ÖAW

ITA INSTITUT FÜR TECHNIKFOLGEN ABSCHÄTZUNG

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Cybersecurity: Systematisierung, Forschungsstand und Innovationspotenziale

Endbericht

Cybersecurity: Systematisierung, Forschungsstand und Innovationspotenziale

Endbericht

Institut für Technikfolgen-Abschätzung
der Österreichischen Akademie der Wissenschaften

Austrian Institute of Technology
Center for Innovation Systems and Policy

Projektleitung: Anna Wang

AutorInnen: Martin Latzenhofer
Stefan Schauer
Niklas Sommerer
Maximilian Zieser

Studie im Auftrag des Österreichischen Parlaments

Wien, Dezember 2021

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 31/2018)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Apostelgasse 23, A-1030 Wien
oeaw.ac.at/ita

AIT Austrian Institute of Technology
Giefinggasse 4, A-1210 Wien
ait.ac.at

Die ITA- und AIT-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung von Forschungsergebnissen. Die ITA-Berichte werden über das Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-projektberichte
Die AIT-Berichte werden über die Website ait.ac.at der Öffentlichkeit zur Verfügung gestellt:
ait.ac.at/ueber-das-ait/center/center-for-innovation-systems-policy/policy-advice-reports/

Projektbericht Nr.: ITA-AIT-16
ISSN: 1819-1320
ISSN-online: 1818-6556
epub.oeaw.ac.at/ita/ita-projektberichte/
parlament.gv.at/SERV/STUD/FTA/

Inhalt

Abbildungsverzeichnis

Executive Summary

Die Durchdringung unserer Gesellschaft mit Informations- und Kommunikationstechnologie (IKT) als wesentlicher Effekt der Digitalisierung bietet unbestritten neue Chancen, aber auch große Herausforderungen. Die vielen neuartigen Services auf multifunktionalen Geräten, die Verbesserung der Kommunikation, die Möglichkeit effektiver zu wirtschaften, neue Organisationsformen, und neue Arten die Freizeit zu erleben sind nur einige der Auswirkungen der digitalen Transformation. Die hochgradige IKT-Vernetzung in allen Lebensbereichen wirft Fragestellungen zur Verletzlichkeit digitaler Technologien und schlussendlich unserer Gesellschaft auf. Um als Gesellschaft diesen Pfad der Digitalisierung aktiv zu gestalten, müssen gleichzeitig auch Sicherheitsaspekte berücksichtigt werden. Einerseits muss Schutz gegen bewusste Angriffe auf (öffentliche und private) IKT-Strukturen, aber auch gegen unbewusstes Fehlverhalten mit potenziell großen Auswirkungen auf unser soziales Zusammenleben hergestellt werden.

Die große Herausforderung besteht darin, dass die Digitalisierung mittlerweile alle Lebensbereiche betrifft. Demzufolge muss auch die Sicherheit und Resilienz digitaler Systeme in all diesen Bereichen berücksichtigt werden. Diese immer intensivere Dynamik macht auch vor den staatlichen Strukturen und ihren Institutionen nicht halt. Cybersecurity ist damit keine für sich alleinstehende Domäne, sondern vielmehr eine essenzielle Querschnittsmaterie mit vielschichtigen Verbindungen in andere Lebensbereiche. Diese inhärente Komplexität von digitaler Sicherheit macht das Thema Cybersecurity schwer abgrenzbar.

Die hier vorliegende Arbeit versucht dieser Denkweise Rechnung zu tragen und unternimmt den Versuch einer systematischen Strukturierung des Themas Cybersecurity aus technischer, gesellschaftlicher sowie Forschungs- und Innovationsperspektive. Um aus österreichischer Sicht Cybersecurity aktiv gestalten zu können, wurden folgende Schlussfolgerungen und Handlungsoptionen unter Einbeziehung von langjährigen ExpertInnen in Interviews und einem Workshops entwickelt:

Cybersecurity ist ein Thema mit hoher gesellschaftlicher Relevanz

Mit der fortschreitenden **Digitalisierung** und der Durchdringung aller Aspekte des Lebens durch digitale Technologien verwandelte sich auch der Sicherheitsaspekt von rein technisch-bezogener IT-Security in ein breiteres Verständnis der Cybersecurity. Cybersecurity ist nunmehr ein Synonym für **umfassenden Schutz des digitalen Lebens** und soll somit auch die Vielschichtigkeit des Themas signalisieren**.**

Die Digitalisierung und der steigende Vernetzungsgrad bewirkt, dass Cybersecurity nun alle Gesellschaftsbereiche und Akteure, von Staaten und Unternehmen bis hin zu Einzelpersonen, betrifft. In diesem Sinne bezieht sich Cybersecurity nicht nur auf das Verhindern vorsätzlicher Cyberattacken, sondern auch auf die zahlreichen anderen vielschichtigen **Risiken für AnwenderInnen und Gesellschaft**. Dazu zählen etwa Bedenken zum Datenschutz und der Privatsphäre, wenn AnwenderInnen mit einer stetig wachsenden Zahl an Kameras, Mikrofonen und Sensoren ausgestattet sind, oder die befürchteten Einschränkungen der Entscheidungs- und Meinungsfreiheit, wenn durch automatisierte Systeme der Informationsstrom zunehmend personalisiert und gefiltert wird.

Die zunehmende **Professionalisierung** der AngreiferInnen, die Entwicklung von Ransomware-Geschäftsmodellen sowie die effektiveren Angriffsmethoden, z.B. Ransomware, DDoS, APT, stellt Cybersecurity vor wachsende Herausforderungen. Durch die steigende Gefahr von hybriden Bedrohungen und Cyber Warfare, also die von Staaten geduldeten oder geförderten Angriffe auf staatliche Institutionen, kritische Infrastrukturen oder gezielte Verbreitung von Desinformation, entstehen auch Risiken für gesellschaftliche Strukturen und demokratische Grundwerte. Nur durch Cybersecurity kann diesen Gefahren begegnet und demokratische Institutionen gestärkt werden.

Angesichts der Bedeutung von Cybersecurity haben interviewte ExpertInnen sowie TeilnehmerInnen des Workshops einstimmig ein **fehlendes Bewusstsein** für Cybersecurity sowie den Auswirkungen der Digitalisierung festgestellt. Dies betrifft alle Akteure, von Organisationen und Unternehmen bis hin zu Einzelpersonen und EndnutzerInnen.

Handlungsempfehlung 1: Bewusstsein über Cybersecurity in der Gesellschaft stärken

Die Digitalisierung hat in den letzten Jahren viele Handlungsfelder geschaffen, mit denen sich Österreich weit mehr als bisher beschäftigen muss. Neuartigen Trends, Gefahren, Risiken und Entwicklungen muss proaktiv begegnet und entgegengewirkt werden. Dabei ist es wichtig, in der breiten Bevölkerung, bei Unternehmen wie auch bei Einzelpersonen aller Altersgruppen ein hohes Maß an Grundverständnis und Bewusstsein zu entwickeln. Vor dem Hintergrund der hohen gesellschaftlichen Relevanz von Cybersecurity und dem gleichzeitig festgestellten Mangel an Bewusstsein über die Risiken der Digitalisierung sind Maßnahmen zur Bewusstseinsbildung über Cybersecurity für Politik, Privatunternehmen bis hin zur Bevölkerung und Einzelpersonen zu empfehlen (siehe auch [1]). Gleichzeitig könnte somit ein gesellschaftlicher Diskurs über Cybersecurity und die proaktive Auseinandersetzung mit den Folgen der Digitalisierung forciert werden. Für Organisationen und Unternehmen könnten im Rahmen der Bewusstseinsbildung **Cybersecurity-Übungen und Trainings** unter Anwendung moderner Ansätze umgesetzt werden (siehe auch [2]). Bewusstseinsbildung bei Einzelpersonen sollte im Kontext der **Digital Literacy** geschehen. Digital Literacy bezeichnet die Fähigkeit, sich sicher in einer digitalen Gesellschaft bewegen und dort auch lernen und arbeiten zu können. Diese Fähigkeit sollten im Idealfall schon in jungen Jahren, beispielsweise im Rahmen der Schulausbildung, erlernt und ständig weiterentwickelt werden.

Handlungsempfehlung 2: Cybersecurity als integralen Bestandteil von IKT-Produkten und Services etablieren und Security-by-Design Methoden anwenden

In engem Zusammenhang mit dem schwach ausgeprägten Bewusstsein über Cybersecurity und die Risiken der Digitalisierung steht auch das Verständnis von Cybersecurity als rein technisches Thema. Durch die fortschreitende Vernetzung hat sich Cybersecurity jedoch längst zu einem gesellschaftlichen Querschnittsthema gewandelt. Vor diesem Hintergrund sollte Cybersecurity als integraler Bestandteil von IKT-Produkten und Services betrachtet werden. Zum Beispiel sollten **Security-by-Design Methoden** beim Aufbau und der Konzeption neuer IKT-Systeme, Netzwerke oder Software berücksichtigt werden. So können Sicherheitseigenschaften bereits initial als Designkriterium integriert werden. Dadurch lassen sich Systemfehler vermeiden und potenziellen AngreiferInnen werden kleinere Angriffsflächen geboten.

Handlungsempfehlung 3: Foresight für Cybersecurity durchführen

Um den **gesellschaftlichen Diskurs** mit Cybersecurity zu forcieren und eine **proaktive Auseinandersetzung** mit Cybersecurity und den Auswirkungen der Digitalisierung zu implementieren, wird ein Foresight-Prozess zu Cybersecurity empfohlen. In diesem Rahmen kann durch Einbindung von PolitkvertreterInnen, ExpertInnen, Stakeholdern und BürgerInnen eine gesamtgesellschaftliche Diskussion über die Folgen der Digitalisierung und deren Auswirkungen auf Sicherheitsaspekte etabliert werden. Dies könnte zugleich einen Beitrag zur höheren Akzeptanz der digitalen Transformation und Etablierung einer Cybersecurity-Kultur leisten (siehe auch [2]).

Cybersecurity stellt höhere Ansprüche an Kooperation und Koordination

Neben der hohen gesellschaftlichen Relevanz ist Cybersecurity auch rechtlich eine Querschnittsmaterie. Die Vielschichtigkeit und Komplexität des Themas bedingt darüber hinaus intensive Koordination, Kooperation, Informationsaustausch und gegenseitige Lernprozesse auf allen Akteursebenen. In diesem Zusammenhang wird der nationale Handlungsrahmen durch die Österreichische Cybersicherheit-Strategie und auf europäischer Ebene durch die Europäische Cybersecurity-Strategie gesetzt. Cybersecurity wird national durch das Bundeskanzleramt koordiniert, zusätzlich sind das Bundesministerium für Inneres, das Bundesministerium für europäische und internationale Angelegenheiten und das Bundesministerium für Landesverteidigungen ebenso für Aspekte von Cybersecurity zuständig. Auf strategischer und operativer Ebene wurde eine interministerielle Koordinationsstruktur etabliert, die Public-Private Partnership Cyber-Sicherheit-Plattform soll zudem den Austausch und die Koordination zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung fördern.

In den Interviews und im Workshop wurde von den ExpertInnen die grundsätzlich gute Vernetzung innerhalb der Cybersecurity-Community hervorgehoben. Jedoch wurde trotz der etablierten Strukturen der Bedarf nach

intensiverer und effektiverer Koordination und Abstimmung zwischen Akteuren und Stakeholdern geäußert. Dies betrifft einerseits die Koordination zwischen **staatlichen und privaten Akteuren**, andererseits die **Kooperation auf operativer Ebene**. In diesem Zusammenhang wurde im Rahmen von Interviews und Workshop auch der Bedarf nach aktiver Gestaltung von Digitalisierung und Cybersecurity geäußert. Einerseits würde das eine proaktive Auseinandersetzung mit Cybersecurity auf allen Ebenen, andererseits auch die proaktive Gestaltung und Positionierung Österreichs in diesem Themengebiet auf europäischer und internationaler Ebene bedeuten. Cybersecurity ist ein länderübergreifendes Thema und kann zudem nicht durch eine einzelne Gruppe von Akteuren oder Stakeholdern erreicht werden.

Handlungsempfehlung 4: Koordination und Kooperation zwischen Akteuren und Stakeholdern stärken

Um der Vielschichtigkeit und Komplexität des Themas gerecht zu werden, sollte die Kooperation und der Austausch auf **operativer Ebene**, genauer gesagt zwischen CERTs, CSIRTs, sowie mittels etablierter Informationsaustauschplattformen (z.B. CSP), gestärkt werden. Zusätzlich sollte auch die Abstimmung zwischen öffentlichen und privaten Akteuren intensiviert werden. Die CSP könnte in diesem Kontext eine prominentere Rolle einnehmen, indem Formate und Prozesse für **bidirektionalen Informationsaustausch** verstärkt werden. Gleichzeitig sollte auch die Kooperation zwischen staatlichen Institutionen und Forschungsakteuren sichergestellt werden, um geeignete Rahmenbedingungen und Schutzmechanismen etablieren zu können (siehe auch [2]). Die effektivere Abstimmung und Kooperation der Akteure könnten das proaktive strategische, politische und gesetzliche Handeln sowie die Steuerung des Cybersecurity-Themas unterstützen.

Handlungsempfehlung 5: Aktive Gestaltung auf europäischer und internationaler Ebene vornehmen

Vor dem Hintergrund der steigenden Risiken von Cyber Warfare ist ein europäisch und international koordiniertes Handeln in Cybersecurity von hoher Relevanz. Österreich verfolgt bereits Aktivitäten und Maßnahmen im Bereich der **Cyberdiplomatie**, und auch auf europäischer Ebene ist Cyberdiplomatie ein zentraler Bestandteil der Cybersecurity-Strategie. Bestrebungen in Cyberdiplomatie und der internationalen Koordination sollten weiter verstärkt werden.

Darüber hinaus könnte sich Österreich und Europa durch existierende **thematische Stärken und Aktivitäten** auch international positionieren. Durch den europäischen Cybersecurity Act wurde ein Rahmen für die Etablierung von Cybersecurity-Zertifizierungsschemen in Produkten, Prozessen und Dienstleistungen geschaffen und die ENISA mit der Entwicklung von Zertifizierungsschemen betraut. Österreich kann in diesem Feld mit wachsender Relevanz Vorbildfunktion einnehmen. Das **österreichische Gütesiegel für Cybersecurity** „Cyber Trust Austria Label“ des KSÖ ist das erste dieser Art in der EU. Zudem wurde bereits ein österreichisches CyberRisk Rating etabliert, um digitale Risiken in globalen Lieferketten sichtbar zu machen und Unternehmen mit einem standardisierten Cyber-Risikomanagement für Lieferanten zu unterstützen.

Österreichische Forschung in Cybersecurity spielt eine bedeutende Rolle auf europäischer Ebene

Die Analyse der österreichischen Beteiligung im europäischen Forschungsrahmenprogramm Horizon 2020 zeigt auf, dass österreichische Organisationen eine bedeutende Rolle einnehmen können und eine hohe Beteiligung an Cybersecurity-Projekten aufweisen. Interviews und Workshop bestätigen dieses Ergebnis: die befragten Cybersecurity-ExpertInnen verweisen einstimmig auf die Existenz mehrerer exzellenter, international sichtbarer Forschungsgruppen an Österreichs Universitäten, Forschungsorganisationen und Unternehmen.

Im Rahmen der Interviews und des Workshops wurden österreichische FTI-Aktivitäten, unter anderem in kooperativen europäischen und nationalen Forschungsprojekten, in Feldern wie **Quantenkryptographie, Quantencomputing, Hardwaresicherheit, neue Werkzeuge und Methoden** der Cybersecurity für öffentliche Organisationen und kritische Infrastrukturen als besondere Stärkefelder genannt. Darüber hinaus wurden durch die Programmdatenanalyse von Horizon 2020 österreichische Beteiligungen an FTI-Aktivitäten zu Cybersecurity in Produkten und Prozessen identifiziert, die durch die digitale Transformation einer zunehmenden Vernetzung erfahren (z.B. Automobilindustrie, Lieferketten). Dies weist auf ein bestehendes Potenzial in

der Innovation und Integration von **Cybersecurity in klassischen Industriefeldern** hin. Darüber hinaus haben ExpertInnen im Rahmen von Interviews und Workshops die Bereiche **OT-Security, E-Identität** und **E-Government** als zusätzliche Stärkefelder Österreichs identifiziert.

Zudem verwiesen ExpertInnen in Interviews und im Workshop auf eine Reihe an FTI-Feldern mit wachsender Bedeutung und hohem Innovationspotenzial. Dazu gehören Cybersecurity-Aspekte im Kontext der Entwicklung von **Künstlicher Intelligenz und Machine Learning**, **Blockchain**, **Desinformationserkennung, Cybersecurity im Kontext von IoT und Smart Devices** sowie **Ethik in Cybersecurity.** Entwicklungen in der Quantentechnologie könnten ebenso eine Innovationschance für Österreich darstellen, nicht zuletzt aufgrund von existierenden FTI-Aktivitäten in den Bereichen **Quantenkryptographie** und **Quantencomputing.**

Handlungsempfehlung 6: Stärkefelder und Nischen ausbauen

Auf Basis der bereits sehr guten Positionierung der österreichischen FTI-Akteure auf europäischer Ebene sollte die österreichische Cybersecurity-Forschung weiter gestärkt werden. Aufgrund der Vielschichtigkeit des Cybersecurity-Themenbereichs ist es empfehlenswert, auf **bestehende Stärkefelder** und **Nischen mit Zukunftspotenzial** zu fokussieren. Zu den Stärkefeldern zählen unter anderem Hardwaresicherheit, neue Werkzeuge und Methoden der Cybersecurity, OT-Security, E-Identität und E-Government. Nischen mit Zukunftspotenzial sollten identifiziert und aktiv durch **gezielten Kompetenzaufbau** gefördert werden. Dazu zählen Maßnahmen wie Förderung der Grundlagenforschung, Einrichtung von Lehrstühlen sowie die Förderung von angewandter, intersektoraler und interdisziplinärer (Sicherheits-) Forschung. Cybersecurity-Aspekte in aktuellen FTI-Feldern wie Künstliche Intelligenz/Machine Learning, Blockchain und Quantencomputing könnten Chancen für österreichische FTI bieten.

Handlungsempfehlung 7: Wissenschaftskommunikation und Wissenstransfer stärken

Um die Anwendbarkeit von Forschungsergebnissen und deren Verbreitung vor allem in der breiten Bevölkerung zu erhöhen, ist es empfehlenswert, Maßnahmen zur Wissenschaftskommunikation und Wissenstransfer zu stärken. Der effektive Wissenstransfer zwischen Wissenschaft, Wirtschaft, Gesellschaft und Politik könnte neben der Sicherstellung der Anwendbarkeit der Ergebnisse für andere FTI-Akteure und andere Disziplinen auch einen Beitrag zur Bewusstseinsbildung über Cybersecurity und den Risiken der Digitalisierung leisten. Die Aufbereitung von Forschungsergebnissen in für Laien nachvollziehbarer Art und Weise, z.B. in Form von „Kids‘ Corners“ auf Webseiten, könnte eines der Maßnahmen darstellen.

Österreich hat ungenutzte Potenziale für ein Cybersecurity-(Innovations-)Ökosystem

Während die Analyse der österreichischen Beteiligungen im europäischen Forschungsrahmenprogramm Horizon 2020 eine sehr gute Positionierung österreichischer FTI-Akteure aufgezeigt hat, die mehrfach in Interviews und Workshop bestätigt wurde, wurde von den befragten ExpertInnen gleichzeitig eine Schwäche des Innovations- und Wirtschaftszweigs Cybersecurity festgestellt. Österreich und Europa sind in diesem Kontext abhängig von Cybersecurity-Lösungen aus Drittstaaten; es gibt kaum österreichische Lösungsanbieter. Die ExpertInnen schreiben diese Problematik vor allem einem fehlenden **Ökosystem** für den Wirtschaftszweig Cybersecurity zu. Zum einen besteht ein **Fachkräftemangel** vor dem Hintergrund der erwarteten steigenden Nachfrage, gleichzeitig auch ein Mangel sowohl an Lösungsanbietern als auch an Cybersecurity-Dienstleistern.

Handlungsempfehlung 8: Den Wirtschaftszweig Cybersecurity gezielt aufbauen und stärken

Vor dem Hintergrund der festgestellten Schwäche in der Cybersecurity-Unternehmenslandschaft und dem Mangel an Cybersecurity-ExpertInnen wird empfohlen, einen Schwerpunkt in die Unterstützung von Cybersecurity-Unternehmen zu legen. Einerseits sollte die **Ausbildung** von Cybersecurity-ExpertInnen, vor allem in außeruniversitären Ausbildungsstätten in der Lehre, Höheren Technischen Lehranstalten und Fachhochschulen zu forcieren. Andererseits sollten Maßnahmen in der Förderung von Cybersecurity-Lösungsanbietern und Dienstleistern umgesetzt werden. Dazu könnten **Anreize für Wirtschaftsansiedlungen**, Risikokapital für innovative Unternehmensgründungen sowie Maßnahmen zur Vernetzung der Unternehmen im Bereich Entwicklung von Cybersecurity-Lösungen zählen.

1. Einleitung

Die Durchdringung unserer Gesellschaft mit Informations- und Kommunikationstechnologie (IKT) als wesentlicher Effekt der Digitalisierung bietet unbestritten neue Chancen, aber auch große Herausforderungen. Die vielen neuartigen Services auf multifunktionalen Geräten, die Verbesserung der Kommunikation, die Möglichkeit effektiver zu wirtschaften, neue Organisationsformen, und neue Arten die Freizeit zu erleben sind nur einige der Auswirkungen der digitalen Transformation. Der Transformationsprozess kann daher als disruptiv angesehen werden, obwohl die Veränderungen oft schleichend und mitunter ungesteuert erfolgt sowie oft gar nicht gemäß seiner Bedeutung wahrgenommen wird.

Die hochgradige IKT-Vernetzung in allen Lebensbereichen wirft Fragestellungen zur Verletzlichkeit digitaler Technologien und schlussendlich unserer Gesellschaft auf. In Europe und Österreich besteht eine starke Abhängigkeit von Technologien aus den USA sowie in jüngerer Zeit auch aus China. Die globale Weltwirtschaft hat sich außerdem stark auf Teilbereiche in der Supply Chain fokussiert, wodurch auch Abhängigkeiten von Zulieferern von Vorprodukten entstehen. Europa scheint hier nicht mehr in der Lage, für die Digitalisierung erforderliche Lieferketten autonom, ganzheitlich und unter Ausnutzung des kompletten Handlungsraums zu bewirtschaften.

Ebenso stammen die großen Hersteller der IKT-Endgeräte aus den USA oder China. Es existieren nur mehr wenige relevante europäische Unternehmen, mit potenziell drastischen Auswirkungen auf die digitale Grundversorgung der Bevölkerung. Auch auf der Service-Ebene, also bei den Anbietern von Apps, IKT-Services und Software-Lösungen, ist eine Dominanz nicht-europäischer Unternehmen festzustellen. Die zunehmende Abhängigkeit von einigen wenigen Anbietern wurde beispielsweise auch im Zuge der Diskussionen zum 5G-Ausbaus sichtbar [3].

Zudem fällt auf, dass diese Aktivitäten und Initiativen mehrheitlich von privatwirtschaftlich organisierten Unternehmen gestaltet und entwickelt werden, Nationalstaaten und supranationale Vereinigungen werden selbst zunehmend abhängig vom Funktionieren dieser Unternehmen, etwa bei den kritischen Infrastrukturen, der Grundversorgung der Bevölkerung mit täglichen Gütern und Dienstleistungen oder der Kommunikation, z.B. über soziale Medien.

Zuletzt wurden diese Defizite durch externe Schocks sichtbar, etwa (zumeist simulierte oder sogar Beinahe-) Blackouts oder einschneidende Krisensituationen wie die Covid-19-Pandemie, in der aufgrund der Distanzregeln die Telekommunikation und IKT-Services eine unverzichtbare Basis für wirtschaftliches und soziales Interagieren darstellten. Um als Gesellschaft diesen Pfad der Digitalisierung aktiv zu gestalten, müssen gleichzeitig auch Sicherheitsaspekte berücksichtigt werden. Einerseits muss Schutz gegen bewusste Angriffe auf (öffentliche und private) IKT-Strukturen, aber auch gegen unbewusstes Fehlverhalten mit potenziell großen Auswirkungen auf unser soziales Zusammenleben hergestellt werden.

Die große Herausforderung besteht darin, dass die Digitalisierung mittlerweile alle Lebensbereiche betrifft. Demzufolge muss auch die Sicherheit und Resilienz digitaler Systeme in all diesen Bereichen berücksichtigt werden. Diese immer intensivere Dynamik macht auch vor den staatlichen Strukturen und ihren Institutionen nicht halt. Cybersecurity ist damit keine für sich alleinstehende Domäne, sondern vielmehr eine essenzielle Querschnittsmaterie mit vielschichtigen Verbindungen in andere Lebensbereiche. Diese inhärente Komplexität von digitaler Sicherheit macht das Thema Cybersecurity schwer abgrenzbar.

Die hier vorliegende Arbeit versucht dieser Denkweise Rechnung zu tragen und unternimmt den Versuch einer systematischen Strukturierung des Themas Cybersecurity aus technischer, gesellschaftlicher sowie Forschungs- und Innovationsperspektive. Um aus österreichischer Sicht Cybersecurity aktiv gestalten zu können, wurden Schlussfolgerungen und Handlungsoptionen unter Einbeziehung von langjährigen ExpertInnen in Interviews und einem Workshops entwickelt.

Die vorliegende Studie basiert auf einem Mixed-Methods Ansatz qualitativer und quantitativer Methoden. In einem ersten Schritt erfolgte eine Literaturrecherche bestehender Analysen, Strategiedokumente und relevanter wissenschaftlicher Publikationen. Diese wurde durch eine Sekundärdatenanalyse der AIT-EUPRO

Datenbank zur Beteiligung österreichischer Akteure im europäischen Forschungsrahmenprogramm Horizon 2020 durchgeführt. Ergänzend fanden acht leitfadengestützte Interviews mit Cybersecurity-ExpertInnen aus Wissenschaft, Wirtschaft, Interessensvertretungen und öffentlicher Verwaltung statt. Eine Liste der InterviewpartnerInnen ist in Anhang I zu finden. Darauf aufbauend wurden die Zwischenergebnisse im Rahmen eines online Stakeholderworkshops mit über 20 TeilnehmerInnen reflektiert, verdichtet und anschließend Handlungsoptionen identifiziert und diskutiert. Die Workshop-Agenda und Liste der TeilnehmerInnen sind in Anhang II beigelegt. Schließlich wurde eine Synthese der Ergebnisse vorgenommen, die einzelnen Befunde trianguliert und Handlungsempfehlungen abgeleitet.

Abschnitt 2 „Technische Aspekte“ versucht, die technische Entwicklung bis heute kurz und prägnant darzustellen und den Begriff Cybersecurity aus verschiedenen Blickwinkeln zu diskutieren. Im darauffolgenden Abschnitt 3 „Gesellschaft und Digitalisierung“ wird versucht, aktuelle Entwicklungen der Digitalisierung zu kategorisieren und in Zusammenhang mit Cybersecurity zu stellen, um der angesprochenen Vielschichtigkeit des Begriffs entsprechend Rechnung zu tragen. Zudem soll der Abschnitt auf Basis von Interviews und einem Workshop gesellschaftliche Anforderungen an Cybersecurity identifizieren. Abschnitt 4 „Strategische und rechtliche Rahmenbedingungen“ bietet einen Überblick über die wesentlichen politischen Aktivitäten auf nationaler und europäischer Ebene, die auf Cybersecurity abzielen oder Einfluss darauf haben. Abschnitt 5 „Forschung, Technologie und Innovation im Bereich Cybersecurity“ analysiert die Position österreichischer Cybersecurity-FTI im europäischen Kontext und gibt Einblick in Beteiligungsstrukturen und Akteure. Der Abschnitt fasst zudem Interviews und Workshopergebnisse zur Zukunft von FTI-Aktivitäten in Österreich zusammen. Zusammenfassende Schlussfolgerungen und Handlungsempfehlungen sind in Abschnitt 6 dargestellt.

