution, also die Zuordnung eines konkreten Angriffs zu jenem Land, von dem er ausging. Das Schweigen ganzer Regierungen darüber, um wen es sich bei den Tätern handelt, hatte in der Vergangenheit mitunter unterschiedliche Gründe. Zum einen geht ein erfolgreicher Cyberangriff auf eine Regierung oder ein großes Unternehmen mit einem gewissen Gesichtsverlust einher, denn man hat sich offensichtlich nicht gut genug dagegen geschützt. Das kann für Machthaber auch politische Kosten verursachen. Firmen hingegen erleiden einen Reputationsverlust. Ein großes Datenleak zu erleiden, ist für die meisten Firmen bereits eine Tragödie. Geschieht das öfter, so liegt es für die Klienten der Firma nahe zu denken, dass ihre Daten dort nicht gut aufgehoben sind. Ein anderer Grund dafür, nach einem Angriff den Täter nicht zu benennen, der besonders die staatliche Ebene betrifft, ist, dass kein Staat einen solchen Angriff auf seine Systeme einfach unbeantwortet lassen kann. Von jenem Staat, der den Schaden hat und den Angreifer benennen kann, wird erwartet, dass er sich wehrt, sei es mittels Gegenschlag, wirtschaftlichen Sanktionen oder auf anderem Wege. Besonders Staaten, die wirtschaftliche Interessen im Angreiferland verfolgen, sind oft abgeneigt, öffentliche Schritte

gegen dieses zu setzen. Die Entwicklungen der letzten Jahre, besonders im Zusammenhang mit russischen, aber auch mit chinesischen, türkischen und iranischen Angriffen, legen nahe, dass gerade Europa beim Thema Attribution in Zukunft anders agieren könnte als bisher.

Eine weitere Möglichkeit, von Angriffen auf die Europäische Union abzuschrecken, wäre eine schnelle und koordinierte Vorgehensweise der EU, wenn es darum geht, Angreifer zu benennen (Liedekerke und Laudrain, 2022). Das betrifft nicht nur Angriffe gegen die Union selbst. Die EU könnte für sich selbst die Rolle wählen, rechtswidriges oder verantwortungsloses Verhalten im Cyberraum wie Spionage oder Sabotage oder den unverantwortlichen Export offensiver Cyberwaffen öffentlich zu benennen (ALDE 2022). Da herkömmliche Waffenexportkontrolle bei Cyberwaffen nicht möglich ist, ist die einzige Form der Kontrolle das Aufdecken solcher Exporte durch andere Stakeholder. Das Ziel muss eine Welt sein, in der sich die mächtigen Staaten selbst regulieren und mehr in Verteidigung als in Angriffswaffen investieren und gleichzeitig verwundbarere Staaten beim Aufbau einer effektiven Cyberabwehr hilft.

Europa verfügt über ein Cybersanktionenregime, das sich insofern als sehr dynamisch erwiesen hat, als dass es bereits kurz nach seiner Einrichtung genutzt wurde. Verbesserungen können hier bei der Treffsicherheit gemacht werden. Cybersanktionen zielen auf Reisefreiheit und in der EU existierende Vermögenswerte potenzieller Angreifer ab, doch handelt es sich bei Angreifern vielfach um Personen, die weder Vermögen in der EU haben noch in die EU einreisen wollen.

Der Strategische Kompass (Council of the European Union, 2022), den die Europäische Union im Frühling 2022 beschlossen hat, hat das Ziel, die EU stärker und widerstandsfähiger zu machen, damit sie ihre Bürger besser schützen und auf der internationalen Bühne glaubwürdig für Frieden und Sicherheit eintreten kann. Der Strategische Kompass soll jene Roadmap sein, die die Union in die strategische Autonomie führt. Darin ist auch die enge Zusammenarbeit mit Partnern, die die europäischen Werte teilen, vorgesehen. Möglicherweise wird die EU aber gerade beim Thema Cybersecurity/Cyberdefense auch mit Ländern zusammenarbeiten müssen, die ihre Werte nicht teilen, aber dafür ein gemeinsames Sicherheitsinteresse mit Europa haben. Möglicherweise wird das nur durch Ad-hoc-Kooperationen möglich sein und nicht, wie bisher gewohnt, multilaterale Praxis durch den Abschluss von internationalen Verträgen.

Empfehlungen

- Am effektivsten ist die Union, wie man auch am Vorgehen gegen Russland seit der Invasion der Ukraine erkennen kann, wenn sie geeint und entschlossen auftritt. Damit das im Bereich der Cyberabwehr möglich ist, gibt es einige Punkte, bei denen die Mitgliedstaaten schnell eine Einigung herbeiführen müssen. Einer davon ist, dass die Union eine gemeinsame Vorgehensweise beim Thema Exploits bzw. Zero Days haben sollte. Exploits, mit denen auf digitalen Schwarzmarkt gehandelt wird, sind eine gefährliche offensive Cyberwaffe. Die Europäische Union sollte sich selbst gemeinsame Regeln darüber geben, ob Regierungen Exploits kaufen und diese auch nutzen dürfen oder nicht. Hinzu kommt, dass mindestens zwei EU-Staaten öffentlich angeben, offensive Cyberwaffen zu entwickeln. Eine Art „unionsinterne" gegenseitige Kontrolle verhindert Willkür und schafft Vertrauen zwischen den Staaten.
- Um einen Weiterverkauf von Exploits unter Cyberkriminellen einzudämmen, sollte die EU finanzielle Anreize dafür bieten, Exploits zu finden und den betroffenen Betreibern zu melden, bevor sie von Angreifern erworben und für einen Angriff genutzt werden können. Diese Maßnahme ist auch auf Mitgliedstaaten-Ebene implementierbar, falls sich kein Konsens auf EU-Ebene finden lässt.
- Eine Union ohne offensive Cyberwaffen wird es nicht geben, diese existieren bereits in manchen Ländern. Im Geiste einer deeskalierenden, friedens-stiftenden und allgemein sicherheitsfördernden Politik sollten sich die EU-Staaten zum Ziel setzen, offensive Operationen nur dazu durchzuführen, einen Gegner davon abzuhalten, eine Attacke gegen die EU oder einen Mitgliedstaat auszuführen.
- Gleichzeitig gilt es gegenüber größeren Partnern wie den Five-Eyes-Staaten selbstbewusst aufzutreten. Europa sollte die einzige Macht sein, die bestimmt, unter welchen Bedingungen es Partnerstaaten außerhalb der EU erlaubt ist, in europäischen Netzwerken operativ tätig zu sein. Es braucht einen Standardprozess inklusive Prior Notificiation zwischen Europa und seinen Partnern, damit ein solcher Eingriff in den souveränen digitalen Raum eines Staates – sei er gerechtfertigt oder nicht – geordnet abläuft und nicht vom Recht des Stärkeren bestimmt wird.

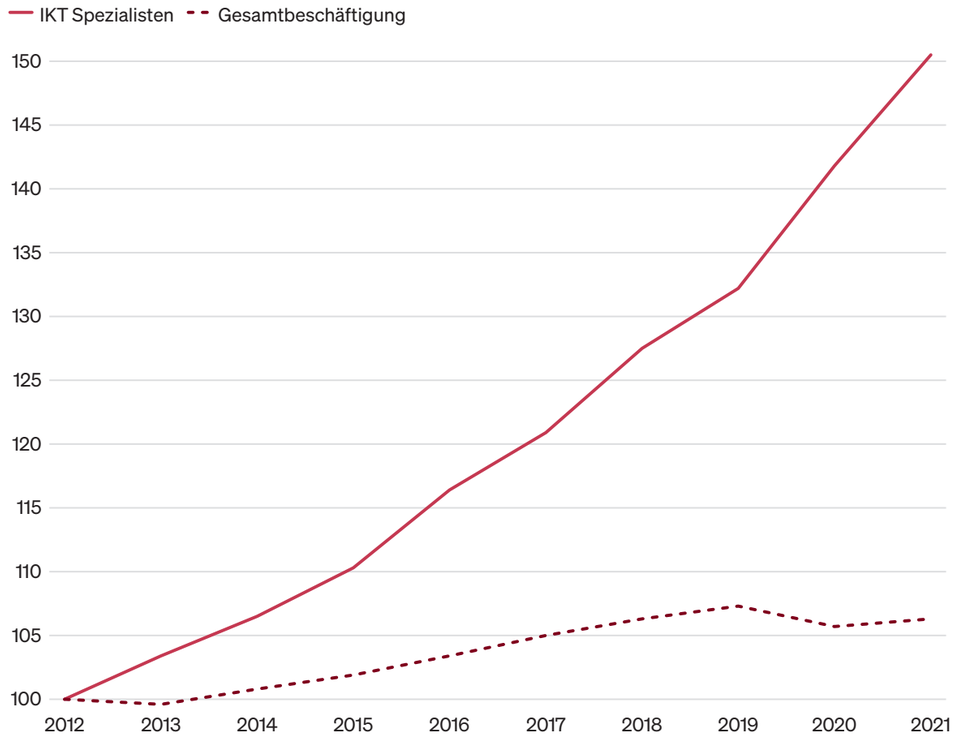
2.3 Skills und Fachkräfte

Bei Wachstumsraten von meist über 10 Prozent und einem europäischen Markt von über 36 Milliarden Euro gehört der Cybersecurity-Sektor zu den am stärksten wachsenden Märkten (Statista 2022a, b). Dies bedeutet auch, dass ein entsprechendes Arbeitskräftepotenzial notwendig ist, um den Bedarf an Sicherheitslösungen zu decken. Hierbei zeigen sich viele Parallelen mit dem Fachkräfteangebot bzw. -mangel im Internet- und Telekommunikationssektor (IKT). Dieser ist in den letzten Jahren massiv gewachsen. Zwischen 2012 und 2021 ist der Anteil an IKT-Spezialisten in Europa um über 50 Prozent gewachsen, während das gesamte Arbeitskräfteangebot im gleichen Zeitraum um 6,3 Prozent gestiegen ist, womit in der Europäischen Union mittlerweile fast 9 Millionen Menschen im IKT-Sektor arbeiten (Eurostat 2022).

Einer Analyse von ENISA (2020b) zufolge sind ca. 13 Prozent aller IKT-Jobs im Cybersecurity-Bereich, womit gemäß Eurostat-Daten davon ausgegangen werden kann, dass knapp eine Million Jobs innerhalb der EU mit Cybersecurity zu tun haben. Gleichzeitig ist der IKT-Bereich derjenige, in dem Fachkräfte in ganz Europa besonders schwierig zu bekommen sind. Gemäß Erhebungen von Eurostat (2022b) haben 55 Prozent aller Unternehmen Probleme dabei, geeignete IKT-Spezialist:innen anzustellen. Das trifft insbesondere in Tschechien (76 Prozent), Österreich (74 Prozent) und den Niederlanden (71 Prozent) zu.