2. Technische Aspekte

2.1 Einleitung

Schlagzeilen über aufsehenerregende Cyberattacken auf kritische Infrastrukturen, Privatunternehmen und Gemeinden sind in den vergangenen Jahren fast alltäglich geworden. Vor allem seit dem Ausbruch der Covid-19-Pandemie kam es zu einem signifikanten Anstieg an Cyberangriffen [1]. Mit der Zunahme von Telearbeit stieg die Zahl an Cyberattacken mit Lösegeldforderungen 2020 um 150 % und die von Opfern gezahlten Beträge haben sich im Vergleich zum Vorjahr um mehr als 300 % erhöht [4]. Die beliebtesten Ziele bei Cyberattacken sind digitale Dienste, Regierungsverwaltungen, Technologiebranchen, Finanzorganisationen und das Gesundheitswesen. Im Durchschnitt dauert es sechs Monate, bis eine Datenschutzverletzung entdeckt wird, was AngreiferInnen viel Zeit gibt, die Daten der Opfer zu missbrauchen [5].

Cyberangriffe können viele unterschiedliche Formen annehmen, von Desinformationskampagnen bis hin zu Ransomware Attacken, und somit folgenschwere Auswirkungen auf eine Vielzahl von Akteuren haben, wie z.B. auf Privatpersonen, Unternehmen und deren Kunden oder gar ganze Staaten. Um sich vor Cybergefahren zu schützen, ist es wichtig, dass die Wirtschaftsakteure, Interessensvertretungen, Regierungen, Behörden, aber auch Privatpersonen selbst Maßnahmen treffen, um dieser Entwicklung in den Cyber-Gefahren und -Risiken entgegenzuwirken. Solche Maßnahmen werden unter Cybersecurity subsumiert.

Aufgrund dieser Zunahme und der Entwicklungen der letzten Jahrzehnte wurde Cybersecurity oder auch Cybersicherheit zu einem „Buzz-Word“. Auch wenn sich Cybersecurity in den letzten Jahren zu einem allgegenwärtigen Thema entwickelt hat, ist die Bedeutung des Begriffes unscharf und wird von verschiedenen Akteuren unterschiedlich aufgefasst. Während für viele Cybersecurity ein rein technologisches Thema darstellt, zeigt sich ein wachsendes Bewusstsein für die Relevanz gesellschaftlicher und sozialer Aspekte von Cybersecurity. Die nachfolgenden Abschnitte beschäftigen sich zunächst mit einer allgemeinen technischen Erläuterung des Themas, um dann mögliche Definitionen mit deutlich breiterer Auslegung des Begriffes zu diskutieren.

2.2 Begriffsdiskurs

2.2.1 Begriffsevolution

Um sich dem Begriff Cybersecurity anzunähern, bedarf es einer kurzen historischen Betrachtung der Sicherheit in der IKT oder – in früheren Zeiten auch – IT (Informationstechnologie). Aufbauend auf den ExpertenInnen Interviews lässt sich ableiten, dass ursprünglich alle Maßnahmen und Aktivitäten mit Beginn der 1990er Jahre unter dem Begriff **IT-Security** zusammengefasst wurden. Dieser hatte eine überwiegend technische Perspektive und versuchte – ausgehend von übergeordneten Schutzzielen – vorwiegend technische Maßnahmen zu subsumieren, um digitale Information zu schützen. Im Kern haben diese Grundaussagen auch heute noch in Cybersecurity Bestand, denn hier nahm der heute noch breit anerkannte „CIA-Ansatz“ seinen Ausgang (vgl. Abschnitt 2.4).

Man erkannte jedoch auch, dass die technische Perspektive mittelfristig zu kurz greift. Einerseits wurde daher die Bedeutung des Begriffs auf jedwede Information ausgeweitet (auch analoge Formen), anderseits wurden Aktivitäten mit diesen Informationen in die Überlegungen einbezogen. Die Weiterentwicklung zum Begriffskonzept **Information Security** war die Folge. Dies war auch deswegen erforderlich, weil die IT sich zunehmend zu einer komplexen Disziplin entwickelte, die von Nicht-ExpertInnen nicht mehr vollumfänglich verstanden wurde und somit Ziel von Auslagerungen an SpezialistInnen wurde. Hier ist auch die beginnende Tendenz zu verorten, IT als „Blackbox“ zu sehen, was auch heute noch gilt und durchaus kritisch zu betrachten ist.

Outsourcing und die Umstellung des Marktes in eine kleinteiligere Struktur der Dienstleistungsanbieter für Unternehmen kennzeichneten den Beginn der 2000er-Jahre. Somit war es auch notwendig, Informationssicherheitsaspekte zu definieren und die Verantwortung aufzuteilen: Der Information Owner (der Eigentümer) lässt sich von einem Information Provider (dem Verarbeiter) servicieren. Dadurch wurde auch der dahinterstehende Akteur verstärkt akzentuiert, also der Mensch, welcher eine Aktivität mit der Information ausführt. Information Security bezeichnet somit auch jene Prozesse, die Informationen – oder in strukturierter Form Daten – schützen, wobei das Format und das Medium irrelevant sind. Es kann sich nämlich sowohl um physische als auch digitale Daten handeln. Information Security beschreibt auch keine einzelne Technologie, sondern steht für eine Strategie, bestehend aus Prozessen, Tools und Richtlinien, welche Bedrohungen verhindern, entdecken, dokumentieren und im schlimmsten Falle Gegenmaßnahmen einleiten sollen. Zusammenfassend steht Information Security für die Prozesse und Richtlinien, die implementiert werden, um jegliche Form von Informationen und Daten vor unautorisierten Zugriffen und unrechtmäßiger Benutzung zu schützen [6].

Aus einem gänzlich anderen Ursprung entwickelte sich parallel der Begriff **OT-Security** (Operation Technology Security). Produktions- und Fertigungssysteme wurden seit Anbeginn vom Lieferanten dieses Systems aufgesetzt, ihre Steuerungen programmiert und im Fehlerfall serviciert. Durch die aufkommenden Möglichkeiten der Informationsverarbeitung wurde Potenzial darin gesehen, diese mit der IT-Welt zu verbinden und sie miteinander kommunizieren zu lassen. Leider schwappten damit die Sicherheitsproblemfelder auch in den Produktions- und Fertigungsbereich über, erste Schadcodes verursachten ebenda ernste Beeinträchtigungen [7]. Insofern war dieses Zusammenwachsen der IT- mit der OT-Welt ein Indikator für die beginnende Vernetzung, zwar noch innerhalb der Organisationsgrenzen und noch vermeintlich kontrollierbar, aber doch die Zukunft vorzeichnend – wieder in der Dualität von neuen Möglichkeiten einerseits und den damit einhergehenden Bedrohungen anderseits.

Beginnend mit dem zunehmenden Grad der Vernetzung wurde es immer schwieriger, Informationssicherheit zwischen unterschiedlichen Akteuren und Organisationen, die nun über das öffentliche Internet enger und intensiver zusammenarbeiten konnten und so neue Services generierten, tatsächlich reibungslos in Einklang zu bringen. Die Evolution von einer reinen Informationsverarbeitung in der IT zur IKT trug dazu ebenso bei, nicht zuletzt, weil die klassische Telefonie technisch immer mehr durch das Internet Protocol (IP) abgewickelt wurde, der Mobilfunk disruptiv auf das Kommunikationsverhalten einwirkte, neben Sprache nun auch vermehrt Daten übertrug, und so die Kommunikation fester Bestandteil in der IT wurde. Diese Vereinigung des Vernetzungsaspektes schuf auch neue Herausforderungen an die Informationen, die durch dieses technologische System zu verarbeiten waren.

Diese Entwicklungen verdeutlicht der Begriff **Cybersecurity** nun plakativer. Alles und jedes, jede mit jedem ist vernetzt, neue Anwendungsdomänen kamen auf, etwa Internet of Things (IoT), soziale Medien und Smart Solutions. Zusätzlich verschwammen die zeitlichen und organisatorischen Grenzen zwischen Privat und Arbeitsleben, eine klare Unterscheidung in Arbeits- und Freizeit geriet zum schwierigen Unterfangen für die NutzerInnen, wie auch der Umgang mit persönlichen und beruflichen Daten.

Im deutschen Sprachraum hat man sich zwar schon früh mit dem Thema **Datenschutz** auseinandergesetzt, auf europäischer Ebene wurden dieses Thema durch die General Data Protection Regulation (GDPR) abgedeckt und in Österreich und Deutschland gelten gelten sehr hohe Maßstäbe durch die Datenschutz-Grundverordnung (DSGVO) [8]. Angesichts des ursprünglichen Aufkommens von neuen Geschäftsmodellen mit Daten ab Mitte der 2000er-Jahre, die von TeilnehmerInnen an Services zur Verfügung gestellt wurden und deren Aufbereitung zum kommerziellen Vorteil genutzt wurden, war dies eher spät, wenngleich durchaus richtungsweisend. In zeitlicher Nähe zu den 2010er-Jahren wurde Privacy auch als wesentlicher Baustein der Sicherheit etabliert und durch die zunehmende Vernetzung naturgemäß wichtiger (vgl. Abschnitt 2.4). Diesen Strömungen musste der bisherige Sicherheitsaspekt nun ebenso Rechnung tragen.

Unter **Cyberspace** wird die virtuelle Welt, der generelle digitale Aktionsraum, verstanden. Dieser muss auf mehreren Betrachtungsebenen analysiert werden, nämlich Technik, Prozesse und Akteure, sowohl vor- als auch nachgelagert sowie auch sämtliche damit im Zusammenhang stehenden Daten und verarbeitenden Systeme, die nicht mehr einzelne, sondern mehrere vernetzte Systeme darstellen. Daher reflektiert der Begriff

Cybersecurity auf die eklatant steigende Anzahl der Akteure und Services. Durch die damit einhergehende Öffnung der Flanken aus der Sicherheitsperspektive erkannten Cyberkriminelle, dass eine Menge Geld lukriert werden kann, etwa durch Ransomware [9]. Dabei werden die unterschiedlichsten Adressaten angesprochen, also Einzelpersonen, Organisationen, öffentliche Verwaltung, bis hin zu Staaten und supranationalen Vereinigungen.

Die Bedeutung von **Cyberdiplomatie** im globalen Kontext ist wohl die bislang jüngste Evolutionsstufe. Durch den Grad der Durchdringung und somit Abhängigkeit der nationalen Gesellschaften von digitaler Infrastruktur steigt auch das Bedrohungsbild auf politischer Ebene, was sich in gezielte Desinformation („Fake News"), Angriffe gegen kritische Infrastrukturen oder staatliche Institutionen, die mitunter von Staaten geduldet oder sogar gefördert werden („Cyber Warfare") [10], manifestiert. Durch die Einsicht, dass Cybersecurity eigentlich ein komplettes IKT-Ökosystem adressieren muss und etwaige Beeinträchtigungen Schaden für alle daran beteiligten Akteure bewirkt, wird dieses zu einer multidimensionalen Querschnittsthematik [10].

Abbildung 1 veranschaulicht schematisch die Begriffsevolution der Sicherheitsaspekte in der IKT. Ausgehend vom technischen Begriff haben sich Information Security und Cybersecurity mit unterschiedlichen Schwerpunkten entwickelt. Daraus wird ersichtlich, dass sich Cybersecurity nur mit dem Schutz von digitalen oder elektronischen Daten befasst und Information Security sich auf den Schutz von sowohl physischen, elektronischen wie auch digitalen Daten fokussiert [11].

Abbildung 1: Begriffsevolution – IT-Security wird zu Information Security wird zu Cybersecurity

Seit den beginnenden 2020er-Jahren gewinnt der Begriff **Resilienz** immer mehr an Bedeutung. Es umfasst die Fähigkeit von IKT, bei (Teil-) Ausfällen oder Störungen von Komponenten, wesentliche Kernfunktionalitäten aufrechtzuerhalten und nur minimale Auswirkungen auf Geschäfts- und Betriebsprozesse zu haben [12]. Allerdings ist es allgemein als Widerstandsfähigkeit zu interpretieren, mit Krisen- oder Mangellagen umzugehen, ist also entsprechend weiter zu fassen als der IKT-Kontext. Resilienz hängt unmittelbar mit Cybersecurity zusammen, manche ExpertInnen sehen diesen sogar als eigenen Baustein dafür (vgl. Abschnitt 2.4). Aufgrund der Tatsache, dass Resilienz weniger als ein technologiefokussierter Begriff, sondern mehr verhaltensorientiert ausgelegt wird, stellt diese Arbeit die Resilienz als gleichbedeutendes Konzept der Cybersecurity dar. Resilienz kann durch Cybersecurity-Maßnahmen verbessert werden, kann aber ebenso ohne Cybersecurity die Widerstandskraft verbessern. In Kombination sind die beiden Begriffe als die aktuellen modernen Schlüsselinstrumente für eine aktive Gestaltung des digitalen Lebens unserer modernen Gesellschaft zu sehen.

2.2.2 Begriffsdefinition

Die Begriffsentwicklung von IT-Security bis hin zu Cybersecurity erfolgte fließend. Dadurch ist es schwierig zu bestimmen, wo das Thema Cybersecurity beginnt oder endet. Bei der Recherche nach einer Definition für den Begriff Cybersecurity wird deutlich, dass sich IKT-Experten und Organisationen, sowohl aus dem privaten wie auch dem öffentlichen Sektor, nicht immer einig sind, wie dieser Terminus genau definiert werden soll.

Die existierenden Begriffe haben nämlich unterschiedliche Konzentrationen oder befassen sich mit dem Thema aus unterschiedlichen Perspektiven, z.B. unternehmerische Sicht gegenüber der Sicht von Einzelpersonen. Aufgrund dessen können sich Begriffsdefinitionen über Cybersecurity stark voneinander unterscheiden.

So definiert zum Beispiel die US Cybersecurity & Infrastructure Agency (US-CISA), Cyber-Security als „*die Kunst Netzwerke, Systeme, Geräte, Daten und sensible Informationen vor unautorisiertem Zugang oder kriminellen Verwendungen zu schützen und die Vertraulichkeit und Verfügbarkeit von Informationen zu bewahren"* [13]. Der globale IT-Konzern IBM stellt fest, dass „*Cyber-Security-Maßnahmen darauf ausgelegt sind Bedrohungen gegen vernetzte Systeme und Anwendungen zu bekämpfen, unabhängig davon, ob diese von innerhalb oder außerhalb einer Organisation ausgehen"* [14]. Der EU-Cybersicherheitsakt besagt, dass „*Cybersicherheit nicht nur eine Frage der Technologie ist, sondern eine, bei der das menschliche Verhalten ebenso wichtig ist"* und beschreibt diesen Begriff als „*alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die NutzerInnen solcher Systeme und andere von Cyberbedrohungen betroffenen Personen zu schützen"* [15] [16].

Insbesondere Definitionen mit technischem Fokus wurden während der ExpertInnen-Interviews kritisiert, da sie wesentliche Teile, wie die sozialen und **menschlichen Komponenten**, auslassen. Es geht nämlich bei Cybersecurity nicht nur darum, die einzelnen Systeme und Daten zu schützen, sondern auch die NutzerInnen und alle jene, mit denen diese in Kontakt stehen. Aufgrund der immer weiteren Ausdehnung von digitalen Bereichen geht Cybersecurity über die klassischen, physischen Unternehmensgrenzen hinaus und es kommt zu einer Verschmelzung zwischen der beruflichen und privaten Welt. Daher ist es wichtig, dass diese Veränderungen und Akteure genauso berücksichtigt werden. Die oben genannte Definition aus dem EU-Cybersicherheitsakt versucht, die menschliche und soziale Komponente mehr miteinzubeziehen, schafft es aber trotzdem nicht zufriedenstellend, einen gelungenen Überblick auf dieses Thema zu geben, da sie sich zu wenig auf die technischen Aspekte bezieht.

Durch die angeführten Definitionen wird ersichtlich, dass Cybersecurity ein extrem breites Thema ist, bei dem man Gefahr läuft, in kurzen Definitionen wichtige Akteure oder Aspekte zu ignorieren. Der vorliegende Bericht legt den Begriff Cybersecurity so breit wie möglich aus, um möglichst viele Detailbereiche des Themas zu erfassen und thematisieren. Eine geeignete Arbeitsdefinition, die dafür herangezogen werden kann, stammt von der European Union Agency for Cybersecurity (ENISA). Die ENISA interpretiert den Begriff wie folgt: „*Cybersecurity umfasst alle Aktivitäten, die erforderlich sind, um den Cyberspace, seine Nutzer und die betroffenen Personen vor Cyber-Bedrohungen zu schützen, sowie alle Aspekte der Prävention, Vorhersage, Toleranz, Erkennung, Schadensbegrenzung, Beseitigung, Analyse und Untersuchung von Cyber-Vorfällen"* [17].

2.3 Spannungsfelder

2.3.1 Cybercrime

Ein Thema, welches oft im Zusammenhang mit Cybersecurity aufkommt, ist **Cybercrime**. Eine häufige Missinterpretation ist die Annahme, dass Cybersecurity eine reine Sammlung von Maßnahmen ist, um Cybercrime oder Cyberverbrechen zu verhindern. Cybersecurity, wie im vorhergehenden Abschnitt argumentiert, beschäftigt sich jedoch unter anderem mit dem Beschützen von Netzwerken, Systemen, Geräten, und deren Nutzern. Daher fokussiert sich Cybersicherheit ausschließlich auf die digitale Welt. Cybercrime hingegen zielt auf den Einsatz von technischen Hilfsmitteln im Cyberspace ab, um in der analogen oder „Offline-Welt" ein Verbrechen zu begehen [17]. Ein Beispiel für ein Cybercrime kann z.B. ein betrügerischer Telefonanruf sein. Es handelt sich bei Cybercrime also um konkrete Straftaten, bei denen die IKT zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird [18].

Nichtsdestotrotz überschneiden sich diese Begriffe oftmals. Bei Cybercrime mit Cybersecurity-Bezug handelt es sich z.B. um Angriffe auf Netzwerke, Software und Hardware durch den Einsatz von schädlichen Programmen, wie Ransomware oder Viren. Bei Cybercrime sind die Verbrechen allerdings meist deutlich weniger

technisch, da das Opfer im Normallfall die Person selbst und kein IKT-System ist. Beispiele für Cybercrime sind unter anderem Cybermobbing, Kinderpornografie oder Betrugsfälle.

Das Ziel von **Cyberattacken** ist in den meisten Fällen auf Daten zuzugreifen, diese zu verändern oder zu zerstören, Geld von BenutzerInnen zu erpressen oder die Dienstleistungen/Geschäftsunternehmen von Organisationen zu unterbrechen [19]. Cybersicherheitsmaßnahmen dienen dazu, das Erreichen der Ziele der AngreiferInnen zu verhindern.

In Österreich sind alle digitalen Bereiche potenziell gefährdet, Opfer eines Cyberangriffs zu werden und einige Unternehmen haben auch schon massive Schäden davongetragen. Erst im Juni 2021 wurde Salzburg Milch Opfer einer Cyberattacke. Das Unternehmen wurde am 22. Juni 2021 aufgrund eines Cyberangriffs lahmgelegt. Ein Angreifer hat sich dabei in die Systeme des Unternehmens gehackt, sämtliche Passwörter geändert und dadurch den Zugriff und Zugang auf alle IKT-Systeme und Server verschlüsselt, womit Salzburg Milch innerhalb kürzester Zeit betriebsunfähig wurde [20].

Doch es sind nicht nur Großunternehmen, welche sich vor solchen Attacken schützen müssen. Auch **kleine und mittlere Unternehmen** (KMU**)** müssen sich auf derartige Szenarien vorbereiten. In Oberösterreich haben es im September 2021 Hacker geschafft, mit nur einem Angriff auf einen IKT-Systemadministrator Zugriff auf die Systeme von 34 Klein- und Mittelbetriebe zu erlangen. Der Schaden für die einzelnen Unternehmen ist noch unklar [21], doch oftmals sind, laut den Interview-ExpertInnen, die Auswirkungen eines Cyberangriffs auf kleinere Betriebe eklatant und wirken sich auf deren weitere Existenz aus. So kann etwa die Betriebsunfähigkeit als Folge eines Cyberangriffes mehrere Tage oder gar Wochen dauern, was aufgrund der kleinen Budgets und Rücklagen der KMUs zu einer Zahlungsunfähigkeit bis hin zur Insolvenz führen kann.

Ein Beispiel für Cybercrime, welches in Österreich sehr häufig aufkommt, ist **Internetbetrug**. Von 2019 auf 2020 ist die Zahl an angezeigten Delikten um 26,3 Prozent gestiegen [22]. Beliebte Methoden für Internetbetrug sind unteranderem Fake-Online-Shops, bei denen Kunden für einen Service oder ein Produkt zahlen, das es gar nicht gibt, oder sogenannte „Romance Scams“, Betrugsfälle, bei denen mit Hilfe von Fake-Profilen in sozialen Medien Opfern eine Verliebtheit vorgespielt wird, um einen wirtschaftlichen Nutzen daraus zu ziehen.

2.3.2 Cyber Warfare

Durchaus martialisch mutet der Begriff **Cyber Warfare** an. Die Kriegsführung im virtuellen Raum hat aber durchaus ernstzunehmenden Charakter erhalten, wenn gezielt demokratische Institutionen oder kritische Infrastrukturen mit einem Cyberangriff aus dem Gleichgewicht gebracht werden sollen. Plakative Beispiele bilden dabei die vermutete Einflussnahme Russlands auf die Präsidentenwahlen 2016 in den USA [23] oder im selben Jahr auf das Brexit-Votum in Großbritannien [24]. Dazu gehören auch gezielte Desinformationskampagnen in Sozialen Medien oder gezielt gegründeten elektronischen Medienkanälen [25]. Hier zeigt sich deutlich eine neue politische Dimension, wenn Cybersecurity von Staaten nicht aktiv gelebt und gestaltet wird.

Die Ziele von staatlichen Cyberattacken sind meist **Militärspionage**, Beeinflussung der öffentlichen Meinung durch Desinformation, die über soziale Medien verbreitet wird, und die Manipulation von Entscheidungsprozessen der angegriffenen Regierung [26]. Cyber Warfare kann aber nicht nur die politische Beeinflussung oder Manipulation der Bevölkerung zur Folge haben. Es kann auch dazu führen, dass Regierungen die Grundrechte außerhalb der eigenen Grenzen massiv beeinträchtigen können. Im Jahr 2014 sorgte ein Angriff von nord-koreanischen Hackern auf Sony Pictures Entertainment dazu, dass das Unternehmen einen Satire-Film über den nord-koreanischen Diktator Kim Jong-Un nicht in die Kinos brachte, da der Angriff auf Sony eine enorme Menge an Daten löschte, geheime E-Mails von Firmenchefs und Hollywood Executives sowie Dateien veröffentlichte. Das Unternehmen musste offline gehen, bis sein Computernetzwerk wieder hergestellt war [27] [28].

Kritische Infrastrukturen sind ebenfalls beliebte Ziele von Cyber-Warefare, da man durch einen erfolgreichen Cyberangriff auf eine kritische Infrastruktur massive Disruptionen auslösen und wichtige Informationen erhalten kann. Im September 2021 erklärte, z.B., die norwegische Regierung, dass eine Reihe von Cyberangriffen auf private und staatliche IT-Infrastrukturen von schädlichen Akteuren ausging, die von China

unterstützt wurden und von dort aus operierten. Bei der Untersuchung der Hacks wurde in den Raum gestellt, die Akteure hätten versucht, geheime Informationen über Norwegens nationale Verteidigung und Sicherheitsinformationen zu erbeuten [29].

2.3.3 Technologieabhängigkeit

Gerade in der IKT ist die Abhängigkeit von Produkten, Technologien und Dienstleistungen aus dem US-amerikanischen und asiatischen Markt frappant. Hard- und Software werden großteils nicht mehr in Europa entwickelt; kurz- und mittelfristig ist ein „Backshoring" – also eine Verlagerung der Produktion ins Heimatland – auch nicht möglich. Daher ist die Sicherstellung des Wissens und das Bewahren des Verständnisses über die Technologie essenziell. Aus den ExpertInnen-Interviews ergab sich, dass es in dieser Situation wichtig ist, in Europa sowie in Österreich das obengenannte Verständnis aufzubauen, Cybersecurity-Knowhow zu entwickeln, das Wissen über Soft- und Hardware zu halten, um Produkte und das Geschäftsmodell von datenzentrieren Plattformen verstehen, validieren, überprüfen, sowie Abweichungen und Angriffe aus „eigener Kraft" noch erkennen zu können.

Im Zusammenhang mit der Technologieabhängigkeit wurde von den interviewten ExpertInnen sowie in der Diskussion im Workshop vielfach auch ein Mangel an österreichischen Cybersecurity-Unternehmen sowie Lösungsanbietern festgestellt. Auch hier sind Österreich und Europa von amerikanischen und asiatischen Lösungen abhängig. Die befragten ExpertInnen verweisen in diesem Zusammenhang auf ein fehlendes (Innovations-) Ökosystem für Cybersecurity-Unternehmen in Österreich sowie auf einen Mangel an Cybersecurity-Fachkräften angesichts erwarteter Nachfragesteigerung, eine Notwendigkeit für Kompetenz- und Kapazitätsaufbau, sowie der Bedarf nach effektiverer Unterstützung für Cybersecurity-Innovation und Markteinführung insbesondere im Bereich Risikokapital. Laut einer Studie der Industriellenvereinigung mangelt es an Risikokapitalgebern sowohl von staatlicher Seite als auch von institutionellen Anlegern [1]. Gleichzeitig herrscht laut ExpertInnen ein fehlendes Bewusstsein für Cybersecurity-Risiken und deren Auswirkungen. Dies beeinflusst die Nachfrage nach Lösungen und hat auch Auswirkungen auf die Anzahl von Cybersecurity-Lösungsanbieter.

2.4 Bedrohungslandschaft (Threat Landscape)

In der digitalen Welt gibt es wesentliche Bausteine für Sicherheit, die es zu schützen gilt. Diese lauten – in der Literatur mitunter auch nicht immer einheitlich genannt – wie folgt und sind in Abbildung 2 dargestellt:

- **Vertraulichkeit (Confidentiality)** ist die Gewährleistung der Sicherheit von gespeicherten Daten und die Sicherheit der Informationen der Datenübertragung. Es muss sichergestellt sein, dass vertrauliche Daten nicht in die falschen Hände fallen [30].
- **Integrität (Integrity)** bezeichnet die Nachvollziehbarkeit von vorgenommenen Änderungen an Daten. Da Daten immer einem gewissen Kreis von autorisierten Personen zur Verfügung stehen, kommt es regelmäßig zu Änderungen. Daher muss gewährleistet sein, dass für jede zugriffsberechtigte Person die Änderungen nachvollziehbar sind [30].
- **Verfügbarkeit (Availability)** repräsentiert die Eigenschaft, dass die gespeicherten Daten in einem größtmöglichen zeitlichen Rahmen verfügbar sind. Daher muss vermieden werden, dass Daten nicht mehr vorhanden sind oder nicht mehr darauf zurückgegriffen werden kann [30].
- **Authentizität (Authenticity)** verifiziert den Urheber von sensiblen Daten. Es darf unter keinen Umständen zu Zweifel am Urheber einer Datei kommen [30].
- **Nicht-Abstreitbarkeit (Non-Repudiation)**: darunter versteht man die Gewährleistung, dass der Versand und Empfang von Daten nachher nicht in Abrede gestellt werden kann. Dabei wird zwischen zwei Arten unterschieden [31]:
    - Nicht-Abstreitbarkeit der Herkunft: es soll einem Absender nicht möglich sein, das Absenden der Nachricht im Nachhinein zu bestreiten.

- Nicht-Abstreitbarkeit der Ankunft: es soll einem Empfänger nicht möglich sein, den Erhalt einer gesendeten Nachricht zu bestreiten.
- Ein weiteres Sub-Ziel, welches es bei der Nicht-Abstreitbarkeit zu schützen gilt, ist die Transparenz (Transparency). Transparenz verfolgt das Ziel, einen/eine NutzerIn zu informieren, was mit deren Daten geschieht, wie damit umgegangen wird und welche Personen Zugriff darauf hatten. Transparenz ist nicht nur ein Schutzziel, sondern auch eines der wesentlichen Ziele der General Data Protection Regulation (GDPR) [32].