Abbildung 9: Massiver Anstieg der IKT-Beschäftigten im Vergleich zur Gesamtbeschäftigung

Relative Entwicklung der Beschäftigung, 2012=100



Quelle: Eurostat

Abbildung 10: In vielen Teilen Europas herrscht starker IKT-Fachkräftemangel

Anteil an Unternehmen die Schwierigkeiten bei der Besetzung freier IKT Stellen haben

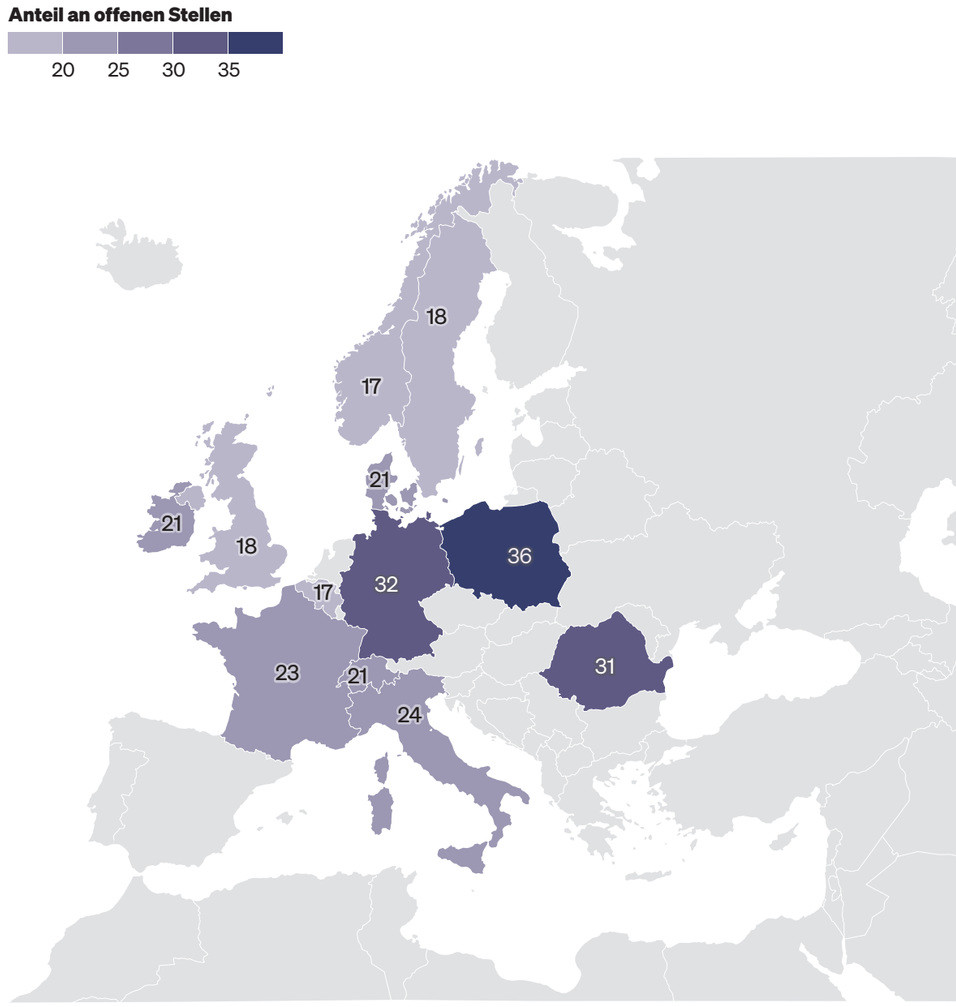
Land	Prozent
Tschechien	76
Österreich	74
Niederlande	71
Slowenien	69
Kroatien	68
Luxemburg	67
Deutschland	66
Malta	66
Rumänien	66
Estland	60
Belgien	59
Litauen	59
Slowakei	59
Finnland	59
Dänemark	58
Frankreich	58
Ungarn	57
Italien	55
Schweden	55
Irland	53
Lettland	48
Portugal	44
Polen	43
Zypern	41
Bulgarien	36
Griechenland	35
Spanien	24

Quelle: Eurostat

Betrachtet man die Zahlen mit Augenmerk auf Unternehmensgrößen, haben insbesondere Klein- und Mittelbetriebe Schwierigkeiten dabei, Positionen zu besetzen (Eurostat 2022b). Diese Probleme finden sich auch im Cybersecurity-Sektor. Basierend auf einer Analyse von Linkedin-Daten in zwölf EU-Mitgliedstaaten prognostiziert Microsoft für diese Länder über 60.000 offene Stellen. Verschärft wird die Situation dadurch, dass innerhalb eines Jahres (2021 auf 2022) der Bedarf an Cybersecurity Skills um 22 Prozent gestiegen ist (Microsoft 2022).

Abbildung 11: Viele offene Cybersecurity Stellen in ganz Europa

Analyse von nicht besetzten Stellen auf LinkedIn



Quelle: Microsoft & LinkedIn

Die European Cyber Security Organisation ESCO (2022) geht davon aus, dass in der gesamten Europäischen Union bis zu 500.000 Fachkräfte fehlen. Dass dies kein europäisches Problem ist, zeigen internationale Erhebungen, die davon ausgehen, dass auch weltweit bis zu 3,5 Millionen Stellen offen sind, die Schere zwischen offenen Stellen und Arbeitskräften um 13 Prozent gestiegen ist und das Arbeitskräftepotenzial in den kommenden Jahren um 80 Prozent steigen müsste, um den aktuellen Bedarf zu decken (Gamal, N., Martino, L., Nestoras, A. 2022).

Auf europäischer Ebene wird diesem Fachkräftemangel massiv entgegengewirkt. Seit Jahren arbeitet ENISA an Programmen zur Stärkung des Bewusstseins für Cybersecurity-Maßnahmen und an Ausbildungsprogrammen für Cybersecurity-Spezialist:innen (ENISA 2020b, 2021d). Die EU-Cybersecurity-Strategie 2020 legt einen wesentlichen Fokus auf Forschung und Ausbildung im Cybersecurity-Bereich und hat im Rahmen des „Digital Europe Programme to Advance on the Digital Transition" 2 Milliarden Euro zur Verfügung gestellt (Europäische Kommission 2021, Gamal, N., Martino, L., Nestoras, A. 2022). Dies hat dazu geführt, dass sich ENISA (2021e) zufolge die Anzahl an universitär ausgebildeten Spezialist:innen in den kommenden Jahren verdoppeln wird.

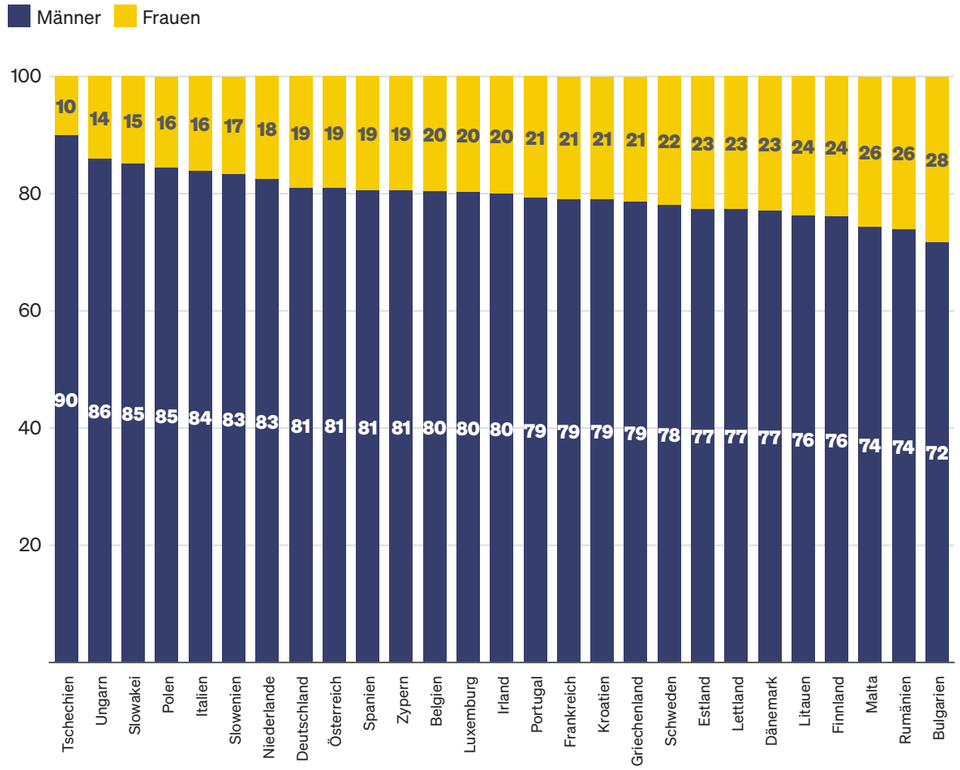
Auch wenn ein Fortschritt zu erkennen ist, deckt dies bei weitem nicht die Anzahl an benötigten Fachkräften ab. Die Gründe für den Arbeitskräftemangel sind vielfältig, jedoch sticht ein Aspekt besonders heraus: die ungleiche Verteilung von Männern und Frauen auf den IKT- und Cybersecurity-Sektor im Vergleich zu anderen Branchen. Gemäß Eurostat (2022) sind über 80 Prozent aller IKT-Arbeitskräfte Männer.

Im Cybersecurity-Sektor gehen Analysen davon aus, dass sich in den letzten fünf Jahren der Anteil an Cybersecurity-Beschäftigten innerhalb des IKT-Sektors von 11 auf 25 Prozent mehr als verdoppelt hat (Gamal, N., Martino, L., Nestoras, A. 2022). Gemäß diesen Analysen ist das Defizit in Europa besonders hoch, da nur 11 Prozent aller Stellen mit Frauen besetzt sind. Zu ähnlichen Ergebnissen kommt auch Microsoft (2022). In den untersuchten Ländern lag der Frauenanteil zwischen 13 (Polen) und 25 Prozent (Italien). Dem steigenden Bedarf an Fachkräften kann daher nur begegnet werden, wenn der Frauenanteil massiv gesteigert wird. Dies ist umso dringender, da durch den russischen Angriffskrieg Cyberattacken in Europa signifikant angestiegen sind (Gamal, N., Martino, L., Nestoras, A. 2022).

Neben dem Gender-Gap ist die zweite große Baustelle im Fachkräftebereich die Aus- und Fortbildung und damit im Zusammenhang stehende Curricula und Zertifizierungsschemata. Die ENISA Higher Education Database (ENISA 2022) ist die größte verifizierte Datenbank von akademischen Ausbildungslehrgängen im europäischen Raum. Stand September 2022 können 124 Programme in 25 EU-Mitgliedstaaten absolviert werden. Hierbei gibt es zwei sofort offensichtliche Probleme: Erstens ist eine ungleiche Verteilung zwischen den EU-Mitgliedstaaten ersichtlich. Während in Deutschland mit über 80 Millionen Einwohnern nur zwei Lehrgänge zu finden sind, finden sich in Spanien 23. Mit zehn Lehrgängen hat Österreich in etwa ein gleich großes Angebot

Abbildung 12: Großer Gender Gap im IKT Bereich

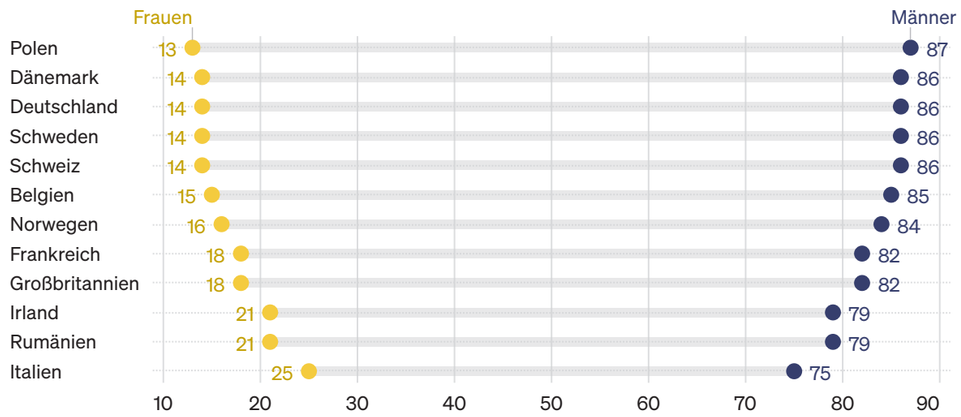
Verteilung der IKT-Beschäftigten nach Geschlecht, 2021