- **Datenschutz (Privacy):** ist das Grundrecht von Personen auf informationelle Selbstbestimmung. Menschen haben dadurch selbst die Freiheit zu bestimmen, wie mit ihren Daten umgegangen wird und wer welche Informationen erhalten darf [33].

Abbildung 2: Cybersecurity Bausteine

Der Verlust einer oder mehrerer dieser Bausteine gehört zu den allgemeinen Grundbedrohungen („Threats“) der Informations- und Cybersicherheit. Im Falle einer Cyberattacke wird versucht, den Verlust von mindestens einem dieser Bausteine zu initiieren. Aus diesem Grund werden diese Bausteine auch als **Schutzziele** bezeichnet, da es erforderlich ist, diese Bausteine zu bewahren. Die Cybergefahren (ungerichtet, sind latent gegeben) oder Cyber-Risiken (gerichtet auf die betrachtete Organisation mit ihren Verwundbarkeiten), welche nachfolgend diskutiert werden, bedrohen diese Schutzziele und wodurch letztlich die Informationen oder Daten eines Opfers von AngreiferInnen kompromittiert werden können.

2.5 Top 5 Gefahren und Modus Operandi

Damit Cyberangriffe erfolgreich durchgeführt werden können, verwenden HackerInnen und AngreiferInnen Methoden und Techniken, die es ihnen ermöglichen, den Zugang zu den gewünschten Geräten, Netzwerken, etc. zu erhalten. Viele dieser Methoden wenden Social Engineering an. Hacker versuchen durch **Social Engineering**, Menschen so zu manipulieren, dass sie Standard-Sicherheitsverfahren brechen. Eine der häufigsten Taktiken besteht darin, jemanden glauben zu lassen, er würde jemandem in Not helfen. Eine AngreiferIn kann sich z.B. als MitarbeiterIn oder Familienmitglied ausgeben, um Zugang zu einem Dokument, einem Bankkonto oder sensiblen Daten zu erlangen [34].

Cyberangriffe und deren Methoden haben sich in den letzten Jahren stark entwickelt und sie wurden zu einer Gefahr für jeden Akteur, der sich innerhalb eines digitalen Netzes oder Systems bewegt. Es folgte auch eine

Professionalisierung der AngreiferInnen und deren Methoden. Eine gefährliche Technik in diesem Bereich sind **Advanced Persistent Threats** (APTs). APTs sind Cyberattacken welche ausgefeilte Hacking-Methoden verwenden um, sich Zugang zu einem System zu verschaffen und dort über einen längeren Zeitraum zu blieben, um Informationen zu stehlen. Eine APT-Attacke findet in unterschiedlichen Phasen statt, in denen die AngreiferInnen Zugang erlangen, sich im Ziel etablieren, indem sie sich Möglichkeiten schaffen, um sich unbemerkt im System bewegen zu können. Danach wird der Zugang ausgebaut und erweitert und die AngreiferInnen verschaffen sich Administrationsrechte, damit sie sich beliebig im Netzwerk bewegen können. Dadurch können die AngreiferInnen ein umfassendes Verständnis über das System und dessen Schwachstellen erhalten, was es ihnen ermöglicht, die gewünschten Informationen nach Belieben zu sammeln. Aufgrund des hohen Aufwands eines solchen Angriffs richten sich APTs in der Regel gegen hochrangige Ziele wie Staaten oder große Unternehmen [35]. Das bedeutet aber nicht, dass andere Akteure weniger gefährdet sind, Opfer eines Cyberangriffs zu werden, dass Cyberangriffe nur auf bestimmte Personengruppen abzielen, oder dass Durchschnittspersonen kaum von einer solchen Attacke gefährdet sind. Cyberangriffe haben sich zu einem globalen Geschäftsmodell entwickelt, welches für AngreiferInnen sehr lukrativ ist. AngreiferInnen benötigen kaum noch eigenes technisches Knowhow, da die Angriffsmethoden, Schadprogramme oder Software, etc. einfach käuflich zu erwerben sind. Diese Art von Cyberangriff ist als Attack-as-a-service bekannt, bei der sich AngreiferInnen Abonnements für Malware and Ransomware Toolkits kaufen können, wodurch sie ohne viel Aufwand ihre Attacken automatisieren und möglichst viele Akteure angreifen können [36]. Diese Kombination von Attack-as-a-Service und die sich immer ausweitende Vernetzung führt schließlich dazu, dass jeder Akteur, unabhängig davon, ob es sich dabei um eine einzelne Person oder ein Unternehmen handelt, ein Opfer einer Cyberattacke werden kann und auch damit rechnen muss, gehackt zu werden.

Die fünf häufigsten Methoden, die in diesem Zusammenhang für einen Cyberangriff verwendet werden, sind Malware, webbasierte Angriffe, Phishing, Angriffe auf Webanwendungen und Spam [37]. Diese werden im Folgenden näher beschrieben.

1. **Malware**

Das Wort Malware leitet sich vom Begriff „Malicious Software“ ab, der „schädliche Software“ bedeutet. Daher fällt unter diese Kategorie jegliche Art von Software, die unerwünschte Handlungen durchführt, wie z.B. Datendiebstahl. Es gibt unzählige Arten von solchen schädlichen Programmen. Allein in den letzten 10 Jahren sind mehr als 100 Millionen neu-entwickelte Schadprogramme dazugekommen und insgesamt gibt es sogar über 1 Milliarde Malware-Programme [38]. Die gängigsten Malware-Typen lauten wie folgt [39]:

- **Trojaner:** ist eine Form von Malware, welche sich als legitime Software ausgibt, um ein Opfer dazu zu bringen, sie zu installieren. Nachdem der Trojaner einmal installiert wurde, ist dieser in der Lage, schädliche Aktivitäten im Hintergrund durchzuführen.
- **Virus:** ist eine Form von Malware, welche sich an Programme, Files, oder Dokumente anhaftet und sich dadurch von einem Rechner (Workstation, Server, Client, Smartphone, Tablet) zum nächsten ausbreitet.
- **Wurm:** ist eine Form von Malware, die Ähnlichkeiten zu einem Virus hat. Deshalb wird ein Wurm auch oftmals als eine Virus-Unterklasse gesehen. Ein Wurm breitet sich von Rechner zu Rechner aus, besitzt aber die Fähigkeit, sich ohne menschliche Interaktion zu verbreiten. Er nutzt meistens Verwundbarkeiten, wie z.B. schwache Passwörter oder Schwachstellen in Betriebssystemen, um sich innerhalb eines Netzwerkes zu verbreiten.
- **Ransomware:** ist eine Form von Malware, die sich Zugang zu Systemen und Informationen verschafft und diese dann verschlüsselt, damit NutzerInnen nicht darauf zugreifen können. Der Angreifer verlangt meist Lösegeld (Ransom) für die Freigabe der Daten.
- **Spyware:** ist eine Form von Malware, bei der die Aktivitäten ohne das Einverständnis des/der NutzerIn beobachtet werden. Häufige Beobachtungsarten sind Keylogging, Activity Monitoring, Data Collection, und andere Arten von Datendiebstahl.

Malware kann zu einer Gefahr für jedes der sechs oben definierten Schutzziele werden, da AngreiferInnen abhängig vom Malware-Programm unbegrenzt Zugang zu den Daten und Systemen des Opfers haben können. TäterInnen wären somit in der Lage, Daten zu lesen, zu bearbeiten und zu löschen [40].

2. Webbasierte Angriffe

Webbasierte Angriffe sind Angriffsmethoden, bei denen AngreiferInnen versuchen, Opfer zu täuschen, indem sie Websysteme und -services verwenden. In diese Kategorie der Cyberattacken fällt eine große Anzahl an Angriffen, wie z.B. den User auf bestimmte, schädliche Websites zu leiten. Die häufigsten Arten von webbasierten Angriffen lauten wie folgt:

- **Drive-By Downloads:** diese Art von Angriff lädt schädliche Inhalte auf das Gerät des Opfers. Damit solch ein Angriff erfolgen kann, müssen NutzerInnen eine legitime Webseite besuchen, die kompromittiert wurde. Das können AngreiferInnen erreichen, indem schädliche Skripte in die legitime Webseite einfügt werden, sogenannte browser-basierte „Exploits" ausgeführt werden oder das Opfer auf eine zuvor kompromittierte Seite umgeleitet wird.
- **Watering Hole Attacks:** ist eine gezielte Angriffsart, welche sich auf eine bestimmte BenutzeInnen-Gruppe fokussiert. Dabei werden Webseiten, die von der betroffenen Gruppe häufig besucht werden, komprimiert, um diese Personen dann zu einer schädlichen Webseite zu locken. Oftmals wird diese Art von Angriff mit Spam-E-Mails kombiniert, um die Wahrscheinlichkeit, dass eine Person eine schädliche Webseite aufruft, zu erhöhen.
- **Formjacking:** fokussiert sich hauptsächlich auf Bank- und andere personenbezogene Daten. Bei dieser Attacke fügen AngreiferInnen einen schädlichen Code in die Zahlungsformulare einer legitimen Webseite ein. Wenn NutzerInnen dann ihre Informationen in das Formular eingeben und absenden, werden diese Daten durch den schädlichen Code sowohl an das Webseiten-Portal sowie an die AngreiferInnen geschickt. AngreiferInnen sind dadurch in der Lage, die gewonnen Informationen für kriminelle Zwecke zu verwenden.
- **Malicious URL:** diese Angriffsart besteht aus einem Link, der erstellt wurde, um Malware zu verbreiten oder sonstige Betrugsarten zu ermöglichen. Dieser Angriff beinhaltet unter anderem Social Engineering, um das Opfer dazu zu verleiten, auf den Link zu klicken, der die Malware lädt, oder den Rechner des Opfers durch sonstige schädliche Inhalte kompromittiert.

Aus den gerade eben genannten Angriffsarten wird klar, dass webbasierte Angriffe zum gleichzeitigen Verlust mehrerer Schutzziele führen können. Unter anderem haben solche Attacken zur Folge, dass ein Opfer einen Verlust von Datenschutz, Vertraulichkeit und Integrität befürchten muss, da personenbezogene Daten abhandenkommen und diese dann zu dem Verlust von weiteren Bausteinen führen können [41].

3. Phishing

Phishing ist eine Form des Social-Engineering-Angriffs und tritt auf, wenn AngreiferInnen falsche Identitäten verwenden, um jemanden dazu zu verleiten, vertrauliche Informationen bereitzustellen, Malware herunterzuladen oder eine Website mit Malware zu besuchen. Einer der häufigsten Phishing-Angriffe verwendet E-Mails als Angriffsvektor. AngreiferInnen erstellen z.B. eine E-Mail, die aussieht, als käme sie von einer vertrauten Organisation und fordert NutzerInnen darin auf, eine Website zu besuchen und den Benutzernamen und das Kennwort einzugeben, um das potenzielle Opfer zur Preisgabe von Informationen, z.B. Bank- oder Anmeldedaten, zu bringen [42].

Aus diesem Grund sind Phishing-Attacken, wie auch Malware-Angriffe, in der Lage, einen Verlust von jedem der sechs Schutzziele zu erzwingen. AngreiferInnen können nämlich mit den gestohlenen Daten Zugang zu weiteren Informationen erlangen und diese dann nach Belieben verändern, bearbeiten, etc. oder sogar Nachrichten im Namen des Opfers versenden.

4. Angriffe auf Webanwendungen

Angriffe auf Webanwendungen sind von den fünf häufigsten Angriffen die komplexeste Form der Cyberattacke. Webservices und Applikationen hängen hauptsächlich von Datenbanken ab, um Informationen zu speichern oder bereitzustellen. Daher konzentrieren sich Angriffe dieser Art meistens auf die Manipulation solcher Datenbanken. Des Weiteren versuchen AngreiferInnen häufig, Webseiten mit Hilfe von schädlichen Skripten zu kompromittieren. Häufige Arten von Angriffen auf Webanwendungen sind unter anderem [43]:

- **SQLi-Angriffe:** SQLi steht für SQL-Injection. SQL ist eine der verbreitetsten Datenbanksprachen, welche zum Aufbau von Datenstrukturen in Datenbanken sowie zum Bearbeiten und Abfragen von

Datensätzen verwendet wird. Ein SQLi-Angriff ist eine Cyberangriffsmethode, bei der AngreiferInnen SQL-Anweisungen an Datenbanken richten, um eine Datenbank zu manipulieren und Zugang zu potenziell wertvollen Informationen zu erhalten. [44]Um eine solche Attacke durchzuführen verwenden AngreiferInnen meist Webformulare von legitimen Webseiten und injizieren ihre SQL-Befehle, um die Ausführung vordefinierter SQL-Befehle zu beeinflussen [44]

- **Cross-Site-Scripting-Angriffe (XSS):** sind eine Angriffsart, bei den schädlichen Skripten – Listen mit Befehlen, die von einem Programm ausgeführt werden – in eine vertrauenswürdige und legitime Webseite injiziert werden. XSS-Attacken treten auf, wenn eine AngreiferIn eine Webanwendung nutzt, um schädlichen Code an einen User zu senden [45].XSS-Attacken treten auf, wenn eine AngreiferIn eine Webanwendung nutzt, um schädlichen Code an einen User zu senden [45].

Diese Form von Cyberangriffen kann wie die vorherigen Arten einen negativen Effekt auf jedes einzelne Schutzziel haben, da der schädliche Code, welcher an die User weitergeleitet wird, dem Angreifer alle Möglichkeiten bieten kann, um die Daten des Opfers zu verwenden und missbrauchen.

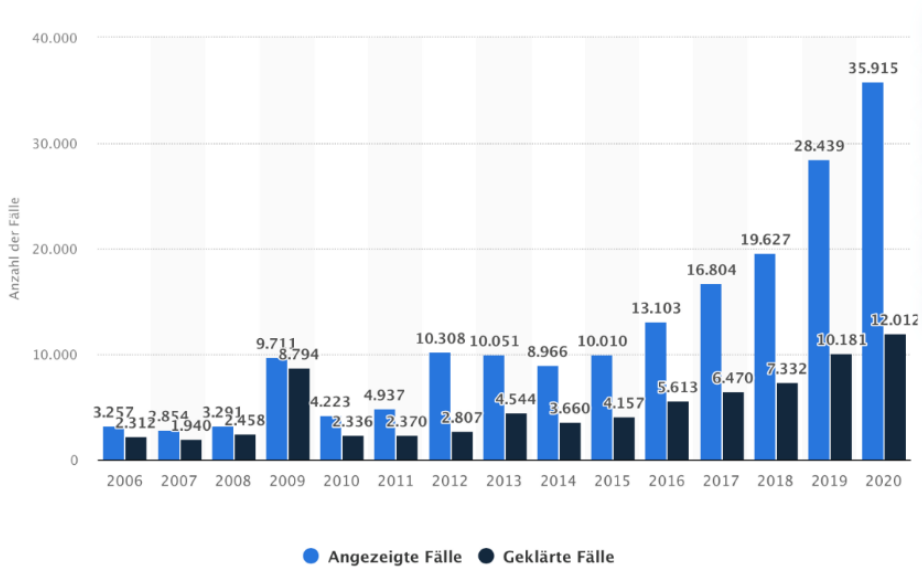
5. **Spam**

Als Spam wird jede Art von ungewollter und unaufgeforderter digitaler Kommunikation verstanden, die in Massen versendet wird. Oftmals wird Spam als E-Mail verschickt, kann aber auch als SMS, Telefonanruf oder via soziale Medien versendet werden. Spammer (jene Personen, die Spam verschicken) verwenden daher viele Kommunikationsformen, um ihre Nachrichten zu verbreiten. Dabei kann es sich sowohl um Marketingnachrichten handeln als auch um Nachrichten, um Malware zu verbreiten oder um Phishing-Attacken auszuführen. Spam-Attacken können ebenfalls zu einem Verlust eines Schutzziels führen, da der Inhalt einer Spam-Nachricht frei gestaltbar ist. Es könnte sich dabei um eine einfache Werbe-E-Mail handeln, aber auch um eine schädliche Software, welche sich nach dem Öffnen auf dem Rechner installieren kann [46].

2.6 Trendanalyse

Wie in den obigen Abschnitten beschrieben, kam es in den letzten Jahren zu einem weltweiten Anstieg an Cyberangriffen. Dieses Problem hat sich vor allem aufgrund der Covid-19-Pandemie und der damit einhergehenden Digitalisierung noch rasanter entwickelt hat. Auch in Österreich fallen immer mehr Privatpersonen und Unternehmen solchen Angriffen zum Opfer. Obwohl letztes Jahr die Gesamtkriminalität noch um 11,3 % gesunken ist, verzeichnete die Cyberkriminalität einen Anstieg von 26,3 % [47], wohingegen die Menge an geklärten Fällen vergleichsweise konstant bleibt, wie in Abbildung 3 zu sehen ist.

Abbildung 3: Entwicklung von Cyberangriffen 2006-2020



Quelle: Statista.com

So geben etwa 38 % der heimischen Unternehmen an, eine Zunahme an Cyberangriffen festgestellt zu haben. 60 % der Unternehmen wurden sogar Opfer einer Cyberattacke in den letzten zwölf Monaten. Die größten Gefahren für Unternehmen, Opfer eines Cyberangriffes zu werden, sind veraltete Systeme, fehlerhafte Software, die Manipulation der Mitarbeiter durch Social Engineering und unzureichend geschützte mobile Endgeräte und Apps [5].

Einen massiven Anteil an diesem Problem hat die Entwicklung von herkömmlichen, gezielten Cyberangriffen zu dem Attack-as-a-Service Model, was auch von mehreren ExpertInnen bestätigt wurde. Dieser Trend ermöglicht es AngreiferInnen, mit geringem technischem Knowhow in dem lukrativen Feld der Cyberkriminalität mitzumischen. Doch auch der rasche, von Covid-19 angetriebene digitale Wandel hatte zur Folge, dass die Gefahr, Opfer eines Cyberangriffs zu werden, gestiegen ist, da es den TäterInnen eine nochmals größere Angriffsfläche bietet. Angestellte waren gezwungen, ihre Arbeit von den offiziellen, zutrittsgesicherten Büros in ihre privaten Wohnsitze zu verlagern. Das führte zu einer exorbitanten Anzahl von vernetzen externen Standorten, welche bei weitem nicht so gut geschützt sind wie traditionelle Bürostandorte, die über sicherere Firewalls, Router und eine von den Sicherheitsteams des Unternehmens betriebene Zugangsverwaltung verfügen.

Das Remote-Arbeiten hat neue Möglichkeiten für AngreiferInnen kreiert, um die Schwächen der Geräte und Netzwerke in den **Home-Offices** auszunutzen [26]. Laut dem Institut der deutschen Wirtschaft (IW) kam es wegen Hackerangriffen auf Menschen im Home-Office bei deutschen Firmen zu Schäden von € 52 Mio. Aufgrund dessen bezeichnet das IW das Home-Office als „Geschenk für Cyberkriminelle“, weil die Verbindungen, die Angestellte Zuhause verwenden leichter angegriffen werden können als Firmennetzwerke. Außerdem mangelt es an Schulungen und Sicherheitskonzepten, was zu einem noch höheren Risiko für Firmen und deren Angestellten führt [48].

Des Weiteren ist das **Internet of Things** (IoT) eine Entwicklung, dessen Ausbreitung in den letzten Jahren ein Mitgrund für die erhöhte Anzahl an Cyberangriffen ist. Durch die geschätzt 50 Milliarden verbundenen Geräte und die darin verbauten Sensoren erhalten Hacker eine erkleckliche Auswahl an Optionen, die Cyberabwehr dieser Geräte zu durchbrechen, um an persönliche Daten zu kommen. Die exponentielle Konnektivität des IoT ist ein sich ständig ausweitendes Netz von Netzwerken und Geräten [26].

Ein nach wie vor beliebtes Tool für Cyberangreifer sind soziale Medien. Diese Seiten sind aus mehreren Gründen eine große Hilfe für Hacker. Erstens ermöglichen Facebook und Co es den Angreifern, ihre Opfer gründlich zu studieren, was es deutlich leichter macht, gezielte Attacken auszuüben. Laut dem Singapore Computer Emergency Response Team posten 84 % der NutzerInnen von sozialen Medien mindestens einmal

die Woche, wovon die Hälfte dieser Gruppe sogar täglich persönliche Informationen teilt [49]. Das macht es noch einfacher, die größere Angriffsfläche auszunutzen. Zweitens sind soziale Medien auch ein optimaler Ort, um Desinformationen zu verbreiten. Fake News und die Manipulation der öffentlichen Meinung wird von vielen als die Nummer 1 Cyber-Gefahr gesehen und wie auch bei den Cyberattacken zeichnet sich hier ein beängstigender Trend ab [50]: Disinformation-for-hire ist ein Modell, bei dem Akteure dafür bezahlen, falsche Informationen zu verbreiten. So wurde etwa im Mai 2021 mehreren französischen und deutschen Influencern von einer Public Relations Agency aus London Geld geboten, damit sie über ihre Kanäle Unwahrheiten über den Covid-19 Impfstoff von Pfizer-BioNTech verbreiten [51].

2.7 Abschätzung zukünftiger Entwicklungen

Nach dem Blick auf die momentanen Trends ist es sinnvoll, eine Abschätzung der zukünftigen Entwicklungen zu machen. Laut ENISA ist in den nächsten Jahren mit signifikanten Änderungen bezüglich Cybersicherheit oder Sicherheit im Cyberspace zu rechnen. Der Schutz dieses komplexen Umfelds wird aufgrund der immer mehr mit Kommunikationstechnik verbundenen Menschen, Rechner und Systeme immer schwieriger. Außerdem wird die heutige Gesellschaft laufend abhängiger von dieser Vernetzung, die bis in alltägliche Aktivitäten reich. Dadurch nehmen auch die Möglichkeiten für schädliche Akteure zu, den Cyberspace zu verwenden, um Individuen und Organisationen zu manipulieren, auszunutzen, oder zu täuschen [52]. Außer der in Abschnitt 2.6 besprochenen Ausweitung der Digitalisierung und Vernetzung gibt es noch weitere gefährliche Entwicklungen, die beobachten werden, müssen. Es kann diesbezüglich zwischen technischen und menschlichen Entwicklungen unterschieden werden.

Eine große Herausforderung für die Zukunft von Cybersecurity wird die Erkennung jener Bedrohungen, die **Künstliche Intelligenz** (KI) oder Artificial Intelligence (AI) nutzen, um einen Angriff zu starten oder eine Identifikation zu vermeiden. KIs lösen Probleme anders als Menschen, sie können deutlich mehr potenzielle Lösungen identifizieren und entdecken eher komplexe Lösungswege als ihre menschlichen Gegenspieler. Hinzu kommt, dass KIs weniger eingeschränkt sind. Sie können daher die Geschwindigkeit und den Umfang des Hackens verändern, und zwar in einem Tempo und Ausmaß, auf das die Gesellschaft noch nicht vorbereitet ist [53].

Ein weitere Technologie-Entwicklung, die es zu beachten gibt, sind **Quantencomputer**. Die Gefahr, die von dieser Technologie ausgeht, ist, dass Angreifer und sogar Regierungen sensible und verschlüsselte Daten in der Hoffnung sammeln, diese in der Zukunft mit Hilfe von Quantencomputern entschlüsseln zu können. Quantencomputer verwenden andere physikalische Prinzipien als klassische Computer, wodurch sie bestimmte Aufgaben und Problemstellungen deutlich schneller lösen können als moderne Computer. So wäre es mit Hilfe von Quantencomputern möglich, Verschlüsselungsmethoden in ein paar Tagen zu knacken, wohingegen die heutigen Supercomputer das nicht einmal in tausend Jahren schaffen würden [54]. Auch wenn diese Technik noch am Anfang steht, kostenintensiv ist und vor vielzähligen Problemen in der praktischen Anwendung steht, muss eine Auseinandersetzung mit diesem Thema stattfinden, damit versucht werden kann, die damit einhergehende, potenzielle Langzeit-Gefahr zu minimieren [55].

Die menschlichen Entwicklungen beziehen sich – anders als die hier bereits diskutierten Technologien – vermehrt auf **NutzerInnen** als auf AngreiferInnen. Der erste Aspekt ist der Wechsel von technischen zu menschlichen Hacks. Social Engineering ist aufgrund der sich immer ausweitenden Vernetzung beliebter geworden. Viele der in 2.5 besprochenen Angriffsmethoden verwenden z.B. Social Engineering, um NutzerInnen dazu zu bringen, auf einen Link zu klicken oder eine E-Mail zu öffnen. Auch in diesem Bereich gibt es immer neue Mittel, die verwendet werden, um Personen zu hacken und zu manipulieren. Eine ernstzunehmende Bedrohung auf diesem Gebiet, die in Zukunft immer mehr Beachtung finden wird, sind **Deep Fakes**. Der Begriff Deep Fake ist eine Kombination aus den Begriffen "Deep Learning" und "Fake" und verweist auf eine KI-basierte Technologie, mit der Bilder, Audio- und Videodateien erstellt oder verändert werden, um falsche Inhalte zu erzeugen, die jedoch authentisch erscheinen. Dies kann von der Nachbildung einer Stimme am Telefon, die wie ein CEO oder CFO klingt, der um eine Geldüberweisung bittet, bis hin zur Darstellung eines genauen Abbilds einer Person in einem Video reichen. Sie können in Echtzeit oder in aufgezeichneten Medien verändert werden [56].

2.8 Cybersicherheit in österreichischen Unternehmen

Wie in Abschnitt 2.6 erwähnt nehmen Cyberattacken auch in Österreich stetig zu und heimische Unternehmen sind von diesem Problem besonders stark betroffen. Die häufigste Gefahr stellen dabei Phishing-Angriffe auf Organisationen, gefolgt von CEO-Fraud/Business-E-Mail-Compromise, eine Betrugsmethode bei dir sich AngreiferInnen als Mitarbeiter oder CEO eines Unternehmens ausgeben, um an Daten zu gelangen, und Malware-Angriffen. Die Auswirkungen im Falle einer erfolgreichen Attacke können für Unternehmen verheerende Folgen haben, da diese zu Unterbrechungen ihrer Geschäftsprozesse und geschäftsbedingendem Imageverlust führen kann.

In den letzten Jahren haben sich österreichische Unternehmen vermehrt auf Cyberkriminalität vorbereitet und es kam auch zu einer stetigen Erhöhung des **Cybersecurity-Budgets** von Unternehmen. Durch die Covid-19-Pandemie kam es noch zu einem zusätzlichen Digitalisierungsschub, wodurch sich die Bedeutung von Cybersecurity in Unternehmen nochmals verändert hat. Deshalb haben im vergangenen Jahr zirka 75 % der Unternehmen ihr Budget für Cybersecurity nochmals erhöht und 20 % investieren 3 % - 5 % des jährlichen IKT-Budgets in die Cybersicherheit ihres Unternehmens. Auch in Österreichs höchsten Unternehmensebenen wird Cybersecurity vermehrt thematisiert und sogar das Interesse der Mitarbeiter wächst. So möchte rund ein Drittel mehr zu diesem Thema wissen, wie aus dem jährlichen Cybersecurity Bericht von KPMG hervorgeht [5]. Des Weiteren haben fast drei Viertel der Unternehmen in Österreich mindestens eine/einen dezidierten Cybersecurity-MitarbeiterIn und jedes fünfte Unternehmen plant die Rolle einer solchen Position. Nur 12 % sind der Meinung, dass sie keine dezidierte Rolle für Cybersecurity benötigen [5].

Auch wenn 89 % der österreichischen Unternehmen den eigenen Cybersicherheits-Schutzmaßnahmen vertrauen, fehlt es dennoch einigen Betrieben am angemessenen Bewusstsein. Vor allem gibt es enorme Unterschiede zwischen Großunternehmen und kritischer Infrastrukturen im Vergleich zu KMUs. Während Großunternehmen sich vermehrt mit diesem Thema beschäftigen, vernachlässigen KMUs das Thema Cybersicherheit, auch wenn ganz genau diese besonders stark von einer erfolgreichen Attacke betroffen wären. Nur 8 % der KMUs vertrauen den Sicherheitsmaßnahmen ihrer Lieferanten und Cloud-Dienstleister. Gleichzeitig investieren aber nur 19 % in die Risikobereiche, die durch Drittparteien, wie etwa Lieferanten oder (Cloud-) Dienstleister entstehen. Der Grund dafür ist, dass einige Unternehmen wegen der Auslagerung ihrer Dienstleistungen ein fehlendes Pflichtbewusstsein haben und die Verantwortung über Cybersicherheit an ihre externen Partner übergeben [57].

Hinsichtlich **Cyberversicherungen** sind österreichische Unternehmen auch noch zurückhaltend: Nur ein Viertel besitzt eine Versicherung gegen Cyberangriffe und weniger als die Hälfte bereiten sich nicht auf die finanziellen Auswirkungen, die zu erwartenden Aufwände und Kosten eines Cyberangriffs vor [57].

Ein weiteres Problem für viele österreichische Betriebe ist, dass es in Österreich einen Mangel an ExpertInnen gibt und es daher schwierig wird, mit der ständig wachsenden Nachfrage an Cybersecurity-MitarbeiterInnen zu befriedigen. Auf den Mangel an Cybersecurity-ExpertInnen wurde mehrfach in Interviews und im Workshop hingewiesen. Es wird zudem erwartet, dass sich der Fachkräftemangel in Zukunft aufgrund der größeren Nachfrage nach Cybersecurity-Dienstleistungen noch verstärken wird. Schon jetzt fehlen laut einer Studie des Industrie Wissenschaftliches Instituts rund 24.000 IT-Fachkräfte [58]. Darüber hinaus wurde von den interviewten ExpertInnen und im Workshop auch ein Bedarf nach mehr Cybersecurity-Dienstleistern identifiziert. Außerdem gibt es trotz des vergleichbar erhöhten Cybersicherheits-Bewusstseins von Unternehmen immer noch einige, die tatsächliche Angriffe verschweigen, wodurch die Bekämpfung von Cyberkriminalität zusätzlich erschwert wird [1].

2.9 Zusammenfassung und Fazit

- Die sich immer ausweiternde Vernetzung und Digitalisierung unserer Gesellschaft verdeutlicht die Vielschichtigkeit des Begriffs Cybersecurity. Dieser entwickelte sich über die letzten drei Dekaden stetig weiter. Ausgehend von einer rein technischen Auffassung aus der IT-Security entstanden Information Security für die klassische Informationsverarbeitung und OT-Security aus IKT-gesteuerten Produktions- und Fertigungssystemen innerhalb von definierten Organisationsgrenzen. Cybersecurity steht schließlich für umfassenden **Schutz des digitalen Lebens**. Viele der Definitionen von Cybersecurity greifen allerdings (zu) kurz, da sich dieses im Kern technische Thema durch die voranschreitende Digitalisierung zu einer komplexen Problematik entwickelt hat, die im Sinne einer Querschnittsmaterie de facto alle gesellschaftlichen Lebensbereiche und Akteure betrifft. Cybersecurity ist daher ein wesentliches Instrument, um Sicherheit im digitalen Raum zu generieren und die Auswirkungen auf die analoge Welt zu minimieren.
- Cybersecurity basiert auf der Stärkung der **Sicherheitsziele** Vertraulichkeit (Confidentiality), Integrität (Integrity), Verfügbarkeit (Availability), Authentizität (Authenticity), Nicht-Abstreitbarkeit (Non-Repudiation), Datenschutz (Privacy). Bedrohungen (Threats) nutzen etwaige Verwundbarkeiten (Vulnerabilities) aus, um digitale Systeme und Daten zu kompromittieren.
- Der Cyberspace ist dadurch gekennzeichnet, dass Europa und Österreich **abhängig von Technologien** sind, die vielfach zur Gänze aus den USA und Asien, insbesondere China, stammen. Die Notwendigkeit eines umfassenden Kompetenz- und Innovations-Ökosystem für Cybersecurity kann eine proaktive gestalterische Handlungsoption für Österreich darstellen.
- Die fünf häufigsten **Methoden**, die **für einen Cyberangriff** verwendet werden, sind Malware, webbasierte Angriffe, Phishing, Angriffe auf Webanwendungen und Spam. Der Trend für Cyberangriffe zeigt eindeutig auf eine deutliche Zunahme von Vorfällen und auf zunehmende Schäden für die heimische Wirtschaft. Neue, sehr viel einfacher zu nutzende Methoden („Attack-as-a-Service“, „Deep Fakes“, Künstliche Intelligenz), neue Technologien (Quantencomputer) und die Kommerzialisierung von Cybercrime („Ransomware“) machen dieses Feld für AngreiferInnen sehr attraktiv. Durch die hochgradige Vernetzung aller Akteure sind staatliche Institutionen, Wirtschaftstreibende bis hin zu Einzelpersonen betroffen. Der Mensch ist vielfach jener Angriffsvektor, der für die AngreiferInnen am einfachsten zu überwinden und somit am verwundbarsten ist.
- **Resilienz und Cybersecurity** sind jene Stellschrauben für politische Handlungsschwerpunkte, die direkt zum Schutz der Gesellschaft – im digitalen und damit unmittelbar in der analogen Welt – beitragen. Die größten **Risiken** liegen in der Technologieabhängigkeit, der Komplexität von Cybersecurity, den immer ausgereifteren Angriffsmethoden und den fehlenden IKT-Fachkräften in Österreich.
- In Österreich gibt es einen massiven **Mangel an IKT-Fachkräften**. 60 % der österreichischen Manager antworteten im österreichischen Infrastrukturreport 2021, dass es nicht ausreichend Fachkräfte im Telekommunikations- und Informationstechnologiebereich gibt. 91 % der Befragten fordern, dass der Fachkräftemangel im IKT-Bereich dringend gelöst werden muss, da in Österreich 24.000 Fachkräfte fehlen [58] und ohne die notwendigen ExpertInnen eine effektive Adressierung des steigenden Risikos schwierig wird.

3. Gesellschaft und Digitalisierung

3.1 Einleitung

Die fortschreitende Digitalisierung hat unsere Gesellschaft nachhaltig verändert. Das Internet als eine der zentralen Technologien der letzten Jahrzehnte hat eine scheinbar unendliche Fülle an Informationen verfügbar gemacht und erlaubt es, nahezu verzögerungsfrei über Textnachrichten, Audio und Video mit anderen in Verbindung zu treten. Nicht nur ist das Internet Dreh- und Angelpunkt unserer zwischenmenschlichen Kommunikation geworden, sondern es ist auch zentrale Infrastruktur in allen Gesellschaftsbereichen.

Zwar ermöglichen immer leistungsfähigere Technologien neue digitale Hilfsmittel in fast jeder Lebenslage, gleichzeitig steht die Gesellschaft aber vor nie dagewesenen Herausforderungen, was die Sicherheit und Resilienz digitaler Systeme und Netzwerke betrifft. Cybersecurity bezieht sich dabei nicht nur auf das Verhindern vorsätzlicher Cyberattacken, sondern auch auf die zahlreichen anderen vielschichtigen Risiken für AnwenderInnen und Gesellschaft. Dazu zählen etwa Bedenken zum Datenschutz und der Privatsphäre, wenn AnwenderInnen mit einer stetig wachsenden Zahl an Kameras, Mikrofonen und Sensoren ausgestattet sind, oder die befürchteten Einschränkungen der Entscheidungs- und Meinungsfreiheit, wenn durch automatisierte Systeme der Informationsstrom zunehmend personalisiert und gefiltert wird.

Das vorliegende Kapitel widmet sich einer Auswahl von Anwendungsbereichen digitaler Technologien, die aktuell und für die weitere Zukunft für Cybersecurity besonders relevant erscheinen. Ziel ist es, einen Überblick über aktuelle Cybersecurity-Themen in verschiedensten Anwendungsbereichen zu bieten und anhand der Themensammlung sowie den Ergebnissen aus Interviews und Workshops aktuelle und zukünftige gesellschaftliche Anforderungen an Cybersecurity zu identifizieren. Die Themenauswahl erfolgte durch Recherche in einschlägigen Medien, Technologie-Foresight-Berichten sowie Publikationen und Medienberichten mit Fokus auf Cybersecurity und verwandten Themen. Abschnitt 3.2 behandelt die Anwendungsbereiche digitaler Technologien mit aktueller Cybersecurity-Relevanz. In Abschnitt 3.3 erfolgt die Exploration aktueller und zukünftiger gesellschaftlicher Anforderungen an Cybersecurity auf Basis der Ergebnisse aus Interviews und Workshops.

3.2 Digitale Technologien und Cybersecurity-Risiken

3.2.1 Splinternet und Netzneutralität

Hinter den für NutzerInnen einfachen Vorgängen – die URL in die Adressleiste eingeben, Begriffe auf Google suchen, oder einen Beitrag auf Facebook markieren („liken“) – bestehen oft **intransparente Netzwerkstrukturen und Algorithmen**, die von verschiedenen gewinnorientierten oder politischen Interessen beeinflusst werden. Dies bedeutet, dass nicht jeder Inhalt für alle NutzerInnen gleichermaßen verfügbar ist. Das sogenannte Splinternet (von „splinter“ für splittern) bezeichnet die Realität eines **fragmentierten Internets**, in der einzelne Websites oder ganze Teilbereiche nicht für alle zugänglich sind. China etwa setzt zur Überwachung und Zensur des Internets eine landesweite Firewall ein, die regierungskritische oder für unsittlich befundene Inhalte gänzlich sperrt [59].

Zudem kann der Internetzugang selbst, also die Kosten und Leistungsfähigkeit der Internetanbindung entscheidend beeinflussen, ob und welche Inhalte verfügbar sind. Die **Netzneutralität** ist in einigen Ländern gefährdet, da Internetprovider bestimmte Inhalte oder Services bevorzugt behandeln, etwa durch höhere Geschwindigkeiten oder geringere Kosten für NutzerInnen. Die Netzneutralitätsverordnung gibt dabei in der EU den Rahmen für diskriminierungsfreien Datenverkehr vor [60], wird jedoch oft als zu wenig umfassend kritisiert.

Neben nationalen und strukturellen Unterschieden im Internetzugang ist weiters entscheidend, ob Internetseiten über herkömmliche Browser und Suchmaschinen erreichbar sind. Im Gegensatz zum sichtbaren

Internet (auch „Clear Web“) wird das sogenannte Deep Web und das **Darknet** unterschieden. Das Deep Web ist zwar Teil des normal zugänglichen Internets, wird allerdings nicht von Suchmaschinen indexiert oder nur eingeschränkt zugänglich und so für die Öffentlichkeit nur eingeschränkt sichtbar. Das Deep Web beinhaltet etwa Online-Speicher, Datenbanken oder Streaming-Server. Das Darknet hingegen ist nur durch die Nutzung spezieller Software oder Netzwerkkonfigurationen zugänglich. Anders als im herkömmlichen Internet ist Kommunikation im Darknet anonym, bietet somit zwar einerseits die Möglichkeit der freien Meinungsäußerung speziell in Ländern mit starker Zensur des Internets, wird jedoch auch häufig als Plattform für kriminelle Aktivitäten angesehen [61].

3.2.2 Filterblasen: Automatisierte Content Curation und Moderation

Auch bei uneingeschränktem Internetzugang sind Informationen nicht für alle NutzerInnen gleichermaßen verfügbar. Suchmaschinen und soziale Netzwerkewie Google oder Facebook, die als private Unternehmen am Markt auftreten, sammeln detaillierte Daten über NutzerInnen und lernen aus deren Verhalten. In Folge werden automatisiert Inhalte präsentiert, die als besonders „relevant“ eingestuft werden. Diese sogenannten **Filterblasen** sind in der Regel gewinnorientiert, d.h. sie priorisieren Inhalte, die durch möglichst viele Klicks Werbeeinnahmen generieren [62]. Besonders aus Sicht des Datenschutzes und der Informations- und Meinungsfreiheit werden diese Entwicklungen kritisch beurteilt. Ein durch Sperren oder Filterblasen fragmentiertes Internet verhindert, dass BürgerInnen auf einen objektiven Querschnitt der verfügbaren Information zugreifen können, und legt detaillierte Informationen über das Verhalten und die Interessen von Nutzerinnen in die Hände einiger weniger Organisationen [63] [64].

Soziale Medien, insbesondere Facebook und Twitter, sind in den letzten Jahren zunehmend aufgrund der dort verbreiteten Desinformation und manipulativen Inhalte kritisiert worden. Die Priorisierung von Inhalten, die besonders viele Interaktionen generieren, gehört zum Geschäftsmodell der meisten sozialen Medien, um die auf den Plattformen verbrachte Zeit maximieren und gezielt personalisierte Werbung schalten zu können. Durch die automatisierte Content Curation, also die Vorauswahl von Inhalten meist ohne Prüfung auf Qualität oder Wahrheitsgehalt, werden den NutzerInnen Inhalte präsentiert, mit denen sie mit hoher Wahrscheinlichkeit interagieren, diese also etwa weiterverbreiten oder kommentieren. Dadurch verbreiten sich emotionalisierende und polarisierende Inhalte, etwa Hass-Botschaften und Verschwörungstheorien, besonders schnell [65]. Zudem entstehen durch die personalisierte Vorauswahl von Inhalten Filterblasen und Echokammern, die die eigenen Ansichten konsequent bestätigen. Durch die mangelnde Diversität an Informationen und Meinungen können so NutzerInnen sukzessive radikalisiert werden [63] [66].

Soziale Medien werden zudem gezielt ausgenutzt, um den öffentlichen Diskurs zu lenken oder sogar den Ausgang von Wahlen zu beeinflussen, wie der Skandal um die Daten von Cambridge Analytica eindrücklich zeigt [67] [68] [69]. In Myanmar befeuerte gezielte **Desinformation** auf Facebook – aufgrund des kostenlosen Zugangs für viele BürgerInnen Myanmars die einzig verfügbare Form des Internetzugangs – die Gewalt gegen die ethnische Gruppe der Rohingya [70]. Zudem werden soziale Medien als wichtiger Treiber von Desinformation und Verschwörungstheorien zur Covid-19-Pandemie gesehen [71].

Neben der Verfügbarkeit von Information kann auch das Recht auf freie Meinungsäußerung durch automatisierte Filterung von Inhalten eingeschränkt werden. Die meisten sozialen Netzwerke und Content-Plattformen wie Google, Facebook und Twitter setzen zur Filterung anstößiger oder illegaler Inhalte und zur Wahrung des Urheberrechts **Algorithmen** ein. Durch die hohe Fehleranfälligkeit der Algorithmen und kaum vorhandene Einspruchs- oder Berufungsmöglichkeiten können jedoch auch legale und regelkonforme Inhalte oder NutzerInnen dauerhaft blockiert werden [63]. Zudem verstehen Filteralgorithmen keinen Kontext oder sprachliche Nuancen und diskriminieren oft gegen marginalisierte Gruppen. So werden etwa Tweets von Afroamerikanern häufiger als anstößig klassifiziert als andere Tweets [72].

3.2.3 Cloud

Cloud Services erlauben, dass persönliche Daten auf externe Server ausgelagert werden und auf mehreren Endgeräten synchronisiert werden. Anbieter wie Dropbox, Google, Apple und Microsoft bieten teilweise kostenfreie oder im Gerätekauf inkludierte Services an, welche die Sicherung von Gerätebackups, Fotos, Musik

und Dokumenten ermöglichen. Dies bedeutet, dass viele AnwenderInnen viele oder sogar alle ihre persönlichen Daten auf Servern im Ausland gesichert haben, und ihre Daten möglichen Cyberattacken ausgesetzt sind. Trotz aller Sicherheitsvorkehrungen berichten Medien regelmäßig über **Datenlecks und Hacks**, wie etwa der Angriff auf Apples iCloud-Service im Jahr 2014, der laut Apple mittels gezielter Phishing-Attacken gelungen ist und durch den unzählige private Fotos von Prominenten im Internet verbreitet wurden [73]. Zudem ist der Datenschutz im Sinne der DSVGO insbesondere bei Cloud-Services in Drittstaaten aufgrund der Möglichkeiten der Rechtsdurchsetzung gegenüber innereuropäischer Datenverarbeitung geschwächt [74] [75].

Cloud-Services können auch **Ermittlungsbehörden** den Zugriff auf Daten erleichtern. Während in den USA der CLOUD Act die Herausgabe von Daten regelt – ein Gesetz, das in starkem Widerspruch zur europäischen DSVGO steht [76] – wird auch in der EU an einer Verordnung gearbeitet, die die Herausgabe von Daten an Strafverfolgungsbehörden regelt. Die „E-Evidence-Verordnung" wird jedoch aufgrund möglicher Grundrechtsverstöße kritisiert [77]. Oft entscheiden allerdings technische Schutzvorrichtungen, insbesondere die fachgerechte Verschlüsselung von Daten, ob und mit welchem Aufwand Behörden Daten nutzen können. In den USA etwa können Berichten zufolge Behörden aufgrund fehlender Verschlüsselung vollständige iPhone-Backups einsehen [78]. Besondere Zugriffsrechte für Behörden „durch die Hintertür" können zudem die Sicherheit der Cloud-Daten gegenüber unautorisierten Akteuren und Cyberkriminellen kompromittieren [79]. Das Dilemma zwischen Verbrechensbekämpfung und Privatsphäre zeigt sich besonders deutlich in der aktuellen Debatte um Apples automatischen Scan aller in der Cloud gespeicherten Fotos nach Bildern von Kindesmissbrauch. Apple möchte dieses System nun erweitern und auch auf Geräten lokal nach Missbrauchs-Bildern suchen. Obwohl die Suche nicht auf den Bildern selbst, sondern auf digitalen Fingerabdrücken („Hashes") der Bilder basiert, befürchten Kritiker, dass solche Systeme einer immer weitläufigeren Überwachung Tür und Tor öffnen [80].

3.2.4 Mobilität, Navigation und Ortungsdienste

Fahrzeuge haben sich in den letzten Jahrzehnten immer weiter zu (selbst)fahrenden IKT-Systemen weiterentwickelt. Als Ersatz für physische Schalter gewinnt der Bildschirm und das Entertainment-System immer mehr an Bedeutung, für das Fahrzeughersteller eigene Benutzeroberflächen und Systeme entwickeln. Zudem bieten einige Systeme die Integration mit Apples CarPlay oder Googles Android Auto und sind über das Mobilfunknetz dauerhaft mit dem Internet verbunden. Auch die Schließsysteme moderner Fahrzeuge sind digital: Diese entriegeln die Türen mittlerweile automatisch mit dem Smartphone über Bluetooth oder Ultrabreitband. Die Steuerung zentraler Funktionen, einschließlich Gas, Bremse, und Lenkung erfolgt mittlerweile oft vollständig rechnergestützt. Zudem verfügen neuere Fahrzeugmodelle über zahlreiche Sensoren, etwa Radar, Kameras (teilweise im Innenraum), Mikrophone, Global Positioning System (GPS), Reifendrucksensoren und Motor- und Abgassensoren, die Komfort, Sicherheit und Effizienz der Fahrzeuge erhöhen.

Neben Spurhalte- und Notbremsassistenten wird auch die Entwicklung selbstfahrender Fahrzeuge weitergetrieben. Tesla etwa bietet für Fahrzeuge einen semi-autonomen Fahrmodus an, und hat kürzlich eine Beta-Version der vollständig autonomen (Full Self Driving) Software veröffentlicht [81]. Die immer komplexeren IKT-Systeme, die direkten Zugriff auf die **Fahrzeugsteuerung** haben, bieten allerdings attraktive Angriffsflächen für Hacker: Am Beispiel eines Teslas gelang es Hackern, mittels Drohne die Türen eines Fahrzeuges zu öffnen [82]. Zudem konnten Hacker die komplette Kontrolle über einen Tesla übernehmen [83], und auch für andere Hersteller liegen ähnliche Berichte vor [84] [85]. Die zahlreichen Sensoren und Online-Anbindung von PKWs werden auch genutzt, um Daten über FahrerInnen zu sammeln. Um selbstfahrende Software und Sicherheitssysteme weiterzuentwickeln, landen deshalb auch Aufnahmen direkt beim Fahrzeughersteller [86].

Neben Fahrzeugen sind mittlerweile nahezu alle Smartphones und viele Smart Devices mit GPS-Empfängern ausgestattet. In Kombination mit Navigationsdiensten wie Google Maps erlaubt dies die Wegführung in Echtzeit mit verschiedensten Fortbewegungsmitteln, einschließlich der **Routenplanung** mit öffentlichen Verkehrsmitteln. Während der Benutzung von Ortungsdiensten am Smartphone – je nach Einstellungen sogar im Hintergrund – zeichnet etwa Google mit seiner App detaillierte Daten über die Bewegungen der NutzerInnen auf, einerseits, um die Services zu verbessern (etwa die Optimierung der Routen und die automatische

Stauumfahrung), andererseits, um personalisierte, situationsabhängige Werbung anzuzeigen [87]. Bei den meisten Online-Diensten ist es zudem aufgrund komplizierter Datenschutzbestimmung (Privacy Policies) für NutzerInnen schwer nachzuvollziehen, welche Daten tatsächlich gesammelt werden und wie diese weiterverarbeitet werden [88].

Ein weiterer, relativ neuer Anwendungsbereich der GPS-Funktion von Smartphones liegt in eigenen **Ortungsgeräten** (Tracking Devices), die selbst nicht auf GPS oder Mobilfunk angewiesen sind, sondern sich automatisch über Bluetooth mit nahegelegenen Smartphones verbinden. Smartphones übermitteln dann an das Ortungsnetzwerk ihren Standort. Im Fall von Apples Produkt AirTags können die Tracker auf ein umfangreiches Netzwerk aus iPhones geortet werden, was je nach iPhone-Dichte eine fast lückenlose Überwachung erlaubt. Aufgrund der geringen Größe, langen Lebensdauer der Batterie, und einfachen Anwendung werden die Geräte zum dauerhaften Tracken persönlicher Gegenstände beworben [89]. Neben allgemeinen Bedenken zum Datenschutz wird aus denselben Gründen befürchtet, dass die Tracker ohne jeglichen Aufwand zum Stalking missbraucht werden können. Apple verspricht, dass die Geräte mit Sicherheitsvorkehrungen ausgestattet sind, die den Missbrauch der Geräte verhindern sollen: Wenn sich ein fremder AirTag mit jemandem mitbewegt, warnt nach gewisser Zeit das eigene iPhone – sofern man denn eines besitzt. Zudem beginnt der Tracker einen Warnton abzuspielen. Der Zeitraum bis zur Warnung beträgt jedoch zwischen 8 und 24 Stunden, und Versuche zeigen, dass der Lautsprecher eines AirTags leicht deaktiviert werden kann [90].

3.2.5 Online-Shops und Bewertungsplattformen

Nicht erst durch die zunehmende Bedeutung des Versandhandels während der Covid-19-Pandemie wächst der Umsatz von Online-Shops stetig. In Österreich belief er sich im Jahr 2019 auf bereits 10 % des Umsatzes im gesamten Einzelhandel [91]. Die Hälfte des Umsatzes fällt auf die zehn größten Anbieter, angeführt von Amazon [92]. Während ÖsterreicherInnen insbesondere Elektronik und Bekleidung online einkaufen [93], wird auch für Lebensmittel großes Wachstum prognostiziert [94]. Zudem werden Essensbestellungen, Restaurantreservierungen, Tickets für Veranstaltungen und Transportmittel, sowie viele andere Dienstleistungen immer häufiger online gebucht.

Es erfolgt jedoch nicht nur der Kauf, sondern auch die Produktrecherche und -auswahl sowie der Preisvergleich immer öfter online. Online-Bewertungen spielen in diesem Prozess eine zentrale Rolle, obwohl Onlineshops und Bewertungsplattformen oft mit gefälschten **Rezensionen** zu kämpfen haben [95]. Insbesondere Amazon als weltweit größter Onlineshop scheint immer öfter mit gefälschten Produktbewertungen und Manipulationen des Empfehlungssystems zu kämpfen [96]. Bewertungs- und Empfehlungsplattformen für Hotels oder Restaurant bleiben von gefälschten Bewertungen ebenfalls nicht verschont. Als eindrückliches Beispiel der Anfälligkeit für Plattformen wie TripAdvisor schaffte es ein Londoner, ein erfundenes Restaurant zum besten Lokal der Stadt zu machen, ohne, dass er jemals eine einzige Speise serviert hat [97].

Unter den Sammelbegriffen **Online-Reputationsmanagement** und Electronic Word of Mouth versteht man die Bemühungen von Unternehmen, auf Bewertungsplattformen, in sozialen Medien und anderen Online-Quellen möglichst viel positiven Diskurs über das Produkt oder Service zu generieren [98] [99]. Oft werden dafür auch bekannte Online-Persönlichkeiten, also Influencer, mit Produkten versorgt oder für Werbeeinschaltungen bezahlt. Der Übergang zwischen objektiven Tests und bezahlter Werbung ist allerdings fließend und das Manipulationspotenzial entsprechend hoch [100].

3.2.6 Personalisierte Werbung und dynamische Preisgestaltung

Online und im physischen Einzelhandel nimmt das Sammeln von Daten stetig zu. Es wird das Verhalten von NutzerInnen auf sozialen Medien, Suchmaschinen durch Cookies verfolgt mit dem Zweck, auf die Situation und Person angepasste Werbung einzublenden [101]. Daten werden allerdings nicht nur online gesammelt, auch im physischen Einzelhandel wird mittels Kundenkarten das Einkaufsverhalten aufgezeichnet. Diese Daten ermöglichen dann ein detailliertes **Profiling** der KundInnen, personalisierte Werbung und maßgeschneiderte Angebote, die per Post oder elektronisch zugestellt werden. Aufgrund mangelnder Transparenz über diese Methoden geriet kürzlich der Jö-Bonusclub ins Visier der österreichischen Datenschutzbehörde [102].

Dynamische personalisierte **Preisgestaltung** geht noch einen Schritt weiter als Werbung: Je nach Profil, Such- und Einkaufsverhalten werden KonsumentInnen unterschiedliche Preise angezeigt [103]. Wenn man zu lange eine bestimmte Flugverbindung sucht, kann es etwa passieren, dass plötzlich der Preis der Tickets steigt [104]. All diese Entwicklungen der personalisierten, auf Überwachung basierten (surveillance-based) Werbung und Preisgestaltungen werden nicht nur aus Datenschutz- und Privatsphäregründen kritisch gesehen, sondern auch, weil sie die Entscheidungsfreiheit durch maßgeschneiderte Manipulation einschränken kann [105]. Zudem wurden bei automatischen Algorithmen für die Preisgestaltung – etwa bei Krediten oder Hypotheken – Diskriminierung zwischen verschiedenen Gruppen von KonsumentInnen beobachtet [106]. Die genannten Methoden stehen zudem oft nur großen Händlern offen, was zu unfairen Marktverhältnissen und einer weiteren Monopolisierung führen kann [107].

3.2.7 Dark Patterns

Dark Patterns (versteckte Muster) bezeichnen eine Vielzahl verschiedener Methoden, die bei der Gestaltung meist digitaler Inhalte und Benutzeroberflächen zur Anwendung kommen, um NutzerInnen zur Wahl der von den Systementwicklern erwünschten Option bewegen, jedoch den Interessen der AnwenderInnen selbst zuwiderlaufen. Es handelt sich dabei um Gestaltungselemente, die sich psychologische und verhaltensökonomische Erkenntnisse zu Nutze machen, um Menschen gezielt zu manipulieren, ohne dass diese jedoch sofort Verdacht schöpfen. Oft wird die Abwahl von Cookies, Werbung, kostenpflichtigen Zusatzdiensten, und der Einwilligung zur Speicherung personenbezogener Daten unnötig verkompliziert [108].

Als typisches manipulatives Gestaltungselement wird vom Entwickler die erwünschte Eingabe durch einen auffälligen Button angeregt, während die alternative Auswahl klein, schwer erkennbar, oder an einer unerwarteten Position ist. Eine andere, oft verwendete Taktik ist es, den Prozess des Kaufens oder Bestellens so einfach wie möglich zu gestalten, jedoch das Abbrechen, Stornieren oder Kündigen von Käufen oder Abonnements zu erschweren [109]. Viele Online-Shops etwa, darunter auch Amazon, verwenden Dark Patterns um das Kaufverhalten zu lenken [110]. Ein Abonnement der New York Times kann mit wenigen Klicks abgeschlossen werden, zum Beenden des Abos muss man jedoch mit dem Kundendienst Kontakt aufnehmen [111].