Quelle: Eurostat

Abbildung 13: Anteil an Frauen im Cybersecurity Sektor

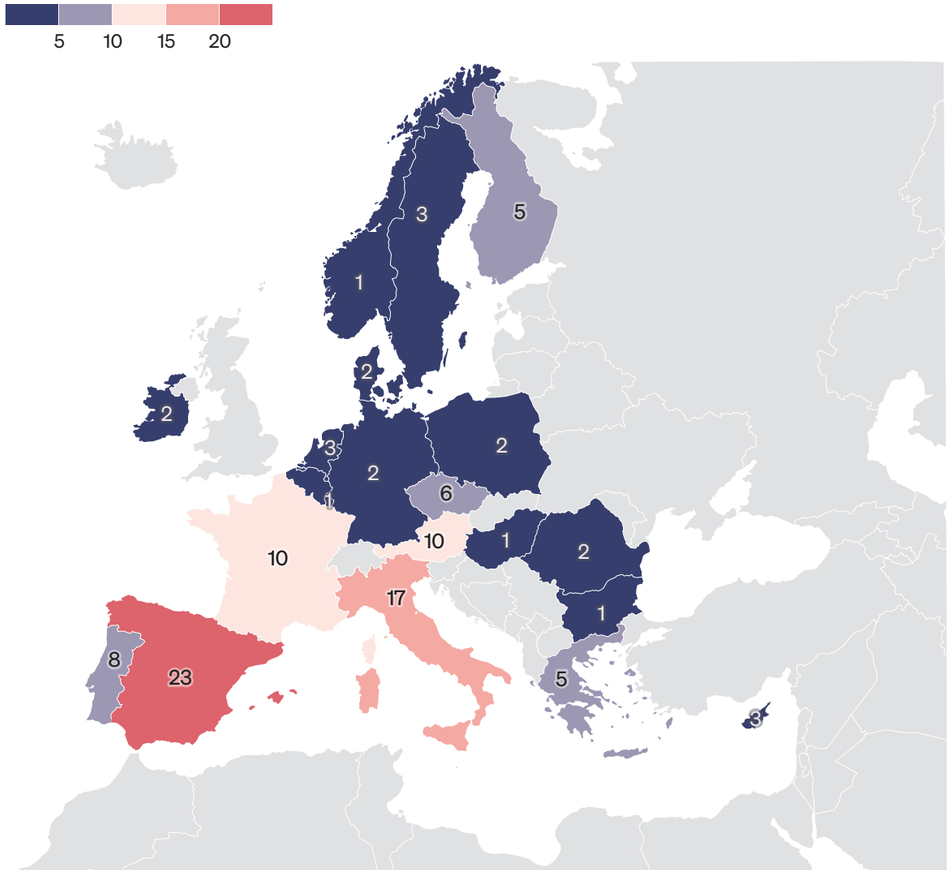
Verteilung der Cybersecurity-Beschäftigten nach Geschlecht



Quelle: Microsoft & LinkedIn

wie alle nordischen Länder zusammen. Zweitens machen den Großteil der Studiengänge Spezialisierungen im Rahmen eines Masterstudiums aus. Vier von fünf Programmen sind Masterstudiengänge, während es EU-weit nur 20 Bachelorprogramme gibt. Insbesondere für einen schnellen Berufseinstig ist dies ein Problem. Hinzu kommt, dass es keine Mindeststandards für Curricula gibt (Gamal, N., Martino, L., Nestoras, A. 2022, ENISA 2020b, 2021e).

Abbildung 14: Anzahl an Cybersecurity Studienprogrammen in Europa



Quelle: ENISA

Die fehlenden Mindeststandards beschränken sich jedoch nicht auf den universitären Bereich. Ebenso gibt es in der Europäischen Union keine standardisierten und zertifizieren Berufsbilder (Gamal, N., Martino, L., Nestoras, A. 2022, ENISA 2020b, Blažič 2021). Dies ist jedoch zentral, um langfristig den Fachkräftebedarf in Europa zu sichern. Jeder Beruf kann in Arbeitstätigkeiten aufgeteilt werden. Damit eine Arbeitstätigkeit erfolgreich ausgeführt werden kann, werden bestimmte Fähigkeiten benötigt (Eder/Feierabend 2017, Blažič 2021). Kompetenz und Rollenprofile helfen dabei, wesentliche Berufe in Arbeitsfelder zu definieren und zu vereinheitlichen, welche Arbeitstätigkeiten und Fähigkeiten für den jeweiligen Beruf notwendig sind (Blažič 2021).

In den Vereinigten Staaten werden Kompetenz und Rollenprofile in der NICE-Initiative festgelegt. NICE definiert sieben spezifische Spezialgebiete, und jedem Rollenprofil werden mindestens zwei Spezialgebiete zugeordnet. Anschließend werden für jedes Arbeitsprofil in allen Kategorien Arbeitstätigkeiten definiert und die damit erforderlichen Fähigkeiten festgeschrieben (Blažič 2021). Das NICE-Schema vereinfacht die Suche nach Mitarbeitern in den USA und ermöglicht eine granulare Darstellung von bestehenden und fehlenden Kompetenzen. Wie sowohl von ENISA (2020b) und einer Vielzahl an anderen Institutionen und Publikationen (Gamal, N., Martino, L., Nestoras, A. 2022) festgestellt wird, ist das Fehlen eines europäischen NICE-Äquivalents eine der wesentlichsten strukturellen Hürden für die Beseitigung des Fachkräftemangels in der EU. Basis für ein europaweites Schema könnten bisherige freiwillige Zertifizierungsschemata wie die von ENISA in Arbeit befindliche „NIS driving licence" oder die Ergebnisse eines Pilotprojekts des CCN-Netzwerks sein (Blažič 2021).

Hierbei gilt es zu berücksichtigen, dass Rollenprofile nicht nur aus technischen Fähigkeiten bestehen. Martin und Collier (2019) argumentieren, dass ein inter-disziplinärer Ansatz, der über technische Fähigkeiten hinausgeht, zu bevorzugen ist, da dies ein besseres Verständnis der Cybersicherheitsherausforderungen ermöglicht. Ähnlich argumentieren Dawson und Thomson (2018) und stellen fest, dass für die komplexen Herausforderungen im Cyberbereich eine stärkere Berücksichtigung von sozialen Aspekten nötig ist. Sie definieren Fähigkeiten, die für Cybersecurity-Fachkräfte von besonderer Relevanz sind: systematisches Denken, gute Kommunikation, Fähigkeit zur Zusammenarbeit, kontinuierliches Lernen und ein Mindestmaß an Wissen über Grundrechte und demokratische Werte. Dies würde es auch ermöglichen, einen bisher oft vernachlässigten Bereich in der Fachkräftediskussion zu stärken: die Erwachsenenbildung. Im Gegensatz zum Cybersecurity-Bereich besitzt Europa mit dem European Qualification Framework (CEDEFOP 2022) ein ausgezeichnetes Programm zur Definition von Lernzielen, Kenntnissen, Fähigkeiten und nicht zuletzt einer Vergleichbarkeit von Aus- und Fortbildungen. Hier gilt es anzusetzen und auf Basis eines europäischen NICE-Äquivalents maßgeschneiderte Fortbildungsprogramme zu definieren. Gerade angesichts des evidenten Fachkräftemangels wäre es für europäische Unternehmen eine Erleichterung, wenn bestehendes Personal bestimmte Arbeitstätigkeiten übernehmen könnte.

Eine der bisher größten Stärken in Europa wird hierbei noch gar nicht genutzt:

die Lehrlingsausbildung. In vielen Staaten ist sie ein wesentlicher Baustein für die Wirtschafts- und Arbeitsmarktpolitik. Während viele IKT-Berufsfelder Lehrlingsausbildungen haben, fehlen diese im Cybersecurity-Bereich. Länder wie Deutschland oder Österreich, in denen es eine lange Tradition der dualen Ausbildung gibt, könnten hier im Rahmen von Pilotprojekten entsprechende Ausbildungen entwickeln. Auch in der formellen Schulbildung kann angesetzt werden. Österreich beispielsweise besitzt mit Höheren Technischen Lehranstalten (HTL) einen weiterführenden Schultyp mit technischen Ausbildungsschwerpunkten. Dies ermöglicht die Festsetzung von Fähigkeiten schon in der Schulbildung.

Empfehlungen

Das massive Wachstum der Cybersecurity-Branche führt zu ähnlichen Problemen, wie sie der gesamte IKT-Sektor kennt: ein immer größer werdender Fachkräftemangel, Diversitätsprobleme und oft zu schwache politische Gegensteuerung. Auch wenn die Anzahl an verfügbaren Fachkräften steigt, sind folgende Maßnahmen unerlässlich:

- Auf universitärer Ebene sind EU-weite Mindeststandards für Curricula festzulegen. Ebenso muss die Anzahl an Bachelorprogrammen und akademischen berufsbegleitenden Fortbildungsmaßnahmen ausgebaut werden.
- Der massive Gender-Gap muss verringert werden. Dies kann unter anderem mit einer Koppelung von Fördergeldern mit Diversitäts-maßnahmen, einen Ausbau von bewusstseinsfördernden Maßnahmen oder Praktika erfolgen.
- Schwachstellen im Zertifizierungsbereich sind zu beheben. Ähnlich der NICE-Initiative für die USA ist eine Standardisierung von Berufen, ihren Arbeitstätigkeiten und den dazugehörigen Fähigkeiten nötig.
- Eine reine Akademisierung wird das Fachkräfteproblem nicht lösen. Deshalb muss die Erwachsenenbildung gestärkt werden, indem spezifische Fortbildungen für bereits im Berufsleben stehende Personen etabliert werden. Wenn hierdurch bestimmte Arbeitstätigkeiten über-nommen werden können, entlastet dies die europäischen Unternehmen.
- In Ländern mit einer starken Tradition von Lehrberufen sollten Pilotprojekte gestartet werden, um innerhalb des Cybersecurity-Bereichs Lehrberufe einzuführen. In den EU-Mitgliedstaaten können in der formellen Schulbildung Cybersecurity-Fähigkeiten vermittelt werden.

2.4 Cyberwirtschaft und Cybersicherheit von KMU

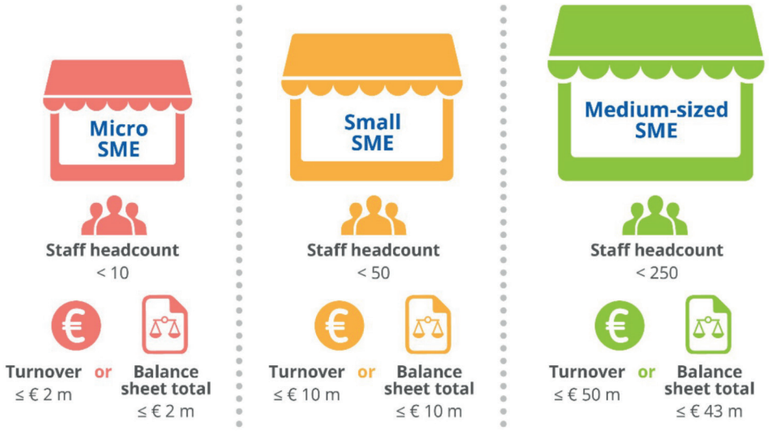
Die Europäische Union ist der größte Binnenmarkt der Welt und eine wirtschaftspolitische Supermacht. Umso zentraler ist es, Cyberattacken als eine der größten Bedrohungen abzuwehren und eine Cybersicherheitsinfrastruktur zu bilden, die auch in Zukunft die wirtschaftliche Prosperität des Kontinents sichert. Kaum eine Branche weist solche Wachstumsraten auf wie der IT-Sektor.