3.2.8 Zahlungsverkehr

Obwohl gerade Österreich als Land der BarzahlerInnen bekannt ist, hat die Digitalisierung auch hierzulande nicht vor dem Zahlungsverkehr Halt gemacht: 2021 nutzten bereits 71 % der Bevölkerung Online-Banking [112]. Durch den potenziellen Schaden bei Cyberattacken sind zwar die Sicherheitsvorkehrungen bei **Online-Banking**-Systemen deutlich erhöht, Cyberkriminelle haben jedoch immer wieder Erfolg, BankkundInnen Login-Informationen und Passwörter mittels **Phising**-Nachrichten abzuluchsen. Mittels gefälschter Mitteilungen der Bank werden AnwenderInnen etwa aufgefordert, sich in ihrem Account anzumelden, um eine Sperrung des Kontos zu verhindern. Der Link der Nachricht führt allerdings auf eine gefälschte Login-Seite, die der echten Website der Bank zum Verwechseln ähnlich sieht [113]. Altmodisch mutet die Methode an, Kartenleser an Bankomaten anzubringen, um Daten und PIN-Codes der NutzerInnen zu stehlen – sogenannte Karten-Skimmer [114]. Allerdings sind Bankomaten auch anfällig für Cyberattacken über das Netzwerk und dürften häufig schwerwiegende Schwachstellen aufweisen [115].Obwohl gerade Österreich als Land der BarzahlerInnen bekannt ist, hat die Digitalisierung auch hierzulande nicht vor dem Zahlungsverkehr Halt gemacht: 2021 nutzten bereits 71 % der Bevölkerung Online-Banking [112]. Durch den potenziellen Schaden bei Cyberattacken sind zwar die Sicherheitsvorkehrungen bei Online-Banking-Systemen deutlich erhöht, Cyberkriminelle haben jedoch immer wieder Erfolg, BankkundInnen Login-Informationen und Passwörter mittels Phising-Nachrichten zu stehlen. Mittels gefälschter Mitteilungen der Bank werden AnwenderInnen etwa aufgefordert, sich in ihrem Account anzumelden, um eine Sperrung des Kontos zu verhindern. Der Link der Nachricht führt allerdings auf eine gefälschte Login-Seite, die der echten Website der Bank zum Verwechseln ähnlich sieht [113]. Altmodisch mutet die Methode an, Kartenleser an Bankomaten anzubringen, um Daten und PIN-Codes der NutzerInnen zu stehlen – sogenannte Karten-Skimmer [114]. Allerdings sind Bankomaten auch anfällig für Cyberattacken über das Netzwerk und dürften häufig schwerwiegende Schwachstellen aufweisen [115].

Als etwas andere digitale Revolution des Zahlungsverkehrs werden seit einigen Jahren **Kryptowährunge**n diskutiert, digitale „Währungen“, die über Blockchains dezentral Transkationen, Vermögen und deren Besitzer speichern. Im aktuellen Boom der Kryptowährungen zeigte sich neben den Befürchtungen des Missbrauchs für Geldwäscherei und andere illegale Transaktionen [116] erneut eine weitere Schattenseite der alternativen Zahlungsmittel, nämlich ihr massiver Energiebedarf. Bei Kryptowährungen muss für jede Transaktion eine Rechenaufgabe gelöst werden. Das sogenannte Mining bezeichnet das Zurverfügungstellen von Computern zur Verarbeitung der Transaktionen, für die je nach Rechenleistung ein gewisser Betrag der Kryptowährung anfällt. Je populärer und dadurch intensiver eine Kryptowährung gehandelt wird, desto größer wird allerdings der Rechen- und somit Energieaufwand, um Transaktionen zu verarbeiten. Hierfür kommen deshalb sogar spezialisierte Rechenzentren zum Einsatz, mit entsprechend hohem Energiebedarf. Schätzungen zufolge konsumiert nur die Kryptowährung Bitcoin jährlich 92 Terawattstunden Strom [117], deutlich mehr als die etwa 70 Terawattstunden, welche ganz Österreich in einem Jahr verbraucht [118].

3.2.9 Arbeit und Bildung

Nicht zuletzt durch die Covid-19-Pandemie sind digitale Informationskanäle aus der Arbeits- und Bildungswelt nicht mehr wegzudenken.

Ein Großteil der österreichischen Berufstätigen, Schüler und Studierenden hat 2020 und 2021 regelmäßig von Zuhause aus gearbeitet oder gelernt, und in vielen Organisationen hat das **Home-Office** dauerhaft Einzug gehalten [119] [120]. Die wichtigste Grundlage dieser Entwicklungen sind dabei digitale Kommunikationskanäle, denn neben E-Mail und Telefon wäre effizientes Arbeiten und Lernen ohne benutzerfreundliche und stabile Services für etwa Videokonferenzen und Filesharing kaum möglich. Microsoft etwa bietet die Software Teams an, mit der Online-Besprechungen abgehalten, Nachrichten ausgetauscht und Dateien in Echtzeit kollaborativ bearbeitet werden können [121].

Die umfassende Nutzung der mitunter sehr komplexen Anwendungen bietet eine Vielzahl von Angriffsflächen und potenziellen Fehlerquellen. Sie setzt deshalb einen verantwortungsvollen Umgang mit den Services und entsprechende Sicherheitsvorkehrungen nicht nur durch die NutzerInnen, sondern auch durch die IT-Abteilung der Organisation voraus [122]. Gleichzeitig werden die Daten der Dienste oft hochgradig zentralisiert in der Cloud (siehe Abschnitt 3.2.3), etwa über Server im Ausland, ausgetauscht, was Bedenken über Datenlecks und die Verletzungen der Privatsphäre verschärft.

Telearbeit und E-Learning werfen dabei auch Fragen zum **Datenschutz** der EndanwenderInnen gegenüber der Organisation auf, da die Nutzung digitaler Kommunikationskanäle und die Aktivitäten auf Organisationsgeräten (etwa der Schullaptop oder das Arbeitshandy) bis zu einem gewissen Grad überwacht werden kann. Besonders problematisch scheint dabei die Nutzung privater Geräte, oft Bring Your Own Device (BYOD) genannt. Zur Wahrung gewisser Sicherheitsstandards und für den Zugriff auf das Organisationsnetzwerk bieten viele Serviceprovider und Entwickler von Betriebssystemen ein **Device Management** (Geräteverwaltung) für alle gängigen Betriebssysteme an. Microsofts Device Management erlaubt etwa, dass Organisationen die installierten Apps auf dem privaten Smartphone einsehen kann [123]. Das E-Learning stellt zudem ganz eigene Herausforderungen an Bildungseinrichtungen und Lehrende, insbesondere wenn es um die Anwesenheitskontrolle und Leistungsbeurteilung geht. So stellt sich etwa die Frage, inwieweit zur Online-Prüfungsaufsicht Webcam-Videos aufgezeichnet werden dürfen [124].

3.2.10 Smart Home und Smart Devices

Smart Devices sind mittlerweile allgegenwärtig. Mobiltelefone sind hochentwickelten Computern für die Hosentasche gewichen, die mit einer Vielzahl an **Sensoren**, enormer Rechenleistung und verschiedenen Netzwerkschnittstellen ausgerüstet sind. Fast alle handelsüblichen Smartphones verfügen über mehrere Kameras, Mikrophone, einen Bewegungssensor, GPS sowie Bluetooth, Wireless Local Area Network (WLAN) und natürlich Zugriff auf das mobile Internet. Moderne Geräte etwa von Apple besitzen mittlerweile sogar 3D-Scanner (light detection and ranging, LIDAR) [125] und Ultra-Breitband-Sender zur genaueren Ortung in der unmittelbaren Umgebung [126]. Ähnliche Entwicklungen sind auch im Haushalt zu beobachten: Viele Geräte, etwa elektrische Zahnbürsten, Alarmanlagen, Türschlösser oder Lampen sind mit komplexen

Computersystemen und Sensoren ausgestattet und an das Internet angebunden [127].) und natürlich Zugriff auf das mobile Internet. Moderne Geräte etwa von Apple besitzen mittlerweile sogar 3D-Scanner (light detection and ranging, LIDAR) [125] und Ultra-Breitband-Sender zur genaueren Ortung in der unmittelbaren Umgebung [126]. Ähnliche Entwicklungen sind auch im Haushalt zu beobachten: Viele Geräte, etwa elektrische Zahnbürsten, Alarmanlagen, Türschlösser oder Lampen sind mit komplexen Computersystemen und Sensoren ausgestattet und an das Internet angebunden [127].

Entsprechend der Vielzahl der Systeme sind auch die potenziellen Angriffsflächen der Smart Devices fast unüberschaubar. Sofern die Software der Geräte vom Hersteller gepflegt wird, werden durch regelmäßige Updates Sicherheitslücken und Softwarefehler behoben. Nicht selten bleiben Schwachstellen lange Zeit unbekannt. **Zero-Day-Exploits** bezeichnen dabei besonders schwerwiegende Schwachstellen, nämlich solche, die weder der Öffentlichkeit noch dem Hersteller bekannt sind, und somit von potenziellen Angreifern ausgenutzt werden können, selbst wenn Geräte auf letztem Stand sind [128]. Immer wieder werden für Geräte und Betriebssysteme Updates veröffentlicht, die zuvor länger bestehende Zero-Day-Exploits beheben. Die Veröffentlichungen der Organisation Zero Day Initiative machen deutlich, wie viele Schwachstellen regelmäßig von ForscherInnen entdeckt werden. Für Microsoft etwa veröffentlichte die Organisation alleine im Jahr 2021 bereits über 150 Schwachstellen in Betriebssystemen oder Anwendungen [129]. Wie auch in anderen Bereichen, in denen persönliche Daten oft in der Cloud gesichert werden oder der Hersteller detaillierte Nutzungsdaten einsehen kann, werden Smart Devices auch aus Datenschutzgründen kritisch gesehen [127].

3.2.11 Gesundheit

Smart Devices und Sensoren sind auch aus dem Gesundheitssektor nicht mehr wegzudenken. Besonders die **Wearables**, also Geräte, die am Körper getragen werden, haben sich in den vergangenen Jahren zu Health Monitors, also Geräten zur Gesundheitsüberwachung, entwickelt. Apple und Samsung etwa vermarkten die Apple Watch oder die Galaxy Watch als Plattform zur umfassenden Überwachung von Gesundheitsindikatoren, etwa der Pulsfrequenz, der Schlafqualität, des Blutsauerstoffgehalts, der sportlichen Betätigung und sogar des Elektrokardiogramms [130] [131]. Für zukünftige Iterationen der Geräte werden zudem Sensoren für Blutzucker und Körpertemperatur prognostiziert [132] [133]. Durch diese neuen Geräte sind Daten über den eigenen Körper verfügbar, die zuvor nur durch spezialisierte Geräte oder medizinisches Fachpersonal erhoben werden konnten. Diese werden nun – wenig überraschend – meist über das Internet synchronisiert und in der Cloud gesichert, mit allen damit einhergehenden Risiken.

Nicht nur Gesundheitsindikatoren, sondern auch Daten über den eigenen **genetischen Code** werden über das Internet versandt und zentral gespeichert. Services zur Verwandtschaftsbestimmung und Ahnenforschung, oder zur Diagnose von Krankheiten, scheinen jedoch manchmal einen laxen Umgang mit diesen hochempfindlichen Daten zu pflegen. So wird in Österreich etwa auch der pränatale Gentest „Nifty“ von der chinesischen Firma BGI Diagnostics angeboten. Es gibt jedoch Befürchtungen, dass die Daten vom chinesischen Konzern gesammelt und für „Bevölkerungsforschung“ verwendet werden [134] oder das Unternehmen gar mit dem chinesischen Militär zusammenarbeitet, auch wenn BGI dies dementiert [135].

3.2.12 Produktion

Der Begriff Industrie 4.0 soll die vierte industrielle Revolution nach der Dampfmaschine, der technologischen Revolution und der digitalen Revolution signalisieren. Industrie 4.0 bezieht sich dabei insbesondere auf die Adaptierbarkeit und Flexibilität von Produktionsprozessen durch Automatisierung und Interkonnektivität [136]. Tatsächlich zeigt sich, dass in Produktion und Lieferketten digitale Systeme, Smart Devices, Sensoren und künstliche Intelligenz eine immer wichtigere Rolle spielen. Das **Internet of Things** (IoT) bezeichnet dabei die zunehmende Vernetzung von virtuellen Systemen und physischen Objekten. Im Smart Farming etwa kommen immer öfter ferngesteuerte oder autonome Maschinen im Ackerbau zum Einsatz, und Sensoren und Geräte übernehmen vollautomatisiert die Futterausgabe in der Tierhaltung [137]. Die starke Vernetzung und Internetanbindung dieser digitalen Lösungen stellen allerdings auch ein beachtliches Risiko dar, denn sie ermöglichen Angriffe auf empfindliche Strukturen und Prozesse aus der Ferne und erfordern ein beachtliches Ausmaß an Wartung und Administration. Als jüngere Beispiele für die Anfälligkeit von IoT dienen etwa

Ransomware-Angriffe auf eine Pipeline sowie auf den weltweit größten Fleischproduzenten der USA, die hohe wirtschaftliche Schäden verursachten [138] [139].

3.2.13 Kritische Infrastruktur

Kritische Infrastrukturen, also Einrichtungen und Versorgungssysteme, die wesentliche Bedeutung für die Sicherheit und das Wohlergehen der Gesellschaft haben, sind in immer größerem Ausmaß von digitalen Systemen und Netzwerken abhängig. Internet und Telekommunikation selbst stellen bereits kritische Infrastrukturen dar, hängt doch das Funktionieren von vielen Informations-, Kommunikations- und Steuerungskanälen vom reibungslosen Funktionieren der zugrundliegenden Netzwerke ab. Durch die fortschreitende Digitalisierung der klassischen kritischen Infrastrukturen, wie etwa die Energie- und Wasserversorgung, Lieferketten im Lebensmittelhandel, Transport und Verkehr oder das Finanzwesen, ergeben sich zudem auch neue, spezifische Angriffsflächen und potenzielle Anfälligkeiten der Systeme [140] [141].

Smart Grids und Smart Meters beispielsweise, also intelligente Stromnetze und Verbrauchszähler, erlauben die effiziente Messung und Steuerung auf Verbraucher- und Erzeugerseite. Durch die Starke Vernetzung der Systeme und ihre zentralisierte Steuerung könnten jedoch Systemfehler oder Hacks weitreichende Konsequenzen für die Stromversorgung haben [142]. Zudem erlaubt die starke Vernetzung der Systeme, wie am Beispiel von Smart Meters, Verbrauchs- und Verhaltensdaten von Haushalten in beispiellosem Detailgrad zu erfassen. Kritik zum Datenschutz und der Privatsphäre wurden laut, und in einigen Ländern wurden bereits besondere Regeln zum Umgang mit Verbrauchsdaten erlassen [143]. Smart Grids und Smart Meters beispielsweise, also intelligente Stromnetze und Verbrauchszähler, erlauben die effiziente Messung und Steuerung auf Verbraucher- und Erzeugerseite. Durch die starke Vernetzung der Systeme und ihre zentralisierte Steuerung könnten jedoch Systemfehler oder Hacks weitreichende Konsequenzen für die Stromversorgung haben [142]. Zudem erlaubt die starke Vernetzung der Systeme, wie am Beispiel von Smart Meters, Verbrauchs- und Verhaltensdaten von Haushalten in beispiellosem Detailgrad zu erfassen. Kritik zum Datenschutz und der Privatsphäre wurden laut, und in einigen Ländern wurden bereits besondere Regeln zum Umgang mit Verbrauchsdaten erlassen [143].

3.2.14 Öffentliche Verwaltung und Sicherheit

Die Digitalisierung hat nicht zuletzt auch staatliche Funktionen erreicht. Unter dem Stichwort **E-Government** etwa wurden auch in Österreich in den vergangenen zwei Jahrzehnten zahlreiche behördliche Funktionen und Leistungen ins Internet verlagert. Beispielsweise müssen viele ÖsterreicherInnen ihre Steuererklärung mittlerweile über das Online-System der österreichischen Finanzverwaltung FinanzOnline einreichen [144], aber auch viele andere Behördenwege und öffentliche Dienstleistungen können oder müssen mittlerweile online erledigt oder beantragt werden [145].

Trotz vermeintlich verstärkter Sicherheitsvorkehrungen und Identitätskontrollen sind öffentliche Online-Systeme für Cyberattacken oder Datenlecks ebenso anfällig. In Bulgarien etwa wurden 2019 die Server der Steuerbehörden gehackt und detaillierte Aufzeichnungen über ca. 5 Millionen bulgarische Steuerzahler gestohlen [146]. In Anbetracht der Sensibilität und Menge der personenbezogenen Daten, die mittels E-Government-Systemen übertragen und gespeichert werden, sind solche Angriffe auf E-Government-Systeme besonders kritisch zu bewerten.

Eine weitere Facette der vorschreitendenden Digitalisierung zeigt sich in der Automatisierung in der Verwaltung sowie in den Bereichen Sicherheit und Justiz. Zum Beispiel wird mittels **Predictive Policing** (vorhersagende Polizeiarbeit) auch in Österreich auf Basis von Tatmustern versucht, Kriminalität vorherzusagen. Der Erfolg der Algorithmen hängt jedoch stark vom verwendeten Datenmaterial ab, und die Genauigkeit und Nützlichkeit der Systeme ist umstritten [147]. Generell zeigt sich, dass immer öfter Algorithmen zur großflächigen Vorhersage oder Bewertung von Situationen und Individuen verwendet werden, dabei allerdings häufig aufgrund oberflächlicher Merkmale diskriminiert wird oder bestehender Vorurteile und Ungleichheiten verstärkt werden [148].

3.3 Gesellschaftliche Anforderungen an Cybersecurity

Die im vorhergehenden Abschnitt 3.2 angeführten Anwendungsbereiche verdeutlichen die immer stärkere Digitalisierung in allen Lebensbereichen und die daraus resultierenden Risiken auf allen gesellschaftlichen Ebenen. Cybersecurity ist mittlerweile, so auch die Auflassung der ExpertInnen in Interviews und dem Workshop, untrennbar mit allen Lebensbereichen verbunden. Wie in Abschnitt 2.2.2 erläutert waren sich die ExpertInnen auch einig, dass Cybersecurity über technische Maßnahmen hinausgeht und **menschliche, soziale und gesamtgesellschaftliche Komponenten** inkludiert.

Nach Auffassung der ExpertInnen bezieht sich Cybersecurity somit beispielsweise auch auf den Schutz vor der Aushöhlung gesellschaftlicher Werte durch schädliche Geschäftsmodelle von Großkonzernen wie Google oder Facebook, denn auch „Gebrauch von Technologie, nicht nur Missbrauch, kann Schaden anrichten“, wie ein Experte es formuliert. Cybersecurity ist somit ein gesellschaftlich hochrelevantes Thema, das vom Schutz des Eigentums von Einzelpersonen bis zum **Schutz gesellschaftlicher Strukturen und der Demokratie** reicht.

Als eine der wichtigsten Voraussetzung für funktionierende Cybersecurity, so die ExpertInnen, müssen Individuen und Organisationen Verständnis und Bewusstsein für Cybersecurity-Risiken und Schutzmöglichkeiten haben. Während große Unternehmen mittlerweile vergleichsweise gut gerüstet seien, sehen die ExpertInnen insbesondere für kleine und mittlere Unternehmen sowie Einzelpersonen großen Bedarf, das Bewusstsein für Cyberrisiken im Sinne der **digital Literacy** zu stärken, damit sich NutzerInnen sicher in einer digitalen Gesellschaft bewegen und Cybersecurity-Lösungen adäquat nutzen können, riskantes Verhalten der NutzerInnen eingeschränkt wird und verantwortungsvoll mit digitalen Technologien umgegangen wird.

Neben einzelnen Organisationen und NutzerInnen sahen ExpertInnen auch einen gesamtgesellschaftlichen Aufholbedarf. Ein Experte verglich das Thema Cybersecurity mit der aktuellen COVID19-Pandemie, die gezeigt habe, wie unvorbereitet die gesamte Welt auf die oft prognostizierte Pandemie reagiert hat. Neben der Resilienz einzelner technischer Systeme und Organisationen sollte demnach auch die **gesellschaftliche Resilienz im** Fokus stehen. In diesem Zusammenhang wurden etwa die starke Abhängigkeit von einzelnen Softwareanbietern im Sinne einer „Monokultur“ kritisiert, und der Bedarf an transdisziplinären Lösungsansätzen hervorgehoben. Cybersecurity sollte dabei als integraler Bestandteil von IKT-Produkten und Services mitgedacht werden. Weiters werden von den ExperInnen Foresight-Prozesse als zentral angesehen, um auf zukünftige Risiken und Bedrohungsszenarien vorbereitet zu sein und so einen gesellschaftlichen Diskurs zu Cybersecurity und den Risiken der Digitalisierung zu forcieren.

3.4 Zusammenfassung und Fazit

- Die Digitalisierung hat jeden Gesellschaftsebene und jeden Bereich unseres Lebens erreicht. Die immer **stärkere Vernetzung** der physischen und digitalen Welt erlauben zwar nie dagewesene Funktionen, Automatisierung, effizientes Arbeiten und verzögerungsfreie Kommunikation, stellen unsere Gesellschaft allerdings auch vor die Herausforderungen, nicht nur digitale Systeme und ihre NutzerInnen zu schützen, sondern auch auf **gesamtgesellschaftliche Risiken** der Digitalisierung zu reagieren.
- Eine zunehmende Komplexität digitaler Technologien und Professionalisierung der Angreifer macht es unabdingbar, das **Bewusstsein** und die Ausbildung in der Gesellschaft zum Thema Cybersecurity und digitale Risiken zu stärken.
- Neben dem Schutz vor gezielten Angriffen gilt es auch, einen **verantwortungsvollen Umgang mit Technologie** zu fördern, denn auch nicht-missbräuchliche Verwendung von digitalen Technologien birgt Risiken für Gesellschaft und Demokratie.

4. Strategische und rechtliche Rahmenbedingungen

4.1 Einleitung

Trotz oder gerade wegen der Querschnittscharakteristik der Cybersecurity-Thematik existieren auf nationaler und europäischer Ebene bereits eine Vielzahl an Initiativen, Aktivitäten und Institutionen, die Rahmenbedingungen schaffen, den Bereich regulieren oder gewisse Koordinationsfunktionen innehaben. Dieses Kapitel bietet eine Kontextualisierung des Themas auf rechtlicher und Policy-Ebene und gibt Überblick über die wichtigsten nationalen und europäischen Strategien, Gesetze, Gremien und Organisationen.

4.2 Österreichische Cybersicherheit-Strategie

Die österreichische Strategie für Cybersicherheit (ÖSCS) aus dem Jahr 2013 bildet den strategischen Rahmen für die nationale Cybersicherheitspolitik; eine Aktualisierung der Strategie ist derzeit in Arbeit. Sie hat zum Ziel, die Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyberraum zu verbessern und soll dazu beitragen, Bewusstsein über und Vertrauen in die digitale Sicherheit in der österreichischen Gesellschaft zu schaffen [149]. Die Strategie verfolgt folgende neun strategische Ziele:

- Verfügbarkeit, Zuverlässigkeit und Vertraulichkeit des Datenaustausches und Integrität der Daten in einem sicheren, resilienten und verlässlichen Cyberraum gewährleisten
- Durch einen gesamtstaatlichen Ansatz der zuständigen Bundesministerien sicherstellen, dass österreichische IKT-Infrastrukturen sicher und resilient gegen Gefährdungen sind
- Österreichische Behörden schützen in Zusammenarbeit mit nicht-staatlichen Partnern das Rechtsgut Cybersicherheit
- Umsetzung von Bewusstseinsbildung und Awareness-Maßnahmen für eine „Kultur der Cybersicherheit“
- Kooperationen sowie neue Initiativen im Rahmen eines nationalen Dialogs stärken und unterstützen
- Aktive Rolle bei der internationalen Zusammenarbeit einnehmen
- E-Government der österreichischen Verwaltung ausbauen
- Unternehmen schützen eigene Anwendungen sowie die Identität und Privatsphäre ihrer KundInnen
- Bewusstsein der Bevölkerung über individuelle Verantwortung im Cyberraum herstellen.

Zur Zielerreichung werden im Rahmen der Strategie Maßnahmen in sieben Handlungsfeldern umgesetzt [149]:

- Handlungsfeld 1: Strukturen und Prozesse
    - Maßnahmen in Handlungsfeld 1 betreffen Prozesse und Strukturen für eine übergeordnete Koordination auf politisch-strategischer und operativer Ebene. Dazu gehören unter anderem die Cyber Sicherheit Steuerungsgruppe und die Einrichtung eines Cyber Krisenmanagements.
- Handlungsfeld 2: Governance
    - Maßnahmen in Handlungsfeld 2 betreffen die Rolle, Zuständigkeiten und Kompetenzen von staatlichen und nicht-staatlichen Akteuren, sowie die Schaffung von Rahmenbedingungen für die Zusammenarbeit von Akteuren. Dazu zählen Aktivitäten wie der jährliche Bericht zur Cyber Sicherheit sowie die Zusammenfassung der gültigen Normen, Standards, Verhaltensregeln und Best Practices in einem österreichischen Informationssicherheitshandbuch.
- Handlungsfeld 3: Kooperation Staat, Wirtschaft und Gesellschaft
    - Maßnahmen in Handlungsfeld 3 betreffen die Stärkung der Kapazitäten und Prozesse in Verwaltung, Wirtschaft und bei BürgerInnen durch gestärkte Zusammenarbeit. Dazu zählen Maßnahmen wie die Einrichtung der Cyber Sicherheit Plattform.
- Handlungsfeld 4: Schutz kritischer Infrastrukturen

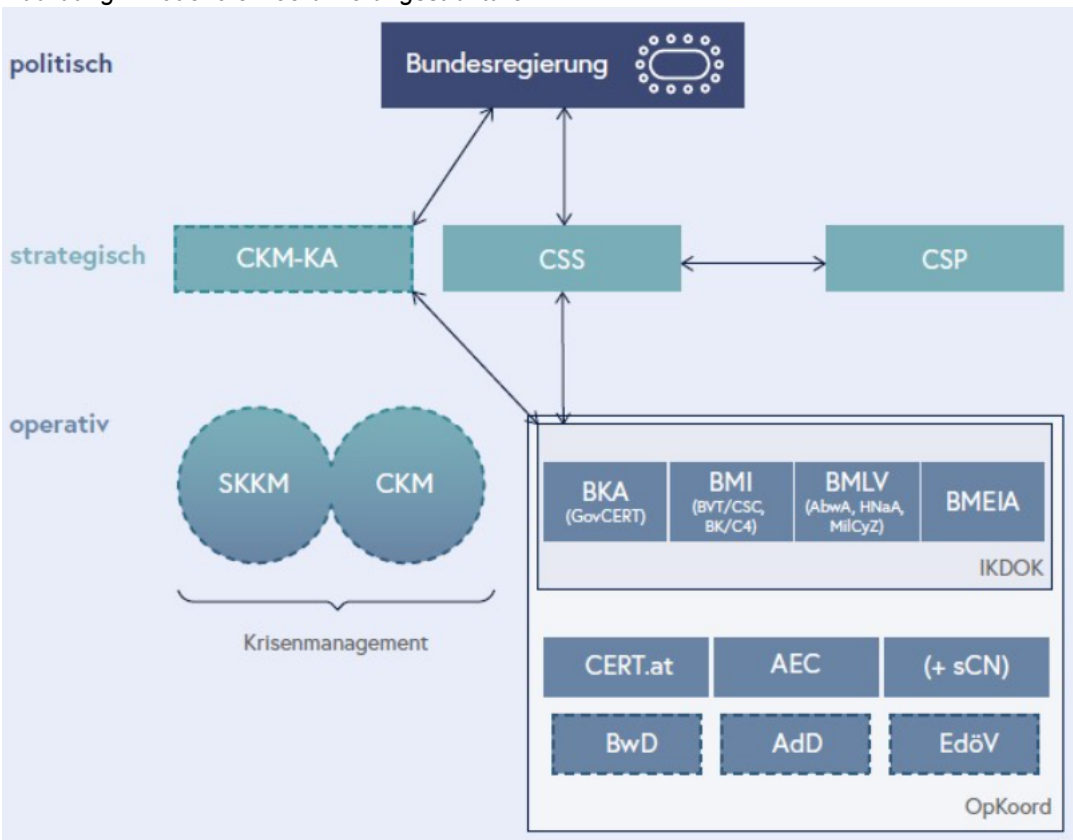
- Maßnahmen in Handlungsfeld 4 betreffen die Erhöhung der Resilienz von kritischen Infrastrukturen, komplementär zu bereits implementierten Aktivitäten im Rahmen des Programms zum Schutz kritischer Infrastrukturen (APCIP).

- Handlungsfeld 5: Sensibilisierung und Ausbildung
  - Maßnahmen in Handlungsfeld 5 betreffen die Bewusstseinsbildung sowie Stärkung von Ausbildung in Cybersecurity und Medienkompetenz in Schulen und anderen Bildungseinrichtungen.
- Handlungsfeld 6: Forschung und Entwicklung
  - Maßnahmen in Handlungsfeld 6 betreffen die Stärkung von Cybersecurity-Forschungs- und Entwicklungsthemen in Forschungsprogrammen wie KIRAS sowie der EU-Sicherheitsforschungsprogramme.
- Handlungsfeld 7: Internationale Zusammenarbeit
  - Maßnahmen in Handlungsfeld 7 betreffen die globale Vernetzung und internationale Zusammenarbeit, sowie die aktive Außenpolitik.

4.3 Nationale Cybersicherheitsstrukturen

Cybersecurity ist in Österreich ein gesamtstaatliches Thema und bedingt aufgrund der rechtlichen Querschnittsthematik eine enge Kooperation und Koordination verschiedener zuständiger Ressorts, da keine Organisation alleine österreichweit verbindliche Vorgaben setzen kann. Das Bundeskanzleramt (BKA) ist dabei für die Koordination der nationalen und europäischen Cybersecurity-Themen verantwortlich und führt das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT Austria) sowie das Ausweichrechenzentrum des Bundes. Neben dem Bundeskanzleramt haben auch das Bundesministerium für Inneres (BMI), Bundesministerium für europäische und internationale Angelegenheiten (BMEIA) und das Bundesministerium für Landesverteidigung (BMLV) Zuständigkeiten in Cybersecurity.

Abbildung 4 Nationale Koordinierungsstrukturen



Quelle: Bundeskanzleramt [150]

Abbildung 4 stellt die nationale Koordinierungsstrukturen für Cybersecurity dar. Die Bundesregierung zeichnet für politische Vorgaben verantwortlich. Auf strategischer Ebene stellt das gesamtstaatliche Cyberkrisenmanagement (CKM) sowie der CKM-Koordinationsausschuss (CKM-KA) eine Plattform für interministerielle Koordination bereit. Die Cyber-Sicherheit-Steuerungsgruppe (CSS) verantwortet auf strategischer Ebene die Umsetzung der österreichischen Cybersicherheit-Strategie. Die Cyber-Sicherheit-Plattform (CSP), eine 2015 ins Leben gerufene Public-Private-Partnership, ist die zentrale Austausch- und Koordinationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung und berät und unterstützt die CSS.

Auf operativer Ebene wurde die sogenannte Operative Koordinierungsstruktur (OpKoord) sowie der Innere Kreis der Koordinierungsstruktur (IKDOK) eingerichtet. Diese sind zuständig für Monitoring und Erstellung ständiger Lagebilder und sollen das koordinierte Vorgehen bei Cybervorfällen ermöglichen. Im Krisenfall bildet das IKDOK, unterstützt durch die OpKoord, die Schnittstelle zum staatlichen Cyberkrisenmanagement.

In Interviews und Workshops wurde die Effektivität der nationalen Koordination und Kooperation in Cybersecurity als gemischt angesehen. Einerseits unterstrichen die ExpertInnen die national bereits sehr gut miteinander vernetzten Cybersecurity-Akteure, insbesondere durch existierende Plattformen und Gremien (CSP, A-SIT, Cyber Security Austria, Kuratorium Sicheres Österreich, CERT, etc.), andererseits wird aber der Bedarf **nach besserer Abstimmung zwischen öffentlicher Hand und Privatwirtschaft, Wissenschaft und Innovation** formuliert. Dies betrifft vor allem einen verstärkt **beidseitigen Informationsfluss** und Kooperation „auf Augenhöhe".

Der inhaltliche und rechtliche Querschnittscharakter von Cybersecurity bedingt die oben erwähnte Koordination und Kooperation zwischen mehreren zuständigen Ressorts. Die Effektivität der Koordination und Abstimmung zwischen den zuständigen Ministerien BKA, BMI, BMEIA, BMLV wurde in einigen Interviews sowie im Workshop kritisch diskutiert. Aus Sicht der ExpertInnen ist eine gewisse **fehlende Fokussierung und fehlende Proaktivität** im politischen und gesetzlichen Handeln beobachtbar, die auf eine nötige Verbesserung in wirksamere und effizientere staatliche Strukturen zurückgeführt wird. Eine effektivere zentrale Koordination aller Cybersecurity-Agenden sollte dabei auch als „Intermediär" und „Multiplikator" der Thematik fungieren und eine proaktive strategische, politische und gesetzliche Schwerpunktsetzung vornehmen. Zusätzlich wurde der **Bedarf nach intensiverer Zusammenarbeit auf operativer Ebene**, i.e. CERTs, CSIRTs, geäußert um der Herausforderung Cybersecurity effektiver zu begegnen und gegenseitig von Informationen und Erfahrungen zu profitieren.

Ebenfalls relevant im Bereich Cybersecurity ist das österreichische Programm zum **Schutz kritischer Infrastrukturen** (APCIP). Da die Funktionsfähigkeit von Infrastrukturen durch Naturkatastrophen, technische Unfälle, menschliches Versagen, Gefahren im Cyberspace, Kriminalität und Terrorismus gefährdet sein kann, hat die österreichische Regierung im Jahr 2008 den Masterplan APCIP, welcher 2014 überarbeitet worden ist, für den Schutz von kritischen Infrastrukturen beschlossen. Kritische Infrastrukturen werden in dem Programm als Infrastrukturen beschrieben, „*die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde*" [151].

APCIP verfolgt das Ziel, die Versorgungssicherheit bei Lebensmitteln, Verkehrs-, Telekommunikation-, Energie-, und Finanzdienstleistungen wie auch die gesicherte Versorgung mit Sozial- und Gesundheitsdienstleistungen zu gewährleisten. Des Weiteren ist APCIP ein wichtiger Beitrag zur Erarbeitung eines gesamtstaatlichen Konzepts zur Steigerung der Resilienz Österreichs, wobei Resilienz beschrieben wird als „*die Fähigkeit eines Systems, einer Gemeinschaft oder einer Gesellschaft, welche(s) Gefahren ausgesetzt ist, deren Folgen zeitgerecht und wirkungsvoll zu bewältigen, mit ihnen umzugehen sich ihnen anzupassen und sich von ihnen zu erholen, auch durch Bewahrung und Wiederherstellung seiner bzw. ihrer wesentlichen Grundstrukturen und Funktionen*" [151].

4.4 Europäische Cybersecurity-Strategie

Neben der österreichischen Strategie spielt im Cybersecurity-Bereich auch die europäische Komponente eine Rolle. Die Europäische Union verfolgt das Ziel, die Cyberabwehrfähigkeit zu verbessern, Cyberkriminalität zu bekämpfen, Cyberdiplomatie zu befördern, die Cyberabwehr zu stärken, Forschung und Innovation zu fördern und kritische Infrastrukturen zu schützen. Im Dezember 2020 wurden eine neue Strategie für Cybersicherheit vorgelegt, welche im März 2021 vom Rat angenommen wurde. Mit der Hilfe dieser Strategie soll die Widerstandsfähigkeit Europas gegenüber Cyberangriffen gestärkt werden und es soll BürgerInnen und Unternehmen gewährleistet werden, dass sie im vollen Umfang von Vertrauenswürdigen und zuverlässigen Diensten und digitalen Instrumenten profitieren können [152]. Die EU-Cybersicherheitsstrategie enthält Vorschläge für Regulierungs-, Investitions-, und Politikinstrumente in drei Aktionsfeldern [153]:

- **Resilienz, technologische Souveränität und Führungsrolle**
  In diesem Aktionsfeld soll durch die Überarbeitung der Richtline zur Netz- und Informationssicherheit (NIS oder „NIS2“) die Abwehrfähigkeit kritischer öffentlicher und privater Sektoren verbessert werden. Darüber hinaus sollen ein Netz von Sicherheitseinsatzzentren (Computer Security Incident Response Teams, CSIRT) zur frühzeitigen Erkennung von Cyberangriffen aufgebaut sowie insbesondere kleine und mittlere Unternehmen (KMU) im Rahmen der Digital Innovation Hubs unterstützt werden.
- **Aufbau operativer Fähigkeiten zur Prävention, Abschreckung und Reaktion**
  Im Rahmen einer neuen gemeinsamen Cyberstelle soll die Zusammenarbeit zwischen Mitgliedstaaten und EU-Einrichtungen gestärkt werden. Mitgliedstaaten sollen auch die ständige strukturierte Zusammenarbeit („Permanent Structured Cooperation“, PESCO) und den Europäischen Verteidigungsfonds nutzen.
- **Zusammenarbeit zur Förderung eines globalen und offenen Cyberraums**
  In diesem Aktionsfeld sind insbesondere Aktivitäten zur Cyberdiplomatie sowie dem Aufbau von Cyberkapazitäten in Drittländern vorgesehen.

4.5 Europäische Strukturen

Cybersecurity ist in den kommenden Jahren auf europäischer Ebene ein zentrales Thema. Cybersecurity ist ein länderübergreifendes Thema – das Internet kennt keine Ländergrenzen – und kann auch nicht durch eine einzelne Gruppe von Akteuren erreicht werden. Im Mehrjährigen Finanzrahmen (MFR) 2021-2027 sind mehr als € 2 Mrd. im Rahmen des Digital Europe Programms der Europäischen Kommission der Unterstützung der Cybersecurity-Industrie und Finanzierung von Cybersecurity-Equiment und -Infrastruktur gewidmet. Zusätzlich soll Forschung und Innovation in Cybersecurity im Rahmen von Horizon Europe gefördert werden. Neben der europäischen Cybersecurity-Strategie sowie der verfügbaren finanziellen Mittel ist die Bedeutung von Cybersecurity auf auch an den jüngsten Entwicklungen im Aufbau von europäischen Initiativen und Koordinierungsstrukturen erkennbar.

<u>European Union Agency for Cybersecurity (ENISA)</u>

Die European Union Agency for Cybersecurity (ENISA) wurde 2004 mit dem Ziel gegründet im EU-Raum die Informationssicherheit zu stärken. 2019 trat der **EU Cybersecurity Act**, europäische Verordnung (EU) Nr. 881/2019, in Kraft. Durch den Cybersecurity Act wurde ein dauerhaftes Mandat für die ENISA geschaffen und die finanziellen und personellen Mittel der Organisation erhöht. Sie soll die Cybersecurity-Kapazitäten der EU erhöhen, die Koordination auf EU-Ebene stärken, Mitgliedstaaten bei Cybersecurity-Vorfällen unterstützen, sowie Wissensaustausch, Sensibilisierung und Wissensaufbau betreiben. Der Cybersecurity Act hat auch einen Rahmen für **Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen** geschaffen. Die ENISA ist in diesem Zusammenhang mit der Entwicklung von Zertifizierungsschemen betraut und soll zugleich auch die Öffentlichkeit über Zertifizierungsschemen informieren.

Interviewte ExpertInnen und TeilnehmerInnen des Workshops wiesen mehrfach auf die Bedeutung bzw. das Zukunftsfeld der Zertifizierungsschemen und Standards für Cybersecurity hin: Der Cybersecurity Act hat den notwendigen Rahmen für die Entwicklung konkreter Zertifizierungsmechanismen geschaffen. Auch in Österreich existieren bereits Zertifizierungen und Gütesiegel für Cybersecurity. Als Beispiel mit potenzieller europäischer/internationaler Vorbildwirkung kann das **österreichische Gütesiegel** für Cybersicherheit „Cyber Trust Austria Label" des Kuratorium Sicheres Österreich (KSÖ) zur Auszeichnung von unternehmensweiter Cybersecurity, das erste dieser Art in der EU, genannt werden. Weiters schufen das KSÖ und der Kreditschutzverband von 1870 (KSV1870) das österreichische CyberRisk Rating, um digitale Risiken in globalen Lieferketten sichtbar zu machen und Unternehmen mit einem standardisierten Cyber-Risikomanagement für Lieferanten zu unterstützen. In diesem Bereich mit wachsender Relevanz kann Österreich und Europa auch international einen wesentlichen Beitrag leisten.

European Cybersecurity Competence Network and Centre

Das European Cybersecurity Competence Network and Centre soll zum Aufbau eines EU-weiten Cybersecurity-Industrie- und Forschungsökosystems beitragen und Kooperationen zwischen Stakeholdern, auch zwischen Zivil- und Militärbereich, stärken. Im Rahmen dieser Initiative ist der Aufbau eines Netzwerks von Nationalen Koordinationszentren (Network of National Coordination Centres) vorgesehen. Nationale Koordinationszentren sollen Cybersecurity-Akteure auf nationaler Ebene vernetzen und die nationale Umsetzung europäischer Aktivitäten und Vorgaben unterstützen. Ein weiteres Element dieser Initiative ist die Gründung des European Cybersecurity Competence Centre (ECC) mit Sitz in Bukarest. Das ECC soll relevante Programmteile von Digital Europe und Horizon Europe abwickeln und zum Kapazitätsaufbau und Stärkung der Wettbewerbsfähigkeit beitragen. Darüber hinaus soll es das Netzwerk der Nationalen Koordinationszentren unterstützen und koordinieren und strategische Investitionsentscheidungen unter Bündelung finanzieller Ressourcen der EU, der Mitgliedstaaten sowie der Industrie treffen.

Cyberdiplomatie

Die EU und Österreich legen neben den bereits erwähnten strategischen, gesetzlichen, Kapazitäts- und Bewusstseinsbildungsmaßnahmen auch einen Fokus auf internationale Kooperation und Koordination in Cybersecurity-Themen. Cyberdiplomatie soll den zunehmenden hybriden Bedrohungen und dem Risiko von Cyberkrieg durch internationale Zusammenarbeit entgegenwirken. Die EU Global Strategy (2016) setzte die Ziele der europäischen Cyberdiplomatie: Sie soll „Abkommen über verantwortungsvolles staatliches Handeln im Cyberraum basierend auf internationalem Recht" sowie eine „multilaterale digitale Governance und einen globalen Kooperationsrahmen" mittels Bündnisse gleichgesinnter Länder, Organisationen, Privatwirtschaft, Zivilgeschafft und ExpertInnen unterstützen.

Die Relevanz und steigende Bedeutung von Cyberdiplomatie wurden in Interviews und Workshop mehrfach von österreichischen ExpertInnen betont. So verlange Cybersecurity nach neuen Fähigkeiten und Tools, auch bei Behörden, und kenne keine Landesgrenzen. Die **internationale Vernetzung** und ein **international koordiniertes Vorgehen** sind dabei wesentlich für Cybersecurity. Europa, und Österreich, sind gut positioniert um im Bereich Cyberdiplomatie eine wesentliche Rolle zu spielen, sofern eine innereuropäische Abstimmung vorgenommen wird und international gleichgesinnte Länder gemeinsam für das Cyber-Gemeinwohl handeln.

Ein Beispiel für das gelungene koordinierte Handeln auf europäischer Ebene ist die European Quantum Communication Infrastructure (EuroQCI) Initiative zum Aufbau einer Verschlüsselungsinfrastruktur in der EU, die auch einen Beitrag zur Datenautonomie in der EU leisten soll. Alle 27 Mitgliedstaaten haben die EuroQCI Erklärung unterschrieben und so ihr Bekenntnis zur Initiative signalisiert.

4.6 Relevante gesetzliche Maßnahmen

4.6.1 Netz- und Informationssicherheit-Richtlinie (NIS-Richtlinie)

Die NIS-Richtlinie ist die erste EU-weite Cybersecurity-Gesetzgebung mit dem Ziel die Cybersicherheit innerhalb der Europäischen Union zu verbessern. Die NIS-Richtlinie wurde als Teil der EU-Cybersecurity-Strategie von der Europäischen Kommission vorgeschlagen und im Jahr 2016 beschlossen. Seit 2018 hat jeder Mitgliedsstaat begonnen, diese Richtlinien in die nationalen Gesetzgebungen aufzunehmen.

Die NIS-Richtlinie der EU besteht aus drei wesentlichen Teilen [154]:

- Nationale Fähigkeiten: EU-Mitglieder müssen über bestimmte nationale Cybersecurity-Fähigkeiten verfügen, z.B. müssen sie Cyber-Übungen durchführen und ein nationales CSIRT haben. Dessen Aufgabe ist es, Informationen über Sicherheitsvorfälle zu sammeln, Analysen durchzuführen und auf Anfragen zu reagieren.
- Grenzüberschreitende Fähigkeiten: EU-Mitgliedsstaaten müssen grenzüberschreitend zusammenarbeiten, z.B. durch ein EU-CSIRT-Netz, NIS-Kooperationsgruppen, etc.
- Nationale Aufsicht über kritische Infrastrukturen: EU-Mitgliedstaaten müssen die Cybersicherheit der kritischen Marktteilnehmer in ihrem Land überwachen.

In Österreich wurde die NIS-Richtlinie mit dem im Dezember 2018 kundgemachten Netzwerk- und Informationssicherheitsgesetz (NISG) zur Gewährleistung eines hohen Sicherheitsniveaus dieser Systeme umgesetzt. In diesem Gesetz werden Aufgaben, die sich aus der NIS-Richtlinie ergeben, bereits bestehenden Strukturen aufgetragen. Das NISG richtet sich daher vor allem an Betreiber wesentlicher Dienste, Anbieter digitaler Dienst und Einrichtungen des Bundes. Diese Organisationen müssen geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen treffen und Sicherheitsvorfälle melden.

Betreiber wesentlicher Dienste werden definiert als öffentliche oder private Einrichtungen

- aus den Sektoren:
    - Energie
    - Verkehr
    - Bankwesen
    - Finanzmarktinfrastrukturen
    - Gesundheitswesen
    - Trinkwasserversorgung
    - Digitale Infrastruktur
- mit Niederlassung in der EU,
- die einen Dienst bereitstellen, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist,
- der abhängig von Netz- und Informationssystemen ist, und
- bei denen ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirkt.

Betreiber wesentlicher Dienste werden durch einen Bescheid ermittelt und müssen mindestens alle drei Jahre nach Zustellung des Bescheids einen Nachweis entsprechender Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme (Aufstellung der Sicherheitsvorkehrungen durch Zertifizierungen oder Überprüfungen durch qualifizierte Stellen) erbringen, wobei der Bundesminister für Inneres die Einhaltung der Anforderungen jederzeit überprüfen kann.

Anbieter digitaler Dienste werden definiert als juristische Person, die einen der folgenden digitalen Dienste anbieten:

- Online-Marktplatz
- Online-Suchmaschine
- Cloud-Computing-Dienst

Ausgenommen sind Kleinunternehmen mit weniger als 50 MitarbeiterInnen und Jahresumsatz/Bilanz von weniger als € 10 Mio.

Im Bereich der Anbieter digitaler Dienste gibt es keine gesonderte Ermittlung durch die Mitgliedstaaten durch Bescheid. Anbieter digitaler Dienste müssen geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen treffen. Sie sind aber grundsätzlich in deren Auswahl frei, sofern diese ein angemessenes Sicherheitsniveau gewährleisten und die Vorgaben der NIS-Richtlinie einhalten [155].

Eine Überarbeitung der NIS-Richtlinie wurde bereits Ende 2020 vorgelegt. Der Legislativvorschlag der Europäischen Kommission zur **NIS2-Richtlinie** enthält im Vergleich **mehr Betroffenheit, Pflichten und Aufsicht**:

- Erweiterung der von NIS2-betroffenen Sektoren: NIS2 wird zusätzlich Einrichtungen aus den Sektoren Herstellung pharmazeutischer Erzeugnisse, Abwasserwirtschaft, öffentliche Verwaltung, Weltraum als Betreiber wesentlicher Dienste einstufen.
- Schwellwerte: Mittlere und größere Unternehmen („Medium“ und „Large Enterprises“) sollen zukünftig betroffen sein.
- Höhere Cybersecurity-Anforderungen für Betreiber und Mitgliedstaaten, Cybersecurity soll auch in Lieferketten betrachtet werden.
- Vertiefte Kooperation zwischen Behörden und Betreibern.
- Ausweitung von Sanktionen.

4.6.2 Datenschutzgrundverordnung (DSGVO)

Die Datenschutzgrundverordnung (DSGVO, General Data Protection Regulation, GDPR) wurde von der Europäischen Union im Jahr 2018 verabschiedet. Seitdem erlegt die DSGVO Verpflichtungen auf jegliche Organisationen auf, die persönliche Daten von EU-BürgerInnen verarbeiten. Die DSGVO legt fest, dass **persönliche Daten** jene Informationen beinhalten, die sich auf ein Individuum beziehen, welches dadurch direkt oder indirekt identifiziert werden kann (z.B. Namen, E-Mail-Adressen, Geburtsdatum, Geschlecht, etc.).

Weitere wichtige Definitionen in der DSGVO lauten:

- **Datenverarbeitung** umfasst jegliche Art von Datenverarbeitung, unabhängig davon, ob diese Aktivität automatisch oder manuell stattgefunden hat, z.B. Daten sammeln, aufnehmen, organisieren, verwenden, speichern, etc.
- **Datensubjekt** ist die Person, dessen Daten verarbeitet werden.
- **Datenverantwortlicher** ist die Person, welche entscheidet, warum und wie persönliche Daten verarbeitet werden.
- **Datenverarbeiter** ist eine dritte Partei, welche persönliche Daten im Namen des Datenverantwortlichen, verarbeitet.

Die DSGVO besteht aus sieben Prinzipien für den Umgang oder die Verarbeitung mit Daten eines EU-Bürgers [32]:

1. **Rechtmäßigkeit, Fairness, Transparenz:** die Verarbeitung von Daten muss rechtmäßig, fair und transparent gegenüber dem Datensubjekt sein.
2. **Zweckbindung:** man darf die Daten nur für die exakten Zwecke, welche dem Datensubjekt genannt worden sind und für welche die Daten gesammelt wurden, verwenden.
3. **Daten Minimierung:** man darf nur die für die genannten Zwecke notwendigen Daten sammeln und verarbeiten.
4. **Richtigkeit:** man muss die persönlichen Daten genau und aktuell halten.
5. **Speicherbegrenzung:** man darf persönliche Daten nur so lange speichern, wie es für den genannten Zweck erforderlich ist.
6. **Integrität und Vertraulichkeit:** die Datenverarbeitung muss auf eine Art und Weise erfolgen, welche angemessene Security, Integrität und Vertraulichkeit sicherstellt.
7. **Verantwortlichkeit:** der Data Controller ist dafür verantwortlich, die Regelbefolgung der DSGVO und der sieben Prinzipien nachzuweisen.

Des Weiteren besagt die DSGVO, dass Daten durch die Implementierung von angemessenen technischen und unternehmerischen Maßnahmen beschützt werden müssen, wie z.B. Zweifaktorauthentifizierung oder Sicherheitsübungen für Angestellte. Das Datenschutzgesetz regelt auch, wie der Schutz von Daten gestaltet werden muss, ab wann es einer Organisation erlaubt ist Daten zu verarbeiten und wie die Zustimmung einer Person, deren Daten verarbeitet werden, gestaltet sein muss.

In Österreich wird die DSGVO durch das Datenschutzgesetzt (DSG) erfüllt. Alle Datenverarbeitungen in Österreich müssen seit Mai 2018 dieser Rechtslage entsprechen. Das DSG setzt die Prinzipien der DSGVO um und zielt gleichzeitig auf eine stärkere Verantwortung für Verantwortliche und Auftragsverarbeiter bei der Datenverarbeitung ab [156].

4.7 Zusammenfassung und Fazit

- Sowohl auf österreichischer als auch auf europäischer Ebene existieren eine Reihe von **Strategien, Initiativen und Maßnahmen** zur Koordination, Unterstützung und Umsetzung von Cybersecurity. Dazu zählen auch **gesetzliche Maßnahmen** im Bereich Datenschutz (DSGVO) und die Netz- und Informationssicherheit-Richtlinie für Betreiber wesentlicher Dienste.
- Die **nationale Cybersicherheit-Strategie** bildet dabei den Rahmen für Österreich, während die etablierte nationale Cybersicherheitsstruktur die strategische und operative Umsetzung und Koordination ermöglicht. Verschiedene Gremien und Institutionen, darunter das CSP, KSÖ, A-Sit ermöglichen eine bereits **gute Vernetzung der Cybersecurity-Akteure**. Verbesserungsbedarf wurde aber insbesondere in der Vernetzung der **öffentlichen Hand mit privaten Akteuren** festgestellt, insbesondere im Sinne eines beidseitigen Informations- und Erfahrungsaustausches.
- Der europäische Kontext ist auch in Cybersecurity ein wichtiger Aspekt. Die **europäische Cybersecurity-Strategie** sowie der **Cybersecurity Act** bilden den Rahmen für gemeinsame Aktivitäten auf europäischer Ebene.
- Entwicklungen in Österreich und Europa im Bereich der **Zertifizierungsschemen und Gütesiegel** für Cybersecurity Produkte, Dienstleistungen und Prozesse sind ein Zukunftsfeld. Das österreichische „Cyber Trust Austria Label“ des KSÖ zur Auszeichnung von unternehmensweiter Cybersecurity ist das erste seiner Art in der EU. Österreich könnte künftig im Bereich Zertifizierung auch international eine Vorbildwirkung erzielen.
- Mit der Stärkung der ENISA sowie die sich in Aufbau befindenden Cybersecurity Competence Centre und dem europäischen Cybersecurity Network werden Strukturen geschaffen, um die Koordination und Kooperation zwischen Mitgliedstaaten zu stärken. In Anbetracht der Querschnittseigenschaft von Cybersecurity, ist **länderübergreifende Kooperation** auf europäischer Ebene essenziell.
- Darüber hinaus wird auch ein international koordiniertes Vorgehen in Anbetracht der steigenden Risiken von hybriden Bedrohungen und Cyberkrieg immer wichtiger. Österreich und die EU sind bereits aktiv in **Cyberdiplomatie**. Es ist wahrscheinlich, dass Cyberdiplomatie künftig eine wichtigere Rolle auf internationaler Ebene spielen wird.

5. Forschung, Technologie und Innovation im Bereich Cybersecurity

Das vorliegende Kapitel beleuchtet die Aktivitäten österreichischer Organisationen in Horizon-2020-Projekten und stellt die relevanten Ergebnisse der Interviews und des Workshops zu aktuellen und zukünftig relevanten FTI-Themen im Bereich Cybersecurity dar.

5.1 Beteiligung österreichischer Akteure in europäischen FTI-Aktivitäten

Die nachfolgenden Darstellungen bieten einen Überblick über die europäische Forschungs- und Förderlandschaft in Cybersecurity und verwandten Forschungsfeldern und illustriert die Aktivität österreichischer Akteure im europäischen Vergleich. Die Analyse der Aktivitäten erfolgte auf Basis einer gezielten Suche nach Horizon-2020-Projekten in der EUPRO-Datenbank des AIT. Neben allgemeinen Statistiken wie den Fördersummen und der Anzahl der Projektteilnahmen bietet die Analyse zudem Einblick in aktive Organisationstypen und die zentralen österreichischen Organisationen und Kooperationen im Bereich Cybersecurity.