Neue Technologien wie Mobile oder Cloud Computing revolutionieren nicht nur die IT-Märkte, sie stellen auch Herausforderungen für die Cybersicherheit dar. Schätzungen von ENISA (2016) gehen davon aus, dass mangelnde Cybersicherheit die EU bei großangelegten koordinierten Angriffen, beispielsweise auf Smart Grids die zu europaweiten Blackouts führen würden, im Erfolgsfall bis zu 640 Milliarden Euro kosten kann. Sicherheitsbedenken spielen angesichts der vorherrschenden Cyberbedrohungen eine zentrale Rolle in Politik, Verwaltung und Wirtschaft. Können diese nicht durch eine adäquate Infrastruktur und geschultes Personal aufgelöst werden, verlangsamt sich die Einführung innovativer Technologien in Europa noch stärker, was europäische Unternehmen daran hindert, Innovationen optimal zu nutzen, um ihre wirtschaftliche Effizienz zu steigern und global wettbewerbsfähig zu werden.

Der EU-Cybersicherheitsmarkt selbst ist mit 36,3 Milliarden Euro ein zentraler Wirtschaftsfaktor, wobei Sicherheitsdienstleistungen mit 21,1 Milliarden den größten Anteil ausmachen, und ist im Vergleich zum Cybersicherheitsmarkt anderer Regionen auf der Welt günstig. Gleichzeitig ist die jährliche Wachstumsrate in Europa geringer als in anderen Regionen, insbesondere geringer als in den Vereinigten Staaten (Statista 2022a, ENISA 2016). Das schwächere Wachstum lässt sich nur durch geringere Ausgaben für Klein- und Mittelbetriebe erklären, da die größeren europäischen Firmen ähnlich hohe Summen für Cybersicherheit ausgeben wie große Firmen aus anderen Weltregionen (ENISA 2016). Viele Standards und Vorgaben gelten jedoch nur für „kritische Infrastruktur" und Großunternehmen. Auch die derzeit in Verhandlung stehende NIS-2-Direktive nimmt KMU aus ihrem Regelwerk aus. Umso wichtiger ist es, durch den Ausbau von Wissen und der Verbreitung von IKT-Sicherheitsstandards die Sicherheit von Klein- und Mittelbetrieben zu gewährleisten. KMU bilden das Rückgrat der europäischen Wirtschaft. Daten der Europäischen Kommission zufolge sind 99 Prozent aller Unternehmen in der EU Klein- oder Mittelbetriebe. Sie beschäftigen europaweit rund 100 Millionen Menschen und erwirtschaften mehr als die Hälfte

des europäischen Bruttoinlandsprodukts (Europäische Kommission 2022b). Mit 93 Prozent sind sogenannte „Micro KMU", also Unternehmen mit weniger als zehn Beschäftigten die vorherrschende Unternehmensgröße.

Abbildung 15: KMU-Definitionen



Quelle: ENISA (2021)

Weit ist die Wahrnehmung verbreitet, dass Cyberangriffe nur auf große Organisationen erfolgen, möglicherweise weil es dort scheinbar am meisten zu holen gibt. Dies ist jedoch nicht korrekt. Organisationen können unabhängig von ihrer Größe auf ähnliche Weise angegriffen werden. KMU sind oft sogar noch gefährdeter, denn bei ihnen lassen sich insbesondere durch Ransomeware bei verhältnismäßig geringem Aufwand hohe Profite erzielen (ENISA 2021b). Statistisch gesehen geben Großunternehmen häufiger an, Cyberangriffen ausgesetzt zu sein. Erfolgreiche Angriffe, die zu Datenlecks führen, finden jedoch oftmals in Klein- und Mittelbetrieben statt, wie Accentures neunte „Annual Cost of Cybercrime"-Studie (Accenture 2019) zeigt. Hinzu kommt, dass etwa in Deutschland durch eine Medienrecherche kürzlich öffentlich wirksam klar geworden ist, dass es auch aufseiten der Behörden – Konkret bei der Polizei – eklatante Mängel bei der Ausbildung jener Beamten gibt, die für die Aufnahme von Cyber Crimes zuständig wären. Cyberbedrohungen sind heute auch für Klein- und Mittelbetriebe zu einem anerkannten Geschäftsrisiko geworden. Laut einer repräsentativen europaweiten Befragung von Klein- und Mittelbetrieben gaben 41 Prozent der Befragten an, schon einmal Opfer von Phishing-Mails geworden zu sein, auch webbasierte Angriffe und Malware sind oft eingesetzte Angriffswerkzeuge gegen KMU.

Abbildung 16: Verteilung von Cybersicherheitsvorfällen basierend auf ihrer Herkunft

Quelle: ENISA (2021)

Erfolgreiche Angriffe erfolgen auch auf Basis von schwachen Passwörtern (für 56 Prozent aller erfolgreichen Angriffe auf KMU war dies ein Erfolgsfaktor) oder unversperrte Geräte (44 Prozent). Dies zeigt, dass es oftmals nicht komplexe technische Probleme sind, die zu Sicherheitsdurchbrüchen führen. Grundsätzlich hat die IKT-Sicherheit einen hohen Stellenwert in den europäischen Unternehmen. Eurostat hat sieben IKT-Sicherheitsmaßnahmen wie beispielsweise Authentifizierungen mit starkem Kennwort oder Datensicherung an einem separaten Speicherort abgefragt. 92 Prozent aller Firmen nutzen mindestens eine der abgefragten Sicherheitsmaßnahmen (Eurostat 2022c). Oftmals werden Sicherheitsprozesse jedoch weder dokumentiert (nur ein Drittel aller Unternehmen tut dies) noch werden die Sicherheitsabläufe regelmäßig evaluiert.

Dies trifft grundsätzlich auch auf Klein- und Mittelbetriebe zu. In einer von ENISA in Auftrag gegebenen Umfrage unter Klein- und Mittelbetrieben in Europa gaben über 70 Prozent der Unternehmen an, Backups anzufertigen, ein Antivirenprogramm installiert zu haben oder regelmäßig die verwendete Software upzudaten. (ENISA 2021b). Andere Sicherheitspraktiken, wie einen Security Officer oder Pläne zur Verwendung von mobilen Datenträgern, sind jedoch nicht weit verbreitet. Weniger als 30 Prozent gaben an, davon Gebrauch zu machen.

Tabelle 5: IKT Sicherheit in Europas Unternehmen

	Mindestens eine IKT-Sicherheitsmaßnahme verwendet	Dokumente zu Maßnahmen, Praktiken oder Verfahren zur IKT-Sicherheit	Die IKT Sicherheitsdokumente wurden innerhalb der letzten 12 Monate definiert oder überprüft
EU-27	92	33	24
Belgien	94	34	27
Bulgarien	85	18	13
Tschechien	94	32	26
Dänemark	97	56	42
Deutschland	97	37	27
Estland	86	27	18
Irland	93	54	42
Griechenland	74	15	10
Spanien	92	33	25
Frankreich	94	26	18
Kroatien	90	41	25
Italien	93	34	28
Zypern	83	32	24
Lettland	98	42	25
Litauen	93	36	22
Luxemburg	93	27	22
Ungarn	86	17	13
Malta	92	32	25
Niederlande	96	42	32
Österreich	91	36	28
Polen	87	23	18
Portugal	98	28	21
Rumänien	73	17	11
Slowenien	84	35	26
Slowakei	90	28	22
Finnland	97	44	35
Schweden	95	52	39

Quelle: Eurostat

Tabelle 6: Viele Standards der CYbersicherheit werden in Klein- und Mittelbetrieben nicht verwendet

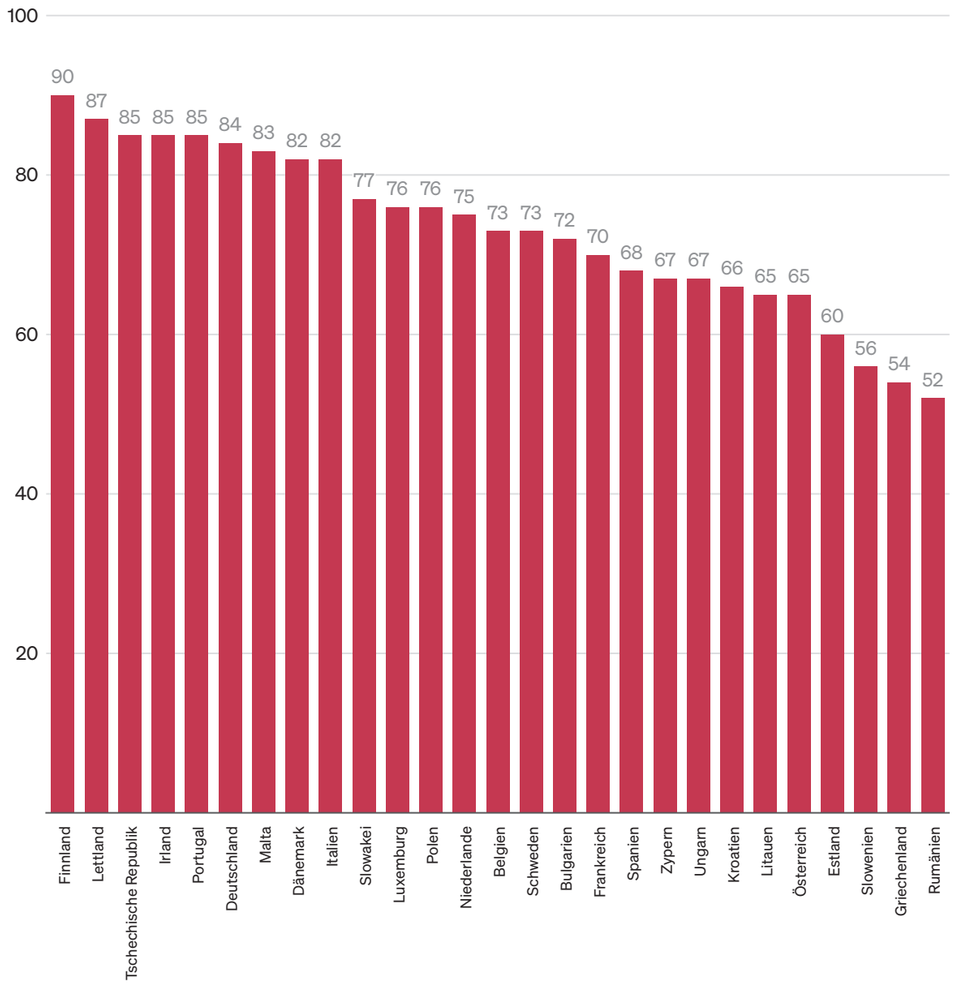
Weniger als 30% der KMU	Mehr als 70% der KMU
Security Officer im Unternehmen	Regelmäßige Backups
Pläne zur Verwendung von Mobilen Datenträgern	Anti-Viren-Programm installiert
Reaktionspläne für Cybersecurity Vorfälle	Firewall
Information Security Management System	Regelmäßige Softwareupdates
Pläne zur Schadensbehebung im Angriffsfall	
Regelmäßige Cyberinformationen für Beschäftigte	

Quelle: ENISA

Schwache Passwörter sind zwar oftmals ein wesentlicher Schlüssel für erfolgreiche Cyberangriffe, doch 76 Prozent aller europäischen Klein- und Mittelbetriebe haben Authentifizierungssysteme, die starke Kennwörter verlangen. Gleichzeitig gibt es deutliche Unterschiede zwischen den Betrieben innerhalb der Europäischen Union. Während neun von zehn finnischen KMU diesen Standard implementiert haben, trifft dies in Griechenland (54 Prozent) und Rumänien (52 Prozent) nur auf knapp die Hälfte aller Klein- und Mittelbetriebe zu.