Die Analyse basiert auf Horizon-2020-Projekten mit Startdatum zwischen Oktober 2014 und Dezember 2019. Die Identifikation der relevanten Projekte erfolgte durch eine automatisierte Suche nach 30 relevanten Schlagworten im Projekttitel sowie der Kurzbeschreibung der Projekte in der EUPRO-Datenbank des AIT. Dieser erste, automatische Suchvorgang resultierte in 548 Projekte. In einem zweiten Schritt wurde durch das AIT-Projektteam überprüft, ob der Fokus der Projekte tatsächlich im Bereich Cybersecurity lag. Nach der manuellen Säuberung verblieben 258 Projekte im Datensatz.

Für die **Schlagwortsuche** wurde neben dem Begriff „Cybersecurity“ gezielt nach verwandten Begriffen (z.B. „Information Security“ oder „Cyberspace“), Methoden und technischen Aspekten (z.B. „Cryptography“), Bedrohungen (z.B. „Malware“) sowie Kombinationen aus Schlagworten (z.B. „Resilience“ + „Network“) gesucht. Die vollständige Liste der Schlagworte und die jeweilige Anzahl der Projekte insgesamt sowie mit österreichischer Beteiligung sind in Tabelle 1dargestellt.

Tabelle 1: Anzahl der identifizierten Projekte pro Schlagwort.

Themenfelder	Alle Projekte	Projekte mit ö. Beteiligung
Cybersecurity	75	14
Cryptography	52	10
Authentication	50	6
Malware	21	1
Resilience + Network	20	7
Resilience + Cyber	20	6
Data Security	18	3
Internet of Things (IoT) & Cybersecurity	17	3
Data Breach	15	2
Information Security	13	2
Hacking	12	3
Blockchain + Cybersecurity	8	1
Network Security	8	
Identity Management	8	1

Identity Theft	7	
Digitalisation	7	2
Digital Twin	6	1
Ransomware	5	1
Threat Landscape	5	1
Computer Security Incident Response Team (CSIRT)	5	2
Botnet	5	
IT Security	5	
ICT Security	4	1
Phishing	3	
Network and Information Security	2	1
Public Key Infrastructure	2	
Distributed Denial of Service	2	
Computer Emergency Response Team (CERT)	1	
Web Application Attacks	1	
Cyber Space	1	

Anmerkung: Es sind mehrere Schlagworte pro Projekt möglich.

5.1.1 Projektbeteiligungen und Kosten

Die in der Schlagwortsuche identifizierten 258 Projekte hatten Gesamtkosten von € 893 Mio. (durchschnittlich € 3,5 Mio. pro Projekt), wovon € 682 Mio. auf europäische Fördergelder entfallen (durchschnittlich € 2,7 Mio. pro Projekt). Im Durchschnitt sind vier Organisationen in einem Projekt vertreten. Tabelle 2 zeigt die Anzahl der Projekte und Projektbeteiligungen sowie die (durchschnittlichen) Kosten insgesamt sowie für Projekte mit österreichischer Beteiligung.

Projekte mit österreichischer Beteiligung fallen im Durchschnitt größer aus. 43 Projekte involvieren im Schnitt 13,3 Organisationen, mit Gesamtkosten von insgesamt € 385 Mio. (durchschnittliche € 9 Mio. pro Projekt) und europäischer Förderung von € 245 Mio. (durchschnittlich € 5,7 Mio. pro Projekt).

Tabelle 2: Überblick über Cybersecurity-Projekte in Horizon 2020

	Alle Projekte	Projekte m. ö. Beteiligung
Anzahl der Projekte	258	43
Anzahl der Projektbeteiligungen	1932	86
Gesamtkosten	€ 893 Mio.	€ 385 Mio.
Europäische Förderung	€ 682 Mio.	€ 245 Mio.
Durchschnittliche Projektkosten	€ 3,5 Mio.	€ 9 Mio.
Durchschnittliche eur. Förderung	€ 2,7 Mio.	€ 5,7 Mio.
Durchschnittliche Anzahl an Organisationen	4,0	13,3

Zudem zeigt sich, dass österreichische Organisationen in der europäischen Projektlandschaft **gut vertreten** sind und an 43 Projekten teilnahmen (siehe Abbildung 5). Auch im Hinblick auf die Projektbeteiligungen (siehe Abbildung 6), also die Summe der Teilnahmen je Land, sind österreichische Organisation sowohl in der Koordination als auch als Projektpartner ähnlich gut positioniert. Mit einem Anteil von 4,5 % an der

Gesamtzahl der Projektteilnahmen sind Projekte mit Cybersecurity-Bezug sind österreichische Akteure sehr stark vertreten. Diese Stärke zeigt sich auch im Vergleich zur Gesamtbeteiligung Österreichs an Horizon 2020 (3,2 %). Die gute Positionierung österreichischer FTI-Akteure wurde mehrfach in Interviews und Workshop bestätigt. Die befragten ExpertInnen verwiesen oft auf die Existenz mehrerer **exzellenter Forschungsgruppen** mit europäischer und internationaler Sichtbarkeit an Österreichs Universitäten, Forschungsorganisationen und Unternehmen. Die relativ hohe Anzahl von österreichischen Beteiligungen an Cybersecurity-Projekten im europäischen Forschungsrahmenprogramm spiegelt die Stärke der österreichischen FTI-Akteure wider.

Abbildung 5: Anzahl der Cybersecurity-Projekte pro Land

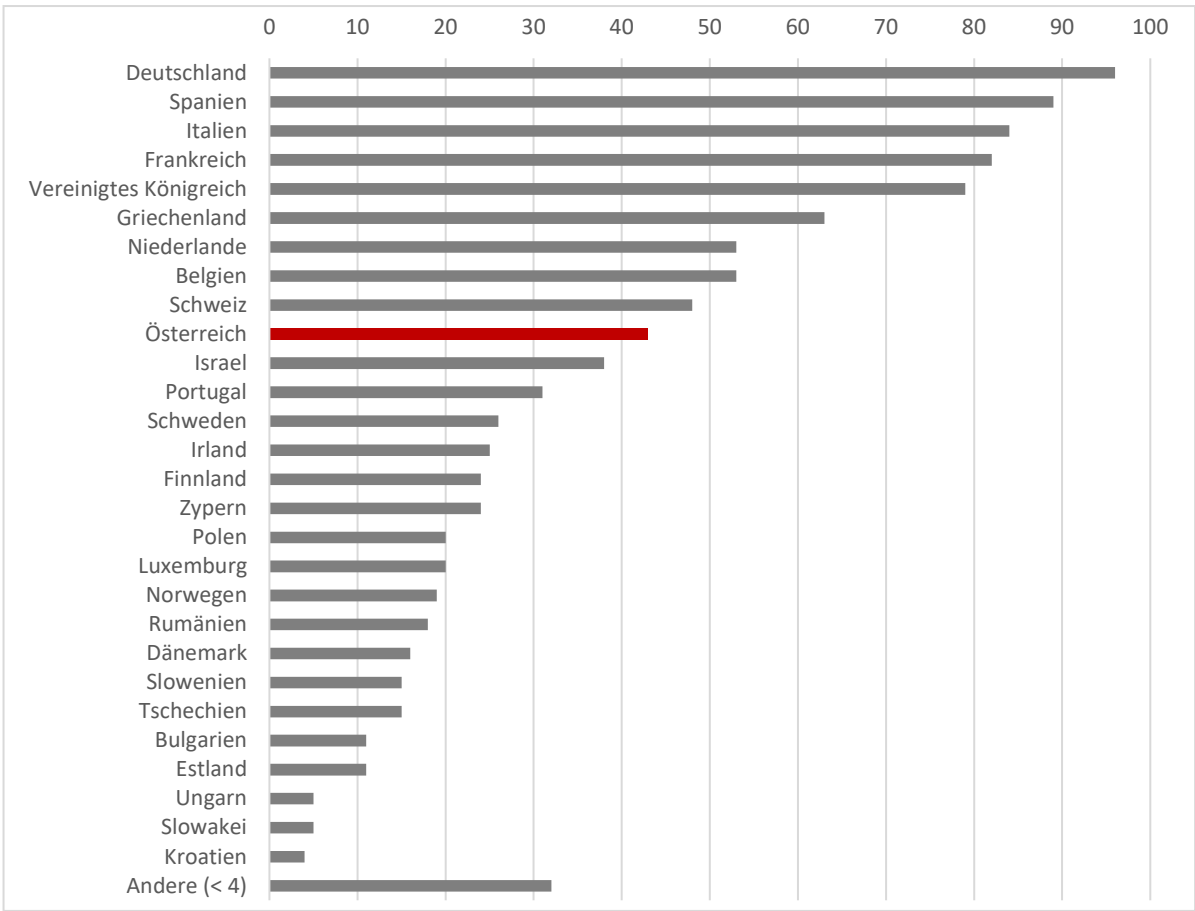
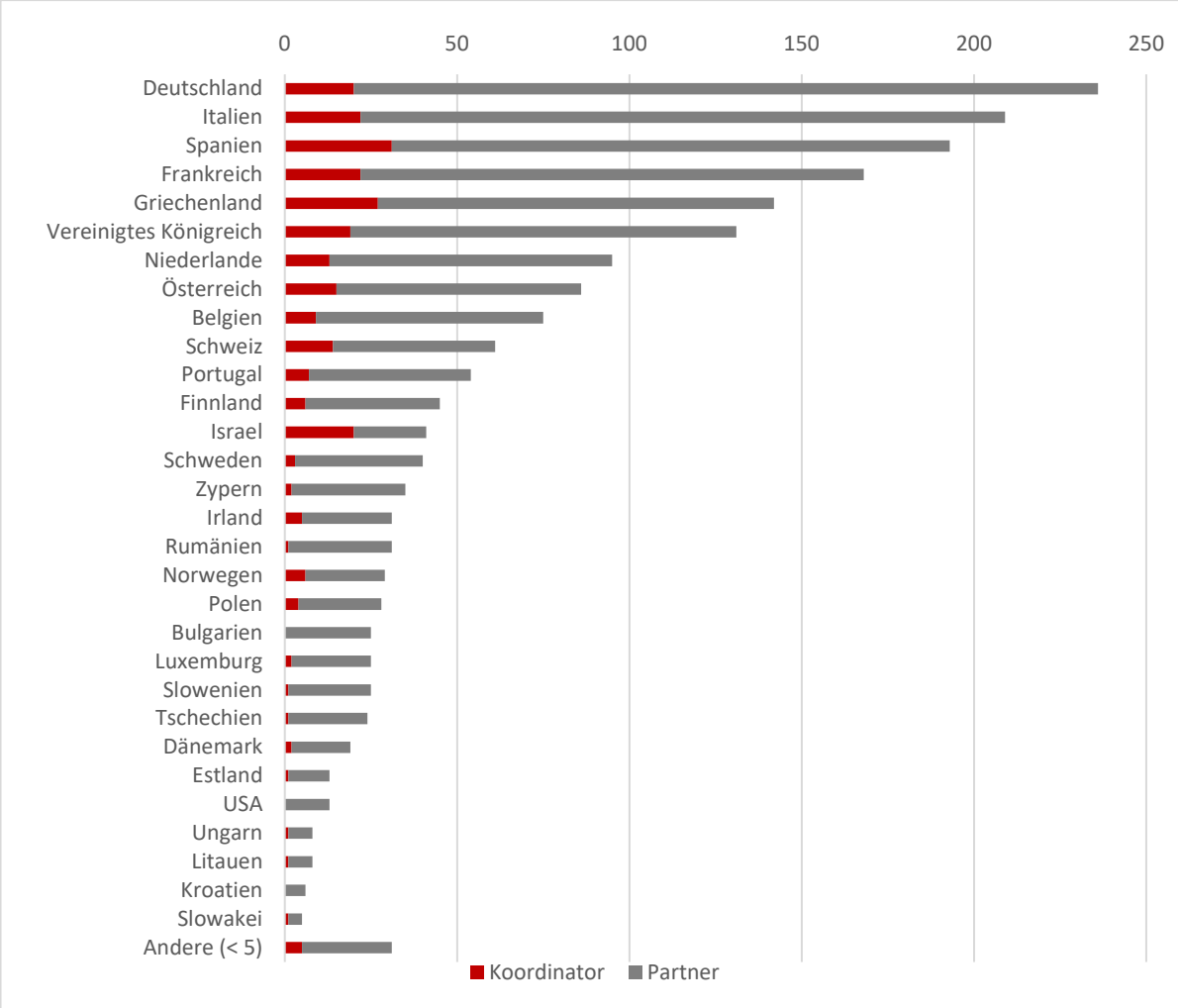


Abbildung 6: Anzahl der Teilnahmen an Cybersecurity-Projekten pro Land



5.1.2 Organisationstyp

Gemessen an der Anzahl der Organisationstypen der teilnehmenden Organisationen sowie den Projektteilnahmen (siehe Tabelle 3 und Tabelle 4) zeigt sich, dass österreichische Industrieorganisationen etwa gleich oft in Projekten vertreten waren wie im europäischen Durchschnitt. Öffentliche und private Forschungsorganisationen aus Österreich nahmen im Verhältnis häufiger an Cybersecurity-Projekten teil als der Durchschnitt. Andere Organisationstypen, darunter österreichische Universitäten und öffentliche Einrichtungen, sind hingegen etwas seltener vertreten.

Tabelle 3 Organisationstypen in Cybersecurity-Projekten

	Alle Länder	Österreich
Öffentliche Einrichtungen	51 (4,09 %)	1 (2,13 %)
Industrie	687 (55,05 %)	25 (53,19 %)
Öffentliche und private Forschungsorganisationen	144 (11,54 %)	10 (21,28 %)
Interessensvertretungen	86 (6,89 %)	2 (4,26 %)
Universitäten	280 (22,44 %)	9 (19,15 %)
Gesamt	1248	47

Tabelle 4: Projektteilnahmen nach Organisationstyp

	Alle Länder	Österreich
Öffentliche Einrichtungen	56 (2,9 %)	1 (1,16 %)
Industrie	950 (49,17 %)	38 (44,19 %)
Öffentliche und private Forschungsorganisationen	316 (16,36 %)	24 (27,91 %)
Interessensvertretungen	100 (5,18 %)	3 (3,49 %)
Universitäten	510 (26,4 %)	20 (23,26 %)
Gesamt	1932	86 (4.45 %)

Organisationen mit den häufigsten Projektteilnahmen sind in Tabelle 5 dargestellt. Das Austrian Institute of Technology ist mit neun Teilnahmen Spitzenreiter, gefolgt von der Technischen Universität Graz mit fünf, und der Universität Klagenfurt und Infineon Technologies mit jeweils vier Teilnahmen. Eine inhaltliche Analyse der Projektbeschreibungen zeigt die **Schwerpunktsetzungen der beteiligten Organisationen** auf: Das AIT ist in mehreren Teilbereichen aktiv, darunter Quantenkommunikation, neue Methoden der Cybersecurity, Cybersecurity von Lieferketten und im Kontext von Industrie 4.0 sowie der Entwicklung der europaweit führenden Technologie zur Analyse von Blockchain-Transaktionen (siehe auch [157]).

Die Universitäten TU Graz und Universität Klagenfurt sind ebenso in mehreren Themenbereichen aktiv: So die TU Graz in Hardware-Security und e-Identität oder die Universität Klagenfurt in Blockhain und neuen Methoden für Resilienz gegen Angriffe. Die beiden Unternehmen mit den meisten Beteiligungen, Infineon Technologies GmbH, ein Halbleiterhersteller, und AVL-List GmbH, Hersteller von Antriebssystemen in der Automobilindustrie (4 bzw. 3 Projektbeteiligungen), sind beides keine Cybersecurity-Unternehmen im Sinne von Lösungsanbietern. Ihre europäischen FTI-Aktivitäten im Bereich Cybersecurity spiegelt die zunehmende **Notwendigkeit von Cybersecurity in „klassischen" Industriefeldern** wider: So ist die AVL-List GmbH an Projekten zur Cybersecurity für autonome und vernetzte Fahrzeuge oder die Infineon Technologies GmbH an Projekten zu kontaktlosen Sicherheitslösungen beteiligt.

Zu den weiteren Akteuren mit zwei oder mehr Projektbeteiligungen zählen vor allem Universitäten und Forschungsorganisationen, aber auch COMET-Kompetenzzentren („Compentece Centers for Excellent Technologies"), sowie Unternehmen vor allem aus der Automobilindustrie. Die Beteiligungsstruktur zeigt, dass insbesondere Wissenschafts- und Forschungseinrichtungen sowie forschungsstarke Unternehmen aus klassischen Industriefeldern im europäischen Forschungsrahmenprogramm aktiv sind. Dies untermauert den auch im Rahmen von Interviews und Workshop von Cybersecurity-ExpertInnen festgestellten **Mangel an österreichischen Unternehmen, die Cybersecurity-Lösungen** entwickeln und herstellen.

Tabelle 5: Österreichische Organisationen mit zwei oder mehr Projektteilnahmen

Organisation	Projektteilnahmen
AIT - Austrian Institute of Technology GmbH	9
Technische Universität Graz (TU Graz)	5
Universität Klagenfurt	4
Infineon Technologies AG	4
AVL - List GmbH - Gesellschaft für Verbrennungskraftmaschinen und Messtechnik Gmbh	3
Technikon Forschungs- und Planungsgesellschaft mbH	3
Minds & Sparks GmbH	3
Wirtschaftsuniversität Wien	2
Technische Universität Wien	2

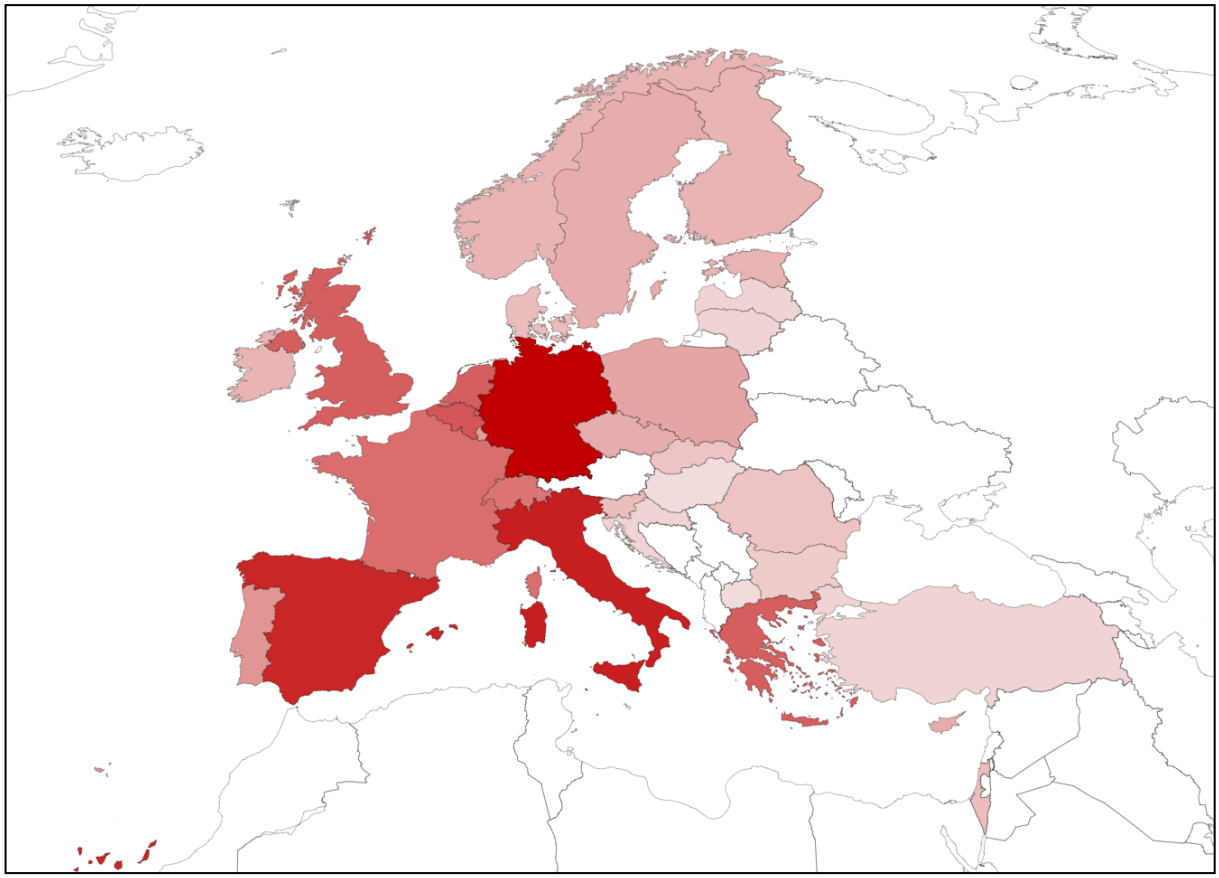
Secure Payment Technologies GmbH	2
D.M.A.T. Consulting KG	2
TTTech Industrial Automation AG	2
Evolaris Research & Development GmbH	2
SBA Research gemeinnützige GmbH	2
Fabasoft R&D GmbH	2
Stiftung Secure Information and Communications Technologies	2
Joanneum Research Forschungsgesellschaft mbH	2
TTTech Computertechnik AG	2
Know-Center GmbH	2
Universität Wien	2
Leopold-Franzens-Universität Innsbruck	2
Virtual Vehicle Research GmbH	2

5.1.3 Kooperationen Österreichs mit anderen Ländern

Abbildung 7 sowie Tabelle 6 (erste Spalte) zeigen die Häufigkeiten der Kooperationen Österreichs mit anderen Ländern in Cybersecurity-Projekten. Es zeigt sich, dass Österreich besonders oft mit **Deutschland, Italien, und Spanien i**n Cybersecurity-Projekten kooperiert. Aufgrund der unterschiedlichen Gesamtzahl der Projekte in den verschiedenen Ländern (siehe Tabelle 6, zweite Spalte) sind diese Ergebnisse jedoch nur bedingt aussagekräftig und spiegeln hauptsächlich die Beteiligung der Länder insgesamt wider.

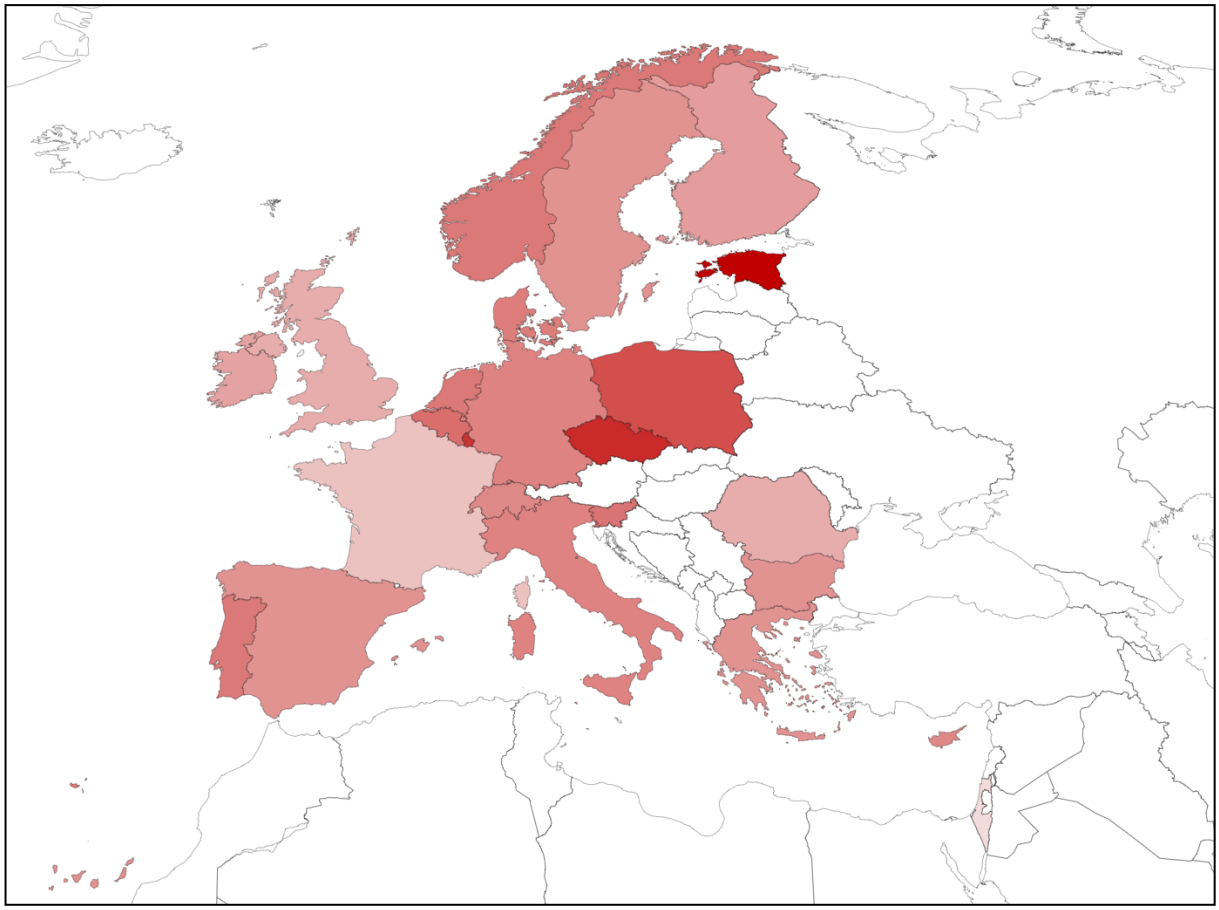
Abbildung 8 sowie Tabelle 6 (dritte Spalte) zeigen deshalb die Häufigkeit österreichischer Kooperationen relativ zur Gesamtzahl der Projekte der jeweiligen Länder, also die Kooperationshäufigkeit gewichtet nach der Gesamtaktivität der Länder. Hier wird deutlich, dass Österreich überdurchschnittlich häufig mit **Estland, Tschechien und Luxemburg** kooperiert, während mit Israel, Rumänien und dem Vereinigten Königreich verhältnismäßig selten in gemeinsamen Projekten gearbeitet wird. In Abbildung 8 werden Länder mit weniger als 6 Projekten insgesamt nicht dargestellt. Allerdings zeigt sich auch, dass insbesondere die Slowakei, Lettland, Litauen und die Türkei ebenfalls häufig mit Österreich kooperieren, diese Länder jedoch eine sehr geringe Gesamtanzahl an Projekten aufweisen.

Abbildung 7: Österreichische Kooperationen mit anderen Ländern.



Anm.: Die Farbe spiegelt die Anzahl der Projekte mit Österreich als Kooperationspartner wider (siehe Tabelle 6, erste Spalte).

Abbildung 8: Österreichische Kooperationen mit anderen Ländern relativ zur Gesamtzahl an Projekten.



Anm.: Die Farbe spiegelt den Anteil der Projekte mit österreichischer Beteiligung wider (siehe Tabelle 6, dritte Spalte). Länder mit unter 6 Projekten insgesamt wurden nicht in die Darstellung aufgenommen.