Abbildung 17: Klein- und Mittelbetriebe mit sicheren Passwörtern

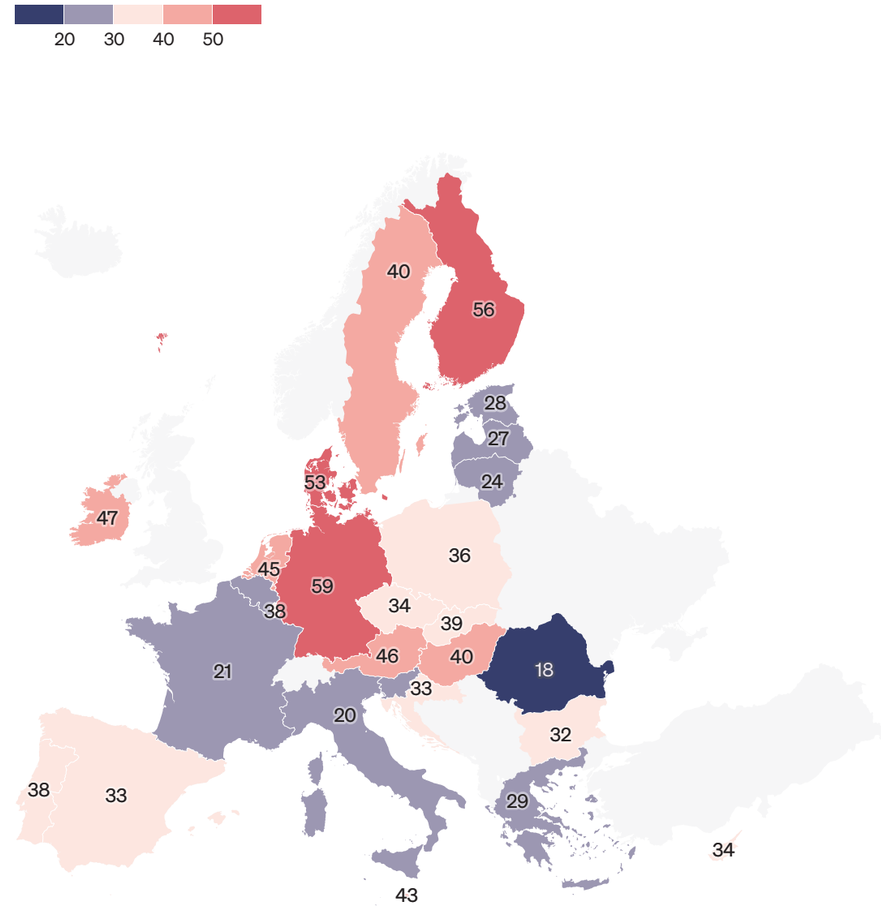
Anteil an Klein- und Mittelbetrieben die angeben, dass in ihren Unternehmen Standards für sichere Passwörter verwendet werden



Quelle: ENISA

Deutlich seltener werden von Klein- und Mittelbetrieben Verschlüsselungstechniken von Daten und Mails verwendet, eine mittlerweile gängige Praxis, um Daten und sensible Informationen zu schützen. Nur 37 Prozent aller KMU nutzen dies, wobei auch hier signifikante Unterschiede innerhalb der Europäischen Union feststellbar sind. Während in Deutschland (59 Prozent), Finnland (56 Prozent) oder Dänemark (53 Prozent) eine Mehrheit der KMU Verschlüsselung verwendet, trifft dies nur auf jedes fünfte Unternehmen aus Frankreich oder Italien zu.

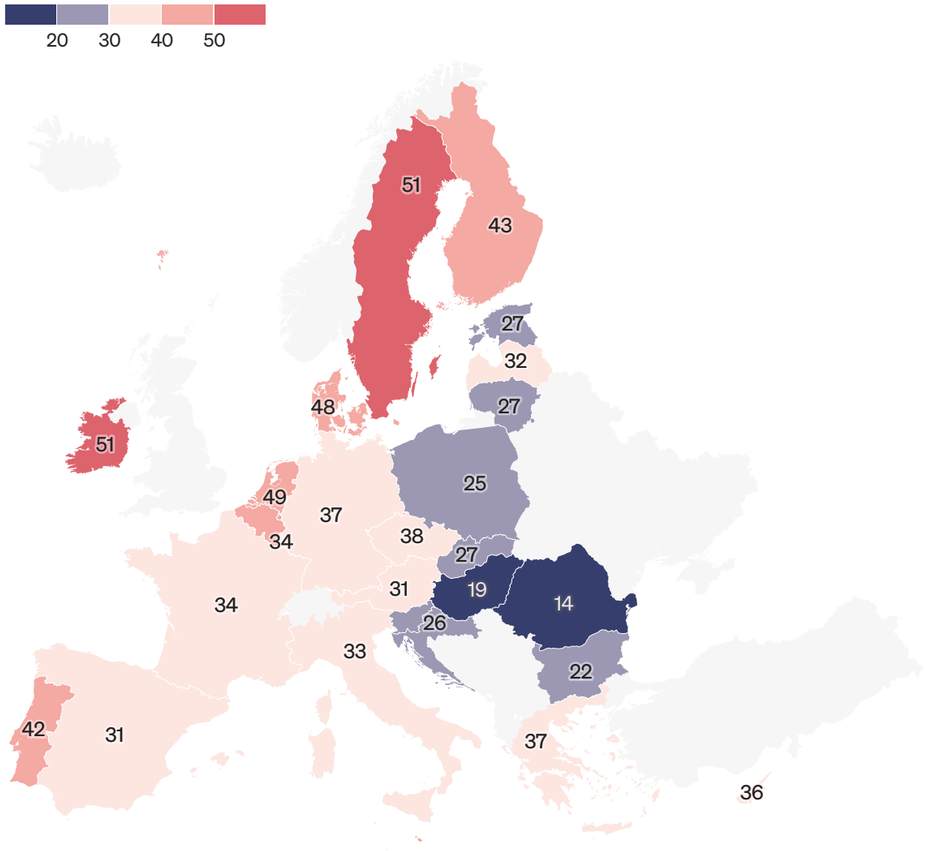
Abbildung 18: KMU die Verschlüsselungstechniken für Daten, Dokumente oder Mails verwenden



Quelle: Eurostat

Neben Softwarelösungen sind Sicherheitsabläufe und -tests, beispielsweise Performing Penetration Tests oder ein Test von Backup-Systemen, von zentraler Bedeutung. Ähnlich wie bei den Verschlüsselungstechniken gibt es hier für Klein- und Mittelbetriebe in ganz Europa Aufholbedarf. Nur knapp jedes dritte KMU führt regelmäßig Sicherheitstests durch. Diese sind in Schweden (51 Prozent), den Niederlanden (49 Prozent) und Dänemark (48 Prozent) weit verbreitet, während KMU in Bulgarien (22 Prozent), Ungarn (19 Prozent) und Rumänien (14 Prozent) diese kaum durchführen.

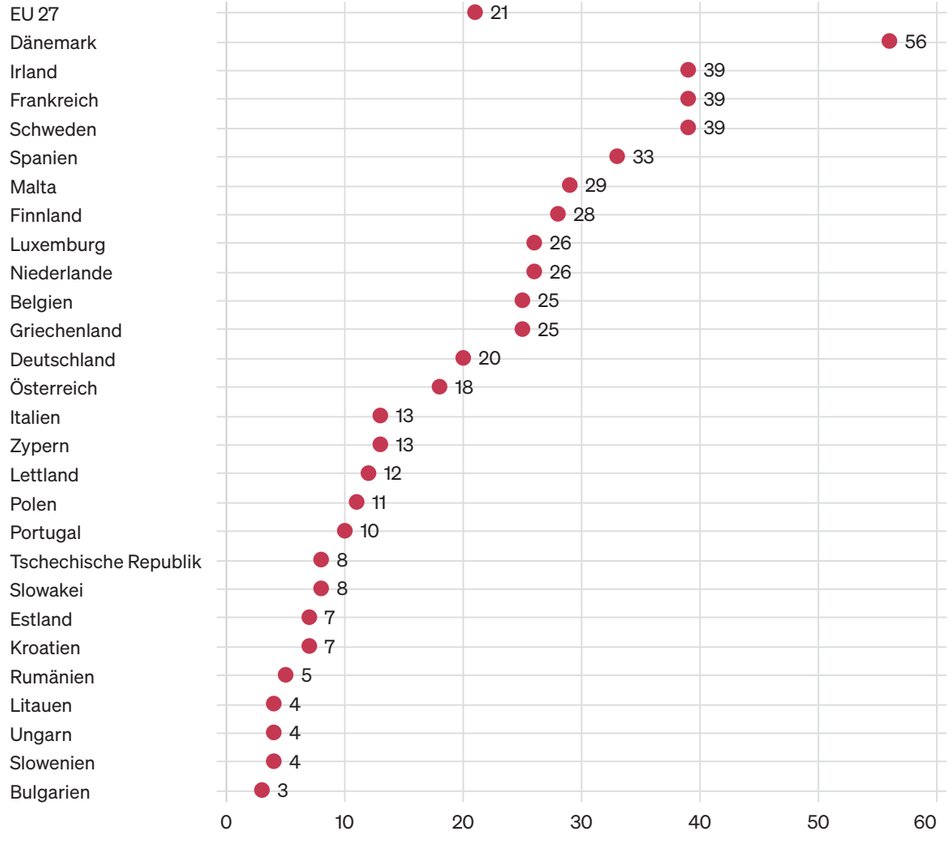
Abbildung 19: KMU die Security Tests durchführen



Quelle: Eurostat

Angesichts der hohen Kosten im Schadensfall (siehe Kapitel 2.1) und der Häufigkeit, mit der Unternehmen Cyberangriffen ausgesetzt sind, werden Versicherungslösungen für IKT-Schadensfälle immer relevanter. Eurostat-Daten zeigen jedoch, dass im gesamten Euroraum nur jedes fünfte Unternehmen eine derartige Versicherung aufweist. Einzig in Dänemark (56 Prozent), Irland (54 Prozent) und Schweden (52 Prozent) haben eine Mehrheit der Unternehmen eine entsprechende Versicherung. In 13 EU-Staaten hat jedoch nicht einmal jedes dritte Unternehmen eine Versicherung abgeschlossen, in Bulgarien, Rumänien, Ungarn und Griechenland nicht einmal jedes fünfte Unternehmen. Dies kann zu erheblichen Unternehmensrisiken führen und angesichts von durchschnittlichen Schadenskosten von 4,4 Millionen Euro pro Angriff (Ponemon/IBM 2022) für viele Unternehmen existenzbedrohend sein.

Abbildung 20: Anteil an KMU die gegen Cyberangriffe versichert ist



Quelle: Eurostat

Aufgeschlüsselt nach Unternehmensgrößen zeigt sich, dass 35 Prozent aller Großunternehmen eine Versicherung gegen IKT-Schadensfälle haben, bei mittelgroßen Betrieben trifft dies auf 28 Prozent zu. Bei kleineren Unternehmen ist es jedoch nur jedes fünfte. Doch auch innerhalb von Unternehmensgrößen zeigen sich deutliche länderspezifische Unterschiede. Wie eine Analyse der OECD (2022) zeigt, spielen länderspezifische Unterschiede eine große Rolle. So haben knapp 60 Prozent der dänischen Kleinstunternehmen eine IKT-Versicherung, aber weniger als 20 Prozent der deutschen oder österreichischen Kleinunternehmen. Ziel muss es daher sein, den europäischen Versicherungsmarkt zu stärken. Dies gilt insbesondere für Länder mit bisher schwachen Versicherungsraten. Auf europäischer Ebene sollte ein Wissenstransfer zwischen den Mitgliedstaaten angeregt werden, insbesondere Dänemark kann für viele Staaten als Vorbild dienen.

Neben dem Ausbau von IKT-Sicherheitslösungen und dem europäischen Versicherungsmarkt zeigt eine Analyse von ENISA (2021b), dass in der Praxis schlechte Guidelines für KMU eine große Hürde darstellen. In den letzten Jahren haben Institutionen auf europäischer und nationaler Ebene viele Guidelines für Klein- und Mittelbetriebe verfasst. Oftmals ist der Bekanntheitsgrad dieser Dokumente in der Zielgruppe gering, und meist sind diese sehr abstrakt und in einer Sprache verfasst, die dem/der einzelne:n Unternehmer:in keine klare Handlungsempfehlung gibt. So zeigt eine qualitative Analyse, dass Unternehmen oftmals geraten wird, „Backups zu implementieren" oder einen „Information Security Officer" zu benennen, ohne zu erklären, wie man ein Backup „implementiert" oder welche Aufgaben ein „Information Security Officer" eigentlich zu erledigen hat (ENISA 2021b). Derartige Dokumente sind in der Praxis nicht effektiv. Als positives Fallbeispiel kann an dieser Stelle Belgien genannt werden, dessen Guide für Klein- und Mittelbetriebe über 70 detailliert beschriebene Maßnahmen, die sowohl grundlegende Elemente wie ein sicheres Passwort als auch fortgeschrittene Maßnahmen beinhaltet (CCB 2022). Europaweit muss es das Ziel sein, bestimmte Sicherheitspraktiken wie die 3-2-1-Regel in allen KMU bekannt zu machen. Unter dieser Regel versteht man, dass es von allen Daten mindestens drei Kopien an zwei verschiedenen Speicherorten geben soll, wobei einer in einer Cloud liegt.

Gerade für Klein- und Mittelbetriebe ist es von elementarer Bedeutung, dass Cybersicherheit leistbar ist. Dies bedeutet, dass Fördersysteme ausgebaut werden müssen oder die gemeinsame Beschaffung von KMU gefördert wird. Ebenso ist eine Forcierung von cloudbasierten Lösungen zentral, da ein Cloud-Provider Cybersicherheitsmaßnahmen garantieren muss und der Nutzer damit automatisch von einem gewissen Schutz profitiert. Beim Abschluss derartiger „fixed Service Level Agreements" zur Nutzung solcher Dienste haben KMU aufgrund ihrer Größe einen Verhandlungsnachteil. Durch Pooling, also den freiwilligen Zusammenschluss mehrerer Unternehmen, könnten Kosten gesenkt werden (ENISA 2021b).

Abbildung 21: 3-2-1 Modell zur Absicherung von Daten

Quelle: ENISA (2021)

Europa hat den größten Binnenmarkt der Welt und ist die größte Volkswirtschaft. Dies bedeutet, dass Cybersicherheit für Unternehmen von zentraler Bedeutung ist, da europäische Unternehmen somit ein attraktives Ziel für Mitbewerber Europas sowie aus Motiven der persönlichen Bereicherung agierenden Cyberkriminellen darstellen. Klein- und Mittelbetriebe sind, entgegen der öffentlichen Wahrnehmung, oft von Cyberangriffen betroffen, werden aber von Gesetzen wie der NIS-Richtlinie, die einen besseren Schutz zum Ziel hat, nicht erfasst. Da sie mehr als die Hälfte des europäischen Bruttoinlandsprodukts erwirtschaften, ist eine Verbesserung der Cybersicherheit von Europas Klein- und Mittelbetrieben von zentraler Bedeutung.

Empfehlungen

- Europaweiter Ausbau von wesentlichen Sicherheitsmechanismen wie Datenverschlüsselung. Hierbei zeigt sich, dass in allen analysierten Maßnahmen deutliche Länderunterschiede zu beobachten sind. Es ist daher von besonderer Relevanz, diese zu minimieren.
- Da Schadensfälle mit hohen Kosten verbunden sind, ist der Versicherungsmarkt für IKT-Schäden in ganz Europa zu stärken. Dänemark bietet sich als Best-Practice-Beispiel an, von dem andere EU-Staaten lernen können
- Leitfäden, sofern sie vorhanden sind, müssen überarbeitet und praxisnah gestaltet werden. Europäischen und nationalen Institutionen wird empfohlen, diese mit der Zielgruppe, also mit Klein- und Mittelbetrieben, gemeinsam zu erarbeiten, damit sie in der Praxis wirksam werden.

- Wesentliche Sicherheitsstandards wie die 3-2-1-Strategie zur Sicherung von Daten müssen europaweit propagiert und unter Klein- und Mittelbetrieben bekannt gemacht werden, da sie effektive und kostengünstige Lösungen darstellen.
- Die Leistbarkeit von Cybersecuritymaßnahmen muss für KMU gestärkt werden. Dies beginnt bei der Überarbeitung von Fördersystemen, jedoch sollten auf nationaler und europäischer Ebene Lösungen forciert werden, die eine gemeinsame Beschaffung erleichtern, wodurch sich die Kosten für KMU verringern.
- Da die meisten Klein- und Mittelbetriebe weniger als zehn Beschäftigte haben, gilt das Motto: Cybersicherheit der Bevölkerung stärken bedeutet KMU stärken. Strategien zur Bewusstseins- und Wissensvermittlung sollten daher explizit praxisnahe Beispiele aus dem Arbeitsalltag vermitteln.

Kapitel 3

Zusammenfassung und Ausblick

In Eurobarometer-Umfragen gibt mittlerweile eine Mehrheit der befragten Bürger:innen regelmäßig an, besorgt über potenziellen Betrug im Netz oder Cyberattacken auf demokratische Wahlen zu sein. Das Thema ist also mittlerweile endlich beim Großteil der Bevölkerung angekommen. Nun ist die Zeit gekommen, unter größtmöglicher Transparenz mit Rücksicht auf Sicherheitsinteressen Europas in die Erklärungsoffensive zu den notwendigen Maßnahmen überzugehen. Realistisch betrachtet können Entscheidungsträger:innen dabei gleich einpreisen, dass es auch in Zukunft noch Irrungen und Wirrungen dabei geben wird, Cyberbedrohungen zu bekämpfen.

Man denke nur an die von vielen Expert:innen als fehlgeleitet kritisierte Debatte um Uploadfilter (automatisierte Filtersysteme die Uploads kontrollieren) auf europäischer Ebene. Ebenso muss bei jedem Schritt, jeder Maßnahme ein realistisches Bild von notwendigen Ausgaben im Bereich Cybersecurity und -defense gegeben werden. Niemand kann sich 2022 noch der Illusion hingeben, dass wir bei digitaler Verteidigung langfristig billiger wegkommen als beim Einsatz von traditionellen polizeilichen und militärischen Mitteln.

Von den Prämissen ausgehend, dass

- Cybersecurity kein Monopol der IT-Abteilungen dieser Welt ist und es diesen allein überhaupt nicht möglich ist, für einen sicheren Cyberraum zu sorgen,
- der Mensch, sein Verhalten, seine Entscheidungen und seine Wahrnehmung beim Thema Cybersecurity die zentrale Rolle spielen,

wurden in dieser Publikation aktuelle Problemfelder und Lösungsansätze aufgezeigt. Wesentlich für die liberale Gemeinschaft Europas ist dabei, dass man ohne Überwachungsmaßnahmen und überschießende Ein-schränkung der Freiheiten der Europäer:innen auskommt.

Alle Empfehlungen im Überblick

- Die Abstimmung von Außen-, Sicherheits- und Wirtschaftspolitik muss verbessert werden, um die europäische digitale Souveränität zu stärken.
- Eine gemeinsame Verständigung von zentralen Zielen und Maßnahmen zur Stärkung der Bewusstseins- und Wissensvermittlung für Cybersecurity in Europa. Insbesondere niederschwellige Angebote, wie der „Cyber Weather Report" des finnischen National Cyber Security Center sind zu etablieren.
- Cybersecurity-Taxonomie ausbauen. Diese muss einen Mix aus strukturellen Indikationen, Daten zu Einstellungen und Verhaltensweisen im Cybersecurity-Bereich und sicherheitspolitisch relevante Indikatoren beinhalten.
- Grundsatzentscheidungen über die Zukunft europäischen Cloud-Computings sind zu treffen (GAIA-X-Standard in Europa oder Tool zur Verbesserung der Wettbewerbsfähigkeit europäischer Cloudanbieter).
- Massive Investitionen in Europas Netzanbindung, um eigene Infrastruktur im 5G- und Glasfaserbereich zu schaffen und zu kontrollieren, um sicherer vor etwaiger Manipulation von außen zu sein.
- Mindeststandards für Universitäts-Curricula und Ausbau der Bachelorprogramme und akademischen berufsbegleitenden Fortbildungsmaßnahmen in Europa.
- Gender-Gap durch Koppelung von Förderungen an Diversitäts-maßnahmen, Bewusstseinsbildung und Praktika schließen.
- Schwachstellen im Zertifizierungsbereich beheben. Ähnlich wie die NICE-Initiative für die USA benötigt es eine Standardisierung von Berufen, ihren Arbeitstätigkeiten und den dazugehörigen Fähigkeiten.
- Erwachsenenbildung stärken durch Etablierung spezifischer Fortbildungen für bereits im Berufsleben stehende Personen.
- Pilotprojekte, um innerhalb des Cybersecurity-Bereichs Lehrberufe einzuführen.
- Versicherungsmarkt für IKT-Schäden in ganz Europa stärken, um hohe Schadenssummen bei Unternehmen abzufedern, die Opfer eines erfolgreichen Cyberangriffs wurden.
- Praxis-Guidelines nationaler und europäischer Institutionen im Cybersecurity-Bereich überarbeiten und vereinfachen
- Europaweite Implementierung und Promotion wesentlicher Sicherheits-standards (z.B. Datenverschlüsselung, 3-2-1-Strategie zur Sicherung von Daten), besonders bei KMU.
- Leistbarkeit von Cybersecuritymaßnahmen für KMU verbessern.
- Strategien zur Bewusstseins- und Wissensvermittlung mit explizit praxisnahen Beispielen aus dem Arbeitsalltag.

Ausblick

Diese Publikation beleuchtet viele Themen, die unsere Überlegungen bewegten, noch nicht. Insofern soll im Folgenden ein kleiner Ausblick stehen, der jene Aspekte der Debatte streift, die diesmal keinen Platz mehr gehabt haben, aber sicherlich eine Schlüsselrolle in Europas digitaler Zukunft spielen werden.

Qualifizierte Zuwanderung

Europa kämpft als Standort für die Cybersecurity-Serviceindustrie mit Giganten im Osten und Westen und hat es sich dabei selbst mitunter (aus guten Gründen) schwergemacht. Die Orientierung an den europäischen Werten, an Grund- und Menschenrechten sowie am Ideal einer gelungenen Wettbewerbspolitik für den europäischen Binnenmarkt schafft manchmal einen Nachteil bei der globalen Wettbewerbsfähigkeit Europas. Rechtliche Vorgänge dauern länger, europäische Monopole, die es mit US- oder chinesischen Mitbewerbern aufnehmen können, existieren in vielen Bereichen der Digitalwirtschaft (noch) nicht. Als Standort für Fachkräfte der Branche ist Europa, was die Industrie und auch rechtliche Beschränkungen im Innovationsbereich sowie bei der qualifizierten Zuwanderung angeht, auch schlechter aufgestellt. Dabei wird leicht vergessen, dass es sich bei Fachkräften um Menschen handelt, die ihren Lebensmittelpunkt nicht nur anhand von Industriegegebenheiten aussuchen. Europa ist ein lebenswerter Kontinent, in dem sozialer Ausgleich eine gewisse Rolle spielt. Rechtsstaatlichkeit, gute Schulsysteme, Kulturangebote, saubere Umwelt und Diversität machen Europa auf andere Weise wettbewerbsfähig, wenn es um Fachkräfte geht. Allerdings muss die Europäische Union ihre Strategien schleunigst reformieren und bürokratische Hürden für qualifizierte Zuwanderung aus anderen Teilen der Welt abbauen.

Trust

Das nächste und in Kreisen von mit der Materie vertrauten Personen bereits gängige Buzzword im Bereich Sicherheit könnte „Trust" sein. Standards, Selbstregulierung, Kontrolle, Transparenz etc. können vertrauenswürdige Digitalanwendungen von allen anderen abheben. Ist der Kampf eines Digitalraums, in dem Regeln gelten, eingehalten werden und Regelbrüche lückenlos geahndet werden, oftmals verloren worden, so ist es weiterhin möglich, darin „Inseln" des Vertrauens aufzubauen. Digitale Schutzzonen sozusagen, in denen das größte Kapital der darin agierenden Anbieter ihre Vertrauenswürdigkeit durch hohe Standards sind. Garantieren kann so etwas allerdings nur der öffentliche Sektor, und auch dann kann es Unfälle geben, die Security Breaches verursachen. Ein Beispiel für eine solche Technologie ist etwa die Idee einer niederschwelligen, einfachen, europäischen Identität, samt europäischer Login-Lösungen für Online-Shopping oder auch Verwaltungsdienstleistungen.

Abschreckung

Neben dem Ziel, ein attraktiver Lebensstandort für IKT-Fachkräfte zu werden, würde es auch der Abschreckung dienen, wenn Europa beim Intelligence Pooling weitere Fortschritte machte. Zwar werden etwa über Meldesysteme der EU und der NATO bereits gewisse Informationen mit den Partnern geteilt, doch ist das Misstrauen zwischen den europäischen Nachrichtendiensten immer noch deutlich vorhanden. Ein sicheres Europa braucht europäische Nachrichtendienste, die einander vertrauen und eng zusammenarbeiten. Der Weg dahin mag ein mühsamer und langwieriger sein, doch wird Europa davon profitieren.

Technikfolgenabschätzung

Der digitale Wandel ist in vollem Gang. Um zukünftige Entwicklungen und die gesellschaftlichen Auswirkungen besser abschätzen zu können, ist eine Kombination von Technikfolgenabschätzung mit ethischen Grundsätzen als „Kompass" zu entwickeln. Eine realistische Technikfolgenabschätzung, mit der Politik, Unternehmen und die Zivilgesellschaft arbeiten können, basiert auf zwei wesentlichen Grundsätzen: Erstens müssen Technikfolgenabschätzungen in Szenarien mit klar definierten Parametern gedacht werden, und es muss klar definiert werden, welche Begrenzungen die jeweiligen Modelle haben. Zweitens ist es für die Bewertung von Technikfolgen notwendig, klare Zielvorgaben, also erwünschte Effekte, zu definieren. Hier kommen ethische Grundsätze ins Spiel. Welches Potenzial derartige Lösungen haben, zeigen Puaschunder und Feierabend (2019b), die historische Rechtssysteme auf die Verwendbarkeit von Interaktionen zwischen automatischer KI und Menschen vergleichen.

Die Zukunft, könnte man manchmal meinen, existiert nicht mehr. Nicht deshalb, weil wir als Menschheit keine hätten, aber deshalb, weil die Beschleunigung des Fortschritts dazu geführt hat, dass keine Innovation mehr so illusorisch und fern scheint, wie das früher der Fall war. Bei der Implementierung der vorgeschlagenen Maßnahmen ist also nicht an ein fernes Morgen zu denken. Die Zukunft ist jetzt.

Quellenverzeichnis

Accenture (2019): The state of cybersecurity resilience 2021. Zuletzt aufgerufen 17. September 2022: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Alliance of Liberals and Democrats for Europe (2022): A liberal response to current and emerging cyber threats. ALDE Party Secretariat, June 2022, Dublin. Zuletzt aufgerufen 17. September 2022: https://assets.nationbuilder.com/aldeparty/pages/5805/attachments/original/1654356480/006_-_A_liberal_response_to_current_and_emerging_cyber_threats_%281%29.pdf?1654356480

Australian Strategic Policy Institute (2020): Cyber-enabled foreign interference in elections and referendums. Zuletzt aufgerufen 17. September 2022: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf?QnX7Dz7akMiLSP5xHWYYo8ZitxOt2_i7=

Australian Strategic Policy Institute (2021): UN Norms for Responsible State-Behaviour in Cyberspace. Zuletzt aufgerufen 18. September 2022: https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

BBC (2020): TikTok: We are not 'under the thumb' of China. Zuletzt aufgerufen 17. September 2022: https://www.bbc.com/news/business-53469766

Bing, C. et. al (2020): 'Powerful tradecraft': how foreign cyber-spies compromised America. Reuters. Zuletzt aufgerufen 17. September 2022: https://www.reuters.com/article/us-global-cyber-usa-insight-idUSKBN28T0XV

Bing, C. and Kelly, S. (2021): Cyber Attack Shuts down U.S. Fuel Pipeline "Jugular", Biden Briefed. Reuters Zuletzt aufgerufen 17. September 2022: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Blažič, B.J. (2021): The cybersecurity labour shortage in Europe: Moving to a new concept for education and Training. In: Technology in Society, Volume 67,

Bloomberg (2022): The TikTok War Didn't Cause the TikTok Boom. Zuletzt aufgerufen 17. September 2022: https://www.bloomberg.com/news/articles/2022-04-07/tiktok-user-growth-surged-before-russia-ukraine-war

Bunde, T., et. al (2022): Munich Security Report 2022: Turning the Tide – Unlearning Helplessness. Munich Security Conference. Zuletzt aufgerufen: 17. September 2022: https://doi.org/10.47342/QAWU4724

Buzzfeed (2022): Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China. Zuletzt aufgerufen 17. September 2022: https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access

CCB (2022): Cybersecurity Guide for SME. Zuletzt aufgerufen 17. September 2022: https://ccb.belgium.be/en/document/guide-sme

Chang, A. (2018): The Facebook and Cambridge Analytica scandal, explained with a simple diagram. Vox. Zuletzt aufgerufen 17. September 2022: https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

CEDEFOP – European Centre for the Developement of Vocational Training (2022): European qualifications framework. Zuletzt aufgerufen 17. September 2022: https://www.cedefop.europa.eu/en/projects/european-qualifications-framework-eqf

Christiani, D. et. al (2021): The Security Implications of Chinese Infrastructure Investment in Europe. GMF. Zuletzt aufgerufen 17. September 2022: https://www.gmfus.org/sites/default/files/2022-01/Cristiani%20et%20al%20-%20report%20%281%29%20Updated.pdf

Cerulus, L. (2022): Cyber 'spillover' from Ukraine looms in the Baltics. Zuletzt aufgerufen: 17. September 2022: https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/

Conley, H. et. al. (2020): Countering Russian & Chinese influence activities, Center for Strategic & International Studies. Zuletzt aufgerufen: 17. September 2022: https://www.csis.org/analysis/countering-russian-chinese-influence-activities

Cooley, A. & Nexon, D. (2022): The Real Crisis of Global Order: Illiberalism on the Rise. Foreign Affairs 101:1 (2022), 103–118. Zuletzt aufgerufen 17. September 2022: https://perma.cc/U8N3-43XH

Couture, S. & Toupin, S. (2018): What does the concept of "sovereignty" mean in digital, network and technological sovereignty?. paper presented at GigaNet: Global Internet Governance Academic Network. Annual Symposium 2017

Council of the European Union (2022): A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. General Secretariat of the Council, Brüssel, 21. März 2022. Zuletzt aufgerufen 17. September 2022: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

CyberSecurity Ventures (2020): The official annual cybercrime report. Zuletzt aufgerufen: 17. September 2022: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

CyberSecurity Ventures (2021) The official annual cybercrime report. Zuletzt aufgerufen: 17. September 2022:https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Dawson, J. Thomson, R. (2018): The future cybersecurity workforce: going beyond technical skills for successful cyber performance Frontier Psychology. Vol. 12.

Deloitte Services Wirtschaftprüfungs GmbH (2022): Deloitte Cyber Security Report 2022. Wie österreichische Unternehmen mit steigenden Cyber-Bedrohungen umgehen. Zuletzt aufgerufen 17. September 2022: https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/at-cyber-security-report-2022.pdf

Eder, G. & Feierabend, D. (2019): You had one job – Transforming social security systems into the digital working age. European Liberal Forum (ELF)

ENISA (2016): Cybersecurity as Economic Enabler. Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler#:~:text=The%20EU%20Cybersecurity%20Market%20is,than%20all%20other%20major%20regions

ENISA (2019): Election Cybersecurity: Challenges and Opportunities. Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities

ENISA (2020): Threat Landscape for Supply Chain Attacks. Zuletzt aufgerufen 5. August 2022: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ENISA (2020b): Cybersecurity Skills Development in the EU. Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ENISA (2021): Threat Landscape 2020/21. Zuletzt aufgerufen: 5. August 2022: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b): Cybersecurity for SMEs - Challenges and Recommendations. Zuletzt aufgerufen: 17. September 2022: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

ENISA (2021c): Research Directions for Digital Strategic Autonomy Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy

ENISA (2021d): Raising awareness for cybersecurity Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

ENISA (2021e): Addressing Skills Shortage and Gap Through Higher Education Zuletzt aufgerufen 17. September 2022: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

ENISA (2022): CYBERHEAD – Cybersecurity Higher Education Database. Zuletzt aufgerufen 5. September 2022: https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/

ENISA (2022b): Threat Landscape 2022. Zuletzt aufgerufen: 5. November 2022: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Erhardt, M. (2019): Alternativen zu Huawei sind teuer und kosten Zeit. Deutschlandfunk. Zuletzt aufgerufen 18. September 2022: https://www.deutschlandfunk.de/5g-technik-alternativen-zu-huawei-sind-teuer-und-kosten-zeit-100.html

Europäische Kommission (2015): The EU and China signed a key partnership on 5G, our tomorrow's communication networks. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_15_5715/IP_15_5715_EN.pdf

Europäische Kommission (2020): The European Data Market Monitoring Tool. https://data.europa.eu/doi/10.2759/72084

Europäische Kommission (2021): Commission to Invest Nearly €2 Billion from the Digital Europe Programme to Advance on the Digital Transition. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5863

Europäische Kommission (2022): SME definition. Zuletzt abgerufen am 17. September 2022: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

Europäische Kommission (2022b): Entrepreneurship and small and medium-sized enterprises (SMEs). Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/growth/smes_en

Eurostat (2022): ICT specialists in employment. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

Eurostat (2022b): ICT specialists – statistics on hard-to-fill vacancies in enterprises. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises#Employment_and_recruitment_of_ICT_specialists

Eurostat (2022c): ICT security in enterprises. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises

Europäisches Parlament (2019): Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Zuletzt aufgerufen 8. August 2022: https://eur-lex.europa.eu/eli/reg/2019/881/oj

FBI (2021): Internet Crime Report 2021. Internet Crime Complaint Center. Zuletzt aufgerufen 17. September 2022: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Puaschunder, J. & Feierabend, D. (2019): Artificial Intelligence in the Healthcare Sector. European Liberal Forum (ELF).

Puaschunder, J. & Feierabend, D. (2019b): Ancient Legal Codes as Basis for Artificial Intelligence Regulations in the 21st Century. Scientia Moralitas. Vol. 5. Zuletzt aufgerufen 17. September 2022: http://scientiamoralitas.com/index.php/sm/article/view/51

Futurezone (2022): Weitere Daten vom Cyberangriff auf Kärnten veröffentlicht. Zuletzt aufgerufen 17. September 2022: https://futurezone.at/digital-life/weitere-daten-cyberangriff-kaernten-ransomware-veroeffentlicht-leak/402044563

GAIA-X (2022): DAs Projekt GAIA-X. Zuletzt aufgerufen 8. August 2022: www.bmwi.de/Redaktion/EN/Publikationen/DigitaleWelt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6;

Gamal, N., Martino, L., Nestoras, A. (2022): European Cybersecurity in Context. A Policy-Oriented Comparative Analysis. European Liberal Forum (ELF).

Gartner (2019): The Data Center is (Almost) Dead. Zuletzt aufgerufen 17. September 2022: https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead/

Gorman, L. (2020):5G Is Where China and the West Finally Diverge. Zuletzt aufgerufen 17. September 2022: https://www.theatlantic.com/ideas/archive/2020/01/5g-where-china-and-west-finally-diverge/604309/

Hansen, I. & Lim, D. (2018): Doxing Democracy: Influencing Elections Via Cyber Voter Interference. Contemporary Politics. Zuletzt aufgerufen 18. September 2022: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3310974

Herpig (2021): Cybersicherheit und Volksrepublik China. Stiftung Neue Verantwortung. Zuletzt aufgerufen 17. September 2022: https://www.stiftung-nv.de/de/publikation/cybersicherheit-und-die-volksrepublik-china-ein-ueberblick-aus-deutscher-perspektive

Hoffman, W., & Maurer, T. (2019): The Privatization of Security and the Market for Cyber Tools and Services. Centre for Security Sector Governance Zuletzt aufgerufen 17. September 2022: https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf

Jennings, R. (2020): Apple's Assemblers Are Looking To Shift Some Operations From China To India. Forbes. Zuletzt aufgerufen 18. September 2022: https://www.forbes.com/sites/ralphjennings/2020/09/18/apples-assemblers-are-looking-to-shift-some-operations-from-china-to-india/?sh=180275c83a37

Juncker, J.-C., 'The hour of European sovereignty', State of the Union 2018. Zuletzt aufgerufen 17. September 2022: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf

Kaspersky (2022): Was ist Social Engineering? Zuletzt aufgerufen 17. September 2022: https://www.kaspersky.de/resource-center/definitions/social-engineering

Kolbe, P. (2020) "With Hacking, the United States Needs to Stop Playing the Victim," The New York Times. Zuletzt aufgerufen 17. September 2022: https://perma.cc/9FJF-JZTK

Langner, R. (2013): To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. Zuletzt aufgerufen 7. Juli 2022: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lee-Makiyama, H. & Forsthuber, F. (2020): Europe's dependency on China? European Centre for International Political Economy. Zuletzt aufgerufen 17. September 2022: https://ecipe.org/blog/europes-dependency-on-china/

Liedereke, A. & Laudrain, A. (2022): Russia's Cyber War: What's Next and What the European Union Should Do. Council on Foreign Relations. Zuletzt aufgerufen 14. September 2022: https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do

Martin, A., Collier, J. (2019): Beyond Awareness: the Breadth and Depth of the Cyber Skills Demand. Center for Technology and Global Affairs Oxford University. Zuletzt aufgerufen 17. September 2022: https://www.ctga.ox.ac.uk/files/wp10thebreadthanddepthofthecyberskillsdemandpdf

Meinek, S. & Fanta, A. (2022): Geleakte Mitschnitte belasten TikTok. netzpolitik.org. https://netzpolitik.org/2022/china-sieht-alles-geleakte-mitschnitte-belasten-tiktok/

Metzger, M. (2022): Wer steckt hinter angeblichem Gazprom-Video? ZDF online. Zuletzt aufgerufen: 17. September 2022: https://www.zdf.de/nachrichten/politik/propaganda-gazprom-video-desinformation-ukraine-krieg-russland-100.html

Microsoft (2022): The urgency of tackling Europe's cybersecurity skills shortage. Zuletzt aufgerufen 17. September 2022: https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/

Nakashima, E. &Timberg, C. (2020): Russian Government Hackers Are behind a Broad Espionage Campaign that has Compromised U.S. Agencies, Including Treasury and Commerce. The Washington Post, December 14, 2020. Zuletzt aufgerufen am: 14. September: https://perma.cc/N7BG-GKFJ

OECD (2022): Helping the Austrian business sector to cope with new opportunities and challenges in Austria. https://doi.org/10.1787/18151973

Office of the UN Secretary General (2020): Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation. Zuletzt aufgerufen 18. September 2022: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement

NCSC (2022): Cyber weather. Zuletzt aufgerufen 17. September 2022: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather

OECD (2009): OECD Legal Instruments. Zuletzt aufgerufen 17. September 2022: https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0372

O'Flaherty, K. (2021): All the ways TikTok tracks you and how to stop it. Wired. Zuletzt aufgerufen 17. September 2022: https://www.wired.co.uk/article/tiktok-data-privacy

Perlroth, N. (2021): This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Books.

PESCO (2022): Projektliste. Zuletzt aufgerufen 18. September 2022: https://www.pesco.europa.eu/

Ponemon/IBM (2022): Cost of a Data Breach Report. Zuletzt aufgerufen: 17. September 2022: https://www.ibm.com/uk-en/security/data-breach

Proofpoint (2022): What is Email Spoofing? Zuletzt aufgerufen 1. September 2022: https://www.proofpoint.com/uk/threat-reference/email-spoofing.

Prodaft (2021): Ransomware Group In-Depth Analysis'. Zuletzt aufgerufen am 18 November 2022, https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis

Statista (2022a): Cybersecurity - EU-27. Zuletzt aufgerufen: 17. September 2022: https://de.statista.com/outlook/tmo/cybersecurity/eu-27#analystenmeinung

Statista (2022b): Cybersecurity - Weltweit. Zuletzt aufgerufen: 17. September 2022: https://de.statista.com/outlook/tmo/cybersecurity/weltweit

Seaman, J. et. al (2022): Dependence in Europe's Relations with China. Weighing Perceptions and Reality. ENTC. Zuletzt aufgerufen 17. September 2022: https://www.ifri.org/sites/default/files/atoms/files/etnc_2022_report.pdf

Stealthlabs (2020): Top 10 Cybersecurity Trends in 2022 and Beyond! Zuletzt aufgerufen 17. September 2022: https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/

Strumpf, D. (2020): U.S. vs. China in 5G: The Battle Isn't Even Close. Wall Street Journal. Zuletzt aufgerufen 17. September 2022: https://www.wsj.com/articles/u-s-vs-china-in-5g-the-battle-isnt-even-close-11604959200

UN General Assembly (2020): Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation. Zuletzt aufgerufen 18. September 2022: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement

UN Office of the Secretary General's Envoy on Technology (2022): Roadmap for Digital Cooperation. Zuletzt aufgerufen 18. September 2022: https://www.un.org/techenvoy/content/roadmap-digital-cooperation

UN Peacekeeping (2021) Strategy for the Digital Transformation of UN Peacekeeping. Zuletzt aufgerufen 18. September 2022: https://peacekeeping.un.org/sites/default/files/20210917_strategy-for-the-digital-transformation-of-un-peacekeeping_en_final-02_17-09-2021.pdf

UNCTAD (2021): Digital Economy Report 2021. Zuletzt aufgerufen 17. September 2022: https://unctad.org/webflyer/digital-economy-report-2021

UNITE (2022): Mission Statement. Zuletzt aufgerufen 18. September 2022: https://unite.un.org/about

UNODC 2022 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Vakakis, N. et al. (2019): Cybersecurity in SMEs. The smart-home/office use case. IEEE International Workshop on Computer-Aided Modeling, Analysis, and Design of Communication Links and Networks. Zuletzt aufgerufen 17. September 2022: https://ieeexplore.ieee.org/document/8858471

Waldron, K. (2019): Resources for Measuring Cybersecurity, R Street, October 2019. Zuletzt abgerufen am 17. September 2022: https://www.rstreet.org/wp-content/uploads/2019/10/Final-Cyberbibliography-2019.pdf

ZDNET (2022): Global security spending to top $103 billion in 2019. Zuletzt aufgerufen 17. September 2022: https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

Abkürzungen

DDoS – Distributed Denial of Service (Attack)
ENISA – European Union Agency for Cybersecurity
EU – Europäische Union
IKT – Informations- und Kommunikationstechnologie
IT – Informationstechnologie
KMU – Klein- und Mittelunternehmen
NATO – North Atlantic Treaty Organisation
OECD – Organisation for Economic Cooperation and Development
PESCO – Permanent Structured Cooperation

AUTOR:INNEN

Teresa Reiter ist ausgebildete Journalistin und Mitglied des Europe's Futures Programmes am Institut für die Wissenschaften vom Menschen in Wien. Sie arbeitet an der Schnittstelle von Europa- und Sicherheits-politik und Digitalisierung. Teresa gestaltete das Liberal Defence Expert Network der Friedrich-Naumann-Stiftung mit und ist Co-Host des zugehörigen Verteidigungspodcasts „The Defence Café". Zuvor arbeitete sie als Journalistin, war Head of Communications and Marketing beim Europäischen Forum Alpbach und Fachreferentin für Außen-, Europa- und Verteidigungspolitik sowie Migrationspolitik für die NEOS im Österreichischen Parlament. Teresa studierte Nachrichtenjournalismus an der Kingston University in London und internationale Beziehungen an der Diplomatischen Akademie Wien.

Dieter Feierabend ist wissenschaftlicher Leiter im NEOS Lab und arbeitet an der Schnittstelle zwischen Wissenschaft, Zivilgesellschaft und Politik an innovativen politischen Lösungen für eine offene Gesellschaft. Vor seinem Einstieg im NEOS Lab arbeitete der studierte Statistiker und Politikwissenschaftler unter anderem am Institut für Höhere Studien und der Universität Wien mit Schwerpunkt auf empirischer Sozialforschung.

INSTITUTIONS

Das Europäische Liberale Forum (ELF) ist das offizielle politische Stiftung der Europäischen Liberalen Partei, der ALDE. Zusammen mit 46 nationalen Organisationen, arbeiten wir in ganz Europa, um neue Ideen in die politische Debatte zu bringen.

ELF wurde 2007 gegründet, um die liberale und demokratische Bewegung in Europa zu stärken. Unsere Arbeit orientiert sich an liberalen Idealen und dem Glauben an das Prinzip der Freiheit. Wir stehen für ein zukunftsorientiertes Europa, das Chancen für jeder Bürger. ELF engagiert sich in allen politischen Ebenen, von der lokalen bis zur europäischen.

www.liberalforum.eu

Das **NEOS Lab,** die Parteiakademie der NEOS, schafft Raum für politische Entfaltung, um neue Lösungen für eine neue Politik zu entwickeln. Hier werden Talente entdeckt, Persönlichkeiten gefördert und Skills trainiert. Unser politischer Ansatz beruht auf Innovation und Partizipation und lädt zu kritischem Denken, selbstbestimmtem Lernen und offenem Diskurs ein. Das NEOS Lab bietet Angebote in der politischen Aus- und Weiterbildung, ist innerhalb von NEOS die Drehscheibe im Wissens Bereich und als offenes Labor Begegnungsplattform für interessierte Bürger_innen.

lab.neos.eu

A liberal future in a united Europe

/europeanliberalforum
@eurliberalforum
#ELFevent

liberalforum.eu

ISBN: 978-2-39067-041-4

This publication was co-financed by the European Parliament. The European Parliament is not responsible for the content of this publication, or for any use that may be made of it.