Tabelle 6: Österreichische Kooperationen mit anderen Ländern

Land	Projekte mit ö. Beteiligung	Projekte insgesamt	Anteil d. Projekte mit ö. Beteiligung
Deutschland	29	96	30 %
Italien	25	84	30 %
Spanien	24	89	27 %
Belgien	18	53	34 %
Griechenland	17	63	27 %
Niederlande	17	53	32 %
Vereinigtes Königreich	17	79	22 %
Frankreich	15	82	18 %
Schweiz	14	48	29 %
Portugal	10	31	32 %
Luxemburg	9	20	45 %
Polen	8	20	40 %
Zypern	7	24	29 %
Tschechien	7	15	47 %
Schweden	7	26	27 %
Estland	6	11	55 %
Finnland	6	24	25 %
Irland	6	25	24 %
Norwegen	6	19	32 %
Dänemark	5	16	31 %
Israel	5	38	13 %
Slowenien	5	15	33 %
Rumänien	4	18	22 %
Slowakei	4	5	80 %
Bulgarien	3	11	27 %
Kroatien	2	4	50 %
Lettland	2	3	67 %
Litauen	2	3	67 %
Türkei	2	3	67 %
Ungarn	1	5	20 %
Nordmazedonien	1	1	100 %

5.2 Forschungs-, Technologie- und Innovationsfelder

Die Analyse der Cybersecurity-Projekte in Horizon-2020 zeigt deutlich, dass österreichische Organisationen gut in die europäische Forschungslandschaft zu Cybersecurity eingebunden sind. Ergebnisse aus Interviews und Workshop legen ebenfalls nahe, dass hervorragende österreichische Forschungsgruppen einen wichtigen Beitrag zur internationalen Forschung und Innovation in Cybersecurity leisten. Österreichs FTI-Aktivitäten sind so laut befragten ExpertInnen insbesondere in folgenden Feldern bedeutsam:

- Quantenkryptographie
- Quantencomputing
- Hardwaresicherheit
- OT-Security

- E-Identität
- E-Government
- Neue Werkzeuge und Methoden der Cybersecurity (für Unternehmen im Kontext von Industrie 4.0, für öffentliche Organisationen und kritische Infrastrukturen)

Trotz der guten Positionierung Österreichs sind sich die ExpertInnen einig, dass Österreich **ungenutzte Potenziale** in FTI-Aktivitäten zu Cybersecurity hat und nehmen insbesondere in Wirtschaftsaktivitäten Schwächen wahr. In Österreich bestehe dahingehend ein eklatanter Fachkräftemangel. Laut ExpertInnen ist Österreich zudem in hohem Maß von Cybersecurity-Lösungen aus Drittstaaten abhängig – österreichische Anbieter von Cybersecurity-Lösungen gibt aus kaum. Das geringe Bewusstsein über Cybersecurity und die Risiken der Digitalisierung bedingt laut interviewten ExpertInnen eine geringe Nachfrage an Cybersecurity-Lösungen und beeinflusst somit auch die österreichische Cybersecurity-Unternehmenslandschaft.

Um Österreichs Innovationssystem in Cybersecurity zu stärken, gilt es laut ExpertInnen, den FTI-Standort Österreich zu stärken, Forschung zu fördern sowie **Ausbildungs- und Karrieremodelle** in Cybersecurity zu modernisieren und attraktiver zu gestalten. So werden laut einer Studie der IV mehr Anreize und positives Marketing für Ausbildungen und Karrierepfade in Cybersecurity benötigt, um dem Fachkräftemangel entgegenzuwirken [1]. Als wichtige Grundlage für erfolgreiche FTI-Aktivitäten in Österreich wird zudem das generelle Bewusstsein zu Cybersecurity-Themen in der Gesellschaft gesehen.

Als Strategie für FTI-Aktivitäten empfehlen die ExpertInnen, sich auf existierende **Stärken** zu konzentrieren und **Nischenthemen**, in denen Österreich erfolgreich ist, weiter auszubauen. Hierbei gilt es, sowohl die „Hidden Champions“ in Österreich zu erkennen und zu fördern, sowie die Angebote großer Cybersecurity-Anbieter sinnvoll zu ergänzen bzw. Lücken im vorhandenen Angebot zu schließen.

Interviews und Workshops ergaben zudem einige FTI-Felder mit hohem Innovationspotenzial, die auch für zukünftige Aktivitäten in Österreich als besonders relevant angesehen werden. Die genannten Themenbereiche umfassen die folgenden Felder:

- Cybersecurity-Aspekte im Kontext der Entwicklung von künstlicher Intelligenz und Machine Learning
- Blockchain
- Desinformationserkennung
- Cybersecurity im Kontext von IoT und Smart Devices
- Cybersecurity in Sensorik
- Ethik in Cybersecurity
- Cybersecurity-Aspekte im Bereich der Quantentechnologie und Quantenkryptographie

Im Rahmen von Interviews und Workshop haben ExpertInnen zudem die Notwendigkeit eines gemeinsamen Verständnisses des Themas Cybersecurity und an verstärkter **Zusammenarbeit zwischen Disziplinen und Stakeholdergruppen**, um Doppelgleisigkeiten und „Silodenken“ zu vermeiden identifiziert. Vor dem Hintergrund der sehr guten Positionierung der österreichischen Cybersecurity-FTI wird so die Kommunikation von Forschungsergebnissen an andere Forschende, FTI-Akteure in anderen Themenfeldern und darüber hinaus an Nicht-ExpertInnen, Politik und Gesellschaft als besonders bedeutend angesehen. So könnten thematische Synergien effektiver genutzt werden und die Relevanz von Cybersecurity für politisches Handeln sowie das Verhalten von Einzelpersonen effektiver kommuniziert werden. Gezielter Wissenstransfer zwischen Universitäten, Forschungsorganisationen und Unternehmen könnte auch einen wichtigen Mehrwert für die Cybersecurity Forschung und Innovation darstellen.

5.3 Zusammenfassung und Fazit

- Österreichische Forschung und Innovation spielt in **Europa eine bedeutende Rolle**. Österreich ist in europäischen Projekten zu Cybersecurity sehr gut vertreten und österreichische Forschungsgruppen leisten zu verschiedenen angewandten sowie Grundlagenthemen einen wichtigen Beitrag. Trotz der bereits guten Positionierung gibt es in Österreich ungenutzte Potenziale im Cybersecurity- (Innovations-) Ökosystem.

- Österreichische FTI-Akteure sind in einigen Themenbereichen **international sichtbar** und exzellent, auch sind Unternehmen aus klassischen Industriefeldern aktiv in Cybersecurity-Forschung und Innovation auf europäischer Ebene.
- Im Rahmen von Interviews und Workshop wurden Österreichs **FTI-Stärkefelder** identifiziert. Dazu gehören unter anderem Quantenkryptographie und Quantencomputing, Hardwaresicherheit, OT-Security, E-Identität, E-Government sowie neue Werkzeuge und Methoden der Cybersecurity.
- Von befragten Cybersecurity-ExpertInnen wurden die Themenbereiche Cybersecurity im Kontext von künstlicher Intelligenz, Blockchain, IoT, Sensorik und Quantentechnologie als FTI-Felder mit besonders **hohem Innovationspotenzial** für die Zukunft gesehen.

6. Schlussfolgerungen und Handlungsempfehlungen

6.1 Cybersecurity ist ein Thema mit hoher gesellschaftlicher Relevanz

Mit der fortschreitenden **Digitalisierung** und der Durchdringung aller Aspekte des Lebens durch digitale Technologien verwandelte sich auch der Sicherheitsaspekt von rein technisch-bezogener IT-Security in ein breiteres Verständnis der Cybersecurity. Cybersecurity ist nunmehr ein Synonym für **umfassenden Schutz des digitalen Lebens** und soll somit auch die Vielschichtigkeit des Themas signalisieren**.**

Die Digitalisierung und der steigende Vernetzungsgrad bewirkt, dass Cybersecurity nun alle Gesellschaftsbereiche und Akteure, von Staaten und Unternehmen bis hin zu Einzelpersonen, betrifft. In diesem Sinne bezieht sich Cybersecurity nicht nur auf das Verhindern vorsätzlicher Cyberattacken, sondern auch auf die zahlreichen anderen vielschichtigen **Risiken für AnwenderInnen und Gesellschaft**. Dazu zählen etwa Bedenken zum Datenschutz und der Privatsphäre, wenn AnwenderInnen mit einer stetig wachsenden Zahl an Kameras, Mikrofonen und Sensoren ausgestattet sind, oder die befürchteten Einschränkungen der Entscheidungs- und Meinungsfreiheit, wenn durch automatisierte Systeme der Informationsstrom zunehmend personalisiert und gefiltert wird.

Die zunehmende **Professionalisierung** der AngreiferInnen, die Entwicklung von Ransomware-Geschäftsmodellen sowie die effektiveren Angriffsmethoden, z.B. Ransomware, DDoS, APT, stellt Cybersecurity vor wachsende Herausforderungen. Durch die steigende Gefahr von hybriden Bedrohungen und Cyber Warfare, also die von Staaten geduldeten oder geförderten Angriffe auf staatliche Institutionen, kritische Infrastrukturen oder gezielte Verbreitung von Desinformation, entstehen auch Risiken für gesellschaftliche Strukturen und demokratische Grundwerte. Nur durch Cybersecurity kann diesen Gefahren begegnet und demokratische Institutionen gestärkt werden.

Angesichts der Bedeutung von Cybersecurity haben interviewte ExpertInnen sowie TeilnehmerInnen des Workshops einstimmig ein **fehlendes Bewusstsein** für Cybersecurity sowie den Auswirkungen der Digitalisierung festgestellt. Dies betrifft alle Akteure, von Organisationen und Unternehmen bis hin zu Einzelpersonen und EndnutzerInnen.

Handlungsempfehlung 1: Bewusstsein über Cybersecurity in der Gesellschaft stärken

Die Digitalisierung hat in den letzten Jahren viele Handlungsfelder geschaffen, mit denen sich Österreich weit mehr als bisher beschäftigen muss. Neuartigen Trends, Gefahren, Risiken und Entwicklungen muss proaktiv begegnet und entgegengewirkt werden. Dabei ist es wichtig, in der breiten Bevölkerung, bei Unternehmen wie auch bei Einzelpersonen aller Altersgruppen ein hohes Maß an Grundverständnis und Bewusstsein zu entwickeln. Vor dem Hintergrund der hohen gesellschaftlichen Relevanz von Cybersecurity und dem gleichzeitig festgestellten Mangel an Bewusstsein über die Risiken der Digitalisierung sind Maßnahmen zur Bewusstseinsbildung über Cybersecurity für Politik, Privatunternehmen bis hin zur Bevölkerung und Einzelpersonen zu empfehlen (siehe auch [1]). Gleichzeitig könnte somit ein gesellschaftlicher Diskurs über Cybersecurity und die proaktive Auseinandersetzung mit den Folgen der Digitalisierung forciert werden. Für Organisationen und Unternehmen könnten im Rahmen der Bewusstseinsbildung **Cybersecurity-Übungen und Trainings** unter Anwendung moderner Ansätze umgesetzt werden (siehe auch [2]). Bewusstseinsbildung bei Einzelpersonen sollte im Kontext der **Digital Literacy** geschehen. Digital Literacy bezeichnet die Fähigkeit, sich sicher in einer digitalen Gesellschaft bewegen und dort auch lernen und arbeiten zu können. Diese Fähigkeit sollten im Idealfall schon in jungen Jahren, beispielsweise im Rahmen der Schulausbildung, erlernt und ständig weiterentwickelt werden.

Handlungsempfehlung 2: Cybersecurity als integralen Bestandteil von IKT-Produkten und Services etablieren und Security-by-Design Methoden anwenden

In engem Zusammenhang mit dem schwach ausgeprägten Bewusstsein über Cybersecurity und die Risiken der Digitalisierung steht auch das Verständnis von Cybersecurity als rein technisches Thema. Durch die

fortschreitende Vernetzung hat sich Cybersecurity jedoch längst zu einem gesellschaftlichen Querschnittsthema gewandelt. Vor diesem Hintergrund sollte Cybersecurity als integraler Bestandteil von IKT-Produkten und Services betrachtet werden. Zum Beispiel sollten **Security-by-Design Methoden** beim Aufbau und der Konzeption neuer IKT-Systeme, Netzwerke oder Software berücksichtigt werden. So können Sicherheitseigenschaften bereits initial als Designkriterium integriert werden. Dadurch lassen sich Systemfehler vermeiden und potenziellen AngreiferInnen werden kleinere Angriffsflächen geboten.

Handlungsempfehlung 3: Foresight für Cybersecurity durchführen

Um den **gesellschaftlichen Diskurs** mit Cybersecurity zu forcieren und eine **proaktive Auseinandersetzung** mit Cybersecurity und den Auswirkungen der Digitalisierung zu implementieren, wird ein Foresight-Prozess zu Cybersecurity empfohlen. In diesem Rahmen kann durch Einbindung von PolitkvertreterInnen, ExpertInnen, Stakeholdern und BürgerInnen eine gesamtgesellschaftliche Diskussion über die Folgen der Digitalisierung und deren Auswirkungen auf Sicherheitsaspekte etabliert werden. Dies könnte zugleich einen Beitrag zur höheren Akzeptanz der digitalen Transformation und Etablierung einer Cybersecurity-Kultur leisten (siehe auch [2]).

6.2 Cybersecurity stellt höhere Ansprüche an Kooperation und Koordination

Neben der hohen gesellschaftlichen Relevanz ist Cybersecurity auch rechtlich eine Querschnittsmaterie. Die Vielschichtigkeit und Komplexität des Themas bedingt darüber hinaus intensive Koordination, Kooperation, Informationsaustausch und gegenseitige Lernprozesse auf allen Akteursebenen. In diesem Zusammenhang wird der nationale Handlungsrahmen durch die Österreichische Cybersicherheit-Strategie und auf europäischer Ebene durch die Europäische Cybersecurity-Strategie gesetzt. Cybersecurity wird national durch das Bundeskanzleramt koordiniert, zusätzlich sind das Bundesministerium für Inneres, das Bundesministerium für europäische und internationale Angelegenheiten und das Bundesministerium für Landesverteidigungen ebenso für Aspekte von Cybersecurity zuständig. Auf strategischer und operativer Ebene wurde eine interministerielle Koordinationsstruktur etabliert, die Public-Private Partnership Cyber-Sicherheit-Plattform soll zudem den Austausch und die Koordination zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung fördern.

In den Interviews und im Workshop wurde von den ExpertInnen die grundsätzlich gute Vernetzung innerhalb der Cybersecurity-Community hervorgehoben. Jedoch wurde trotz der etablierten Strukturen der Bedarf nach intensiverer und effektiverer Koordination und Abstimmung zwischen Akteuren und Stakeholdern geäußert. Dies betrifft einerseits die Koordination zwischen **staatlichen und privaten Akteuren**, andererseits die **Kooperation auf operativer Ebene**. In diesem Zusammenhang wurde im Rahmen von Interviews und Workshop auch der Bedarf nach aktiver Gestaltung von Digitalisierung und Cybersecurity geäußert. Einerseits würde das eine proaktive Auseinandersetzung mit Cybersecurity auf allen Ebenen, andererseits auch die proaktive Gestaltung und Positionierung Österreichs in diesem Themengebiet auf europäischer und internationaler Ebene bedeuten. Cybersecurity ist ein länderübergreifendes Thema und kann zudem nicht durch eine einzelne Gruppe von Akteuren oder Stakeholdern erreicht werden.

Handlungsempfehlung 4: Koordination und Kooperation zwischen Akteuren und Stakeholdern stärken

Um der Vielschichtigkeit und Komplexität des Themas gerecht zu werden, sollte die Kooperation und der Austausch auf **operativer Ebene**, genauer gesagt zwischen CERTs, CSIRTs, sowie mittels etablierter Informationsaustauschplattformen (z.B. CSP), gestärkt werden. Zusätzlich sollte auch die Abstimmung zwischen öffentlichen und privaten Akteuren intensiviert werden. Die CSP könnte in diesem Kontext eine prominentere Rolle einnehmen, indem Formate und Prozesse für **bidirektionalen Informationsaustausch** verstärkt werden. Gleichzeitig sollte auch die Kooperation zwischen staatlichen Institutionen und Forschungsakteuren sichergestellt werden, um geeignete Rahmenbedingungen und Schutzmechanismen etablieren zu können (siehe auch [2]). Die effektivere Abstimmung und Kooperation der Akteure könnten das proaktive strategische, politische und gesetzliche Handeln sowie die Steuerung des Cybersecurity-Themas unterstützen.

Handlungsempfehlung 5: Aktive Gestaltung auf europäischer und internationaler Ebene vornehmen

Vor dem Hintergrund der steigenden Risiken von Cyber Warfare ist ein europäisch und international koordiniertes Handeln in Cybersecurity von hoher Relevanz. Österreich verfolgt bereits Aktivitäten und Maßnahmen im Bereich der **Cyberdiplomatie**, und auch auf europäischer Ebene ist Cyberdiplomatie ein zentraler Bestandteil der Cybersecurity-Strategie. Bestrebungen in Cyberdiplomatie und der internationalen Koordination sollten weiter verstärkt werden.

Darüber hinaus könnte sich Österreich und Europa durch existierende **thematische Stärken und Aktivitäten** auch international positionieren. Durch den europäischen Cybersecurity Act wurde ein Rahmen für die Etablierung von Cybersecurity-Zertifizierungsschemen in Produkten, Prozessen und Dienstleistungen geschaffen und die ENISA mit der Entwicklung von Zertifizierungsschemen betraut. Österreich kann in diesem Feld mit wachsender Relevanz Vorbildfunktion einnehmen. Das **österreichische Gütesiegel für Cybersecurity** „Cyber Trust Austria Label" des KSÖ ist das erste dieser Art in der EU. Zudem wurde bereits ein österreichisches CyberRisk Rating etabliert, um digitale Risiken in globalen Lieferketten sichtbar zu machen und Unternehmen mit einem standardisierten Cyber-Risikomanagement für Lieferanten zu unterstützen.

6.3 Österreichische Forschung in Cybersecurity spielt eine bedeutende Rolle auf europäischer Ebene

Die Analyse der österreichischen Beteiligung im europäischen Forschungsrahmenprogramm Horizon 2020 zeigt auf, dass österreichische Organisationen eine bedeutende Rolle einnehmen können und eine hohe Beteiligung an Cybersecurity-Projekten aufweisen. Interviews und Workshop bestätigen dieses Ergebnis: die befragten Cybersecurity-ExpertInnen verweisen einstimmig auf die Existenz mehrerer exzellenter, international sichtbarer Forschungsgruppen an Österreichs Universitäten, Forschungsorganisationen und Unternehmen.

Im Rahmen der Interviews und des Workshops wurden österreichische FTI-Aktivitäten, unter anderem in kooperativen europäischen und nationalen Forschungsprojekten, in Feldern wie **Quantenkryptographie, Quantencomputing, Hardwaresicherheit, neue Werkzeuge und Methoden** der Cybersecurity für öffentliche Organisationen und kritische Infrastrukturen als besondere Stärkefelder genannt. Darüber hinaus wurden durch die Programmdatenanalyse von Horizon 2020 österreichische Beteiligungen an FTI-Aktivitäten zu Cybersecurity in Produkten und Prozessen identifiziert, die durch die digitale Transformation einer zunehmenden Vernetzung erfahren (z.B. Automobilindustrie, Lieferketten). Dies weist auf ein bestehendes Potenzial in der Innovation und Integration von **Cybersecurity in klassischen Industriefeldern** hin. Darüber hinaus haben ExpertInnen im Rahmen von Interviews und Workshops die Bereiche **OT-Security, E-Identität** und **E-Government** als zusätzliche Stärkefelder Österreichs identifiziert.

Zudem verwiesen ExpertInnen in Interviews und im Workshop auf eine Reihe an FTI-Feldern mit wachsender Bedeutung und hohem Innovationspotenzial. Dazu gehören Cybersecurity-Aspekte im Kontext der Entwicklung von **Künstlicher Intelligenz und Machine Learning**, **Blockchain**, **Desinformationserkennung, Cybersecurity im Kontext von IoT und Smart Devices** sowie **Ethik in Cybersecurity.** Entwicklungen in der Quantentechnologie könnten ebenso eine Innovationschance für Österreich darstellen, nicht zuletzt aufgrund von existierenden FTI-Aktivitäten in den Bereichen **Quantenkryptographie** und **Quantencomputing.**

Handlungsempfehlung 6: Stärkefelder und Nischen ausbauen

Auf Basis der bereits sehr guten Positionierung der österreichischen FTI-Akteure auf europäischer Ebene sollte die österreichische Cybersecurity-Forschung weiter gestärkt werden. Aufgrund der Vielschichtigkeit des Cybersecurity-Themenbereichs ist es empfehlenswert, auf **bestehende Stärkefelder** und **Nischen mit Zukunftspotenzial** zu fokussieren. Zu den Stärkefeldern zählen unter anderem Hardwaresicherheit, neue Werkzeuge und Methoden der Cybersecurity, OT-Security, E-Identität und E-Government. Nischen mit Zukunftspotenzial sollten identifiziert und aktiv durch **gezielten Kompetenzaufbau** gefördert werden. Dazu zählen Maßnahmen wie Förderung der Grundlagenforschung, Einrichtung von Lehrstühlen sowie die Förderung

von angewandter, intersektoraler und interdisziplinärer (Sicherheits-) Forschung. Cybersecurity-Aspekte in aktuellen FTI-Feldern wie Künstliche Intelligenz/Machine Learning, Blockchain und Quantencomputing könnten Chancen für österreichische FTI bieten.

Handlungsempfehlung 7: Wissenschaftskommunikation und Wissenstransfer stärken

Um die Anwendbarkeit von Forschungsergebnissen und deren Verbreitung vor allem in der breiten Bevölkerung zu erhöhen, ist es empfehlenswert, Maßnahmen zur Wissenschaftskommunikation und Wissenstransfer zu stärken. Der effektive Wissenstransfer zwischen Wissenschaft, Wirtschaft, Gesellschaft und Politik könnte neben der Sicherstellung der Anwendbarkeit der Ergebnisse für andere FTI-Akteure und andere Disziplinen auch einen Beitrag zur Bewusstseinsbildung über Cybersecurity und den Risiken der Digitalisierung leisten. Die Aufbereitung von Forschungsergebnissen in für Laien nachvollziehbarer Art und Weise, z.B. in Form von „Kids' Corners" auf Webseiten, könnte eines der Maßnahmen darstellen.

6.4 Österreich hat ungenutzte Potenziale für ein Cybersecurity-(Innovations-) Ökosystem

Während die Analyse der österreichischen Beteiligungen im europäischen Forschungsrahmenprogramm Horizon 2020 eine sehr gute Positionierung österreichischer FTI-Akteure aufgezeigt hat, die mehrfach in Interviews und Workshop bestätigt wurde, wurde von den befragten ExpertInnen gleichzeitig eine Schwäche des Innovations- und Wirtschaftszweigs Cybersecurity festgestellt. Österreich und Europa sind in diesem Kontext abhängig von Cybersecurity-Lösungen aus Drittstaaten; es gibt kaum österreichische Lösungsanbieter. Die ExpertInnen schreiben diese Problematik vor allem einem fehlenden **Ökosystem** für den Wirtschaftszweig Cybersecurity zu. Zum einen besteht ein **Fachkräftemangel** vor dem Hintergrund der erwarteten steigenden Nachfrage, gleichzeitig auch ein Mangel sowohl an Lösungsanbietern als auch an Cybersecurity-Dienstleistern.

Handlungsempfehlung 8: Den Wirtschaftszweig Cybersecurity gezielt aufbauen und stärken

Vor dem Hintergrund der festgestellten Schwäche in der Cybersecurity-Unternehmenslandschaft und dem Mangel an Cybersecurity-ExpertInnen wird empfohlen, einen Schwerpunkt in die Unterstützung von Cybersecurity-Unternehmen zu legen. Einerseits sollte die **Ausbildung** von Cybersecurity-ExpertInnen, vor allem in außeruniversitären Ausbildungsstätten in der Lehre, Höheren Technischen Lehranstalten und Fachhochschulen zu forcieren. Andererseits sollten Maßnahmen in der Förderung von Cybersecurity-Lösungsanbietern und Dienstleistern umgesetzt werden. Dazu könnten **Anreize für Wirtschaftsansiedlungen**, Risikokapital für innovative Unternehmensgründungen sowie Maßnahmen zur Vernetzung der Unternehmen im Bereich Entwicklung von Cybersecurity-Lösungen zählen.

7. Literaturverzeichnis

[1] S. Borgas *u. a.*, „Digital.Erfolgreich.Industrie. - Transformation zum digitalen Österreich 2030+“. Vereinigung der österreichischen Industrie (Industriellenvereinigung), 2021. [Online]. Verfügbar unter: https://www.iv.at/Themen/Aktuelle-Schwerpunkte/Aktionsplan-digitales--sterreich/Industrie-praesentiert-Aktionsplan-fuer-digitales-Oesterr.html

[2] H. Leopold, „Cybersicherheit und Datensouveränität für eine zuverlässige digitale Zukunft Europas“, in *30 Ideen für Europa*, Wien: Österreichische Gesellschaft für Europapolitik (Hg.), 2021.

[3] M. Dinges *u. a.*, „5G supply market trends“. Luxembourg: Publications Office of the European Union, 2021. Zugegriffen: Okt. 12, 2021. [Online]. Verfügbar unter: https://op.europa.eu/en/publication-detail/-/publication/074df4ff-f988-11eb-b520-01aa75ed71a1

[4] B. R. Sharton, „Ransomware Attacks Are Spiking. Is Your Company Prepared?“, *Harvard Business Review*, Mai 20, 2021. Zugegriffen: Dez. 01, 2021. [Online]. Verfügbar unter: https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

[5] KPMG, „Cyber Security in Österreich 2021“, Apr. 2021. [Online]. Verfügbar unter: https://home.kpmg/at/de/home/insights/2021/04/cyber-security-in-oesterreich-2021.html

[6] NIST, „INFOSEC - Glossary“, *NIST*, n.V. https://csrc.nist.gov/glossary/term/infosec (zugegriffen Dez. 01, 2021).

[7] J. Alvarez, Stanford, und C. 94305 C. Complaints, „Stuxnet: The world’s first cyber weapon“, *Stanford Center for International Security and Cooperation*, Feb. 03, 2015. https://cisac.fsi.stanford.edu/news/stuxnet (zugegriffen Dez. 01, 2021).

[8] Datenschutzbehörde, „Datenschutzrecht in Österreich“, *Datenschutzbehörde*, n.V. https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html (zugegriffen Nov. 25, 2021).

[9] S. Durbin, „Cybercrime: The Next Entrepreneurial Growth Business?“, *Wired*, Okt. 14, 2014. Zugegriffen: Dez. 01, 2021. [Online]. Verfügbar unter: https://www.wired.com/insights/2014/10/cybercrime-growth-business/

[10] S. Andriole, „Cyberwarfare Will Explode In 2020 (Because It’s Cheap, Easy And Effective)“, *Forbes*, Jan. 14, 2020. https://www.forbes.com/sites/steveandriole/2020/01/14/cyberwarfare-will-explode-in-2020-because-its-cheap-easy--effective/ (zugegriffen Dez. 01, 2021).

[11] University of San Diego, „Cybersecurity vs. Information Security vs. Network Security“, *University of San Diego*, Jan. 27, 2020. https://onlinedegrees.sandiego.edu/cyber-security-information-security-network-security/ (zugegriffen Nov. 25, 2021).

[12] Accenture, „COVID-19: Unternehmenssysteme resilient gestalten | Accenture“, *Accenture*, n.V. https://www.accenture.com/at-de/about/company/coronavirus-systems-resilience (zugegriffen Dez. 10, 2021).

[13] CISA, „What is Cybersecurity?“, Mai 06, 2009. https://us-cert.cisa.gov/ncas/tips/ST04-001 (zugegriffen Sep. 08, 2021).

[14] IBM, „What is Cybersecurity?“, n.V. https://www.ibm.com/topics/cybersecurity (zugegriffen Nov. 25, 2021).

[15] Bundeskanzleramt, „Cybersicherheit - Bundeskanzleramt Österreich“, *Bundeskanzleramt*, n.V. https://www.bundeskanzleramt.gv.at/themen/cybersicherheit.html (zugegriffen Sep. 08, 2021).

[16] European Commission, „The EU Cybersecurity Act“, S. 55, Apr. 2019.

[17] R. Tirtea, „ENISA overview of cybersecurity and related terminology“, S. 8, 2017.

[18] BMI, „Internetkriminalität“, *Bundesministerium Inneres*, n.V. https://bundeskriminalamt.at/306/start.aspx (zugegriffen Nov. 25, 2021).

[19] CISCO, „What Is Cybersecurity?“, *Cisco*, n.V. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html (zugegriffen Sep. 08, 2021).

[20] S. Hofer, „‚You are fucked‘: Wie Hacker SalzburgMilch lahmlegten“, *Profil*, Aug. 19, 2021. https://profil.at/gesellschaft/you-are-fucked-wie-hacker-salzburgmilch-lahmlegten/401471785 (zugegriffen Nov. 25, 2021).

[21] Der Standard, „Cyberangriff auf 34 Firmen in Oberösterreich“, *Der Standard*, Sep. 02, 2021. https://www.derstandard.at/story/2000129348698/cyberangriff-auf-34-firmen-in-oberoesterreich (zugegriffen Nov. 25, 2021).

[22] Salzburger Nachrichten, „Cybercrime Report - Internetbetrug blieb 2020 Topdelikt“, *Salzburger Nachrichten*, Aug. 11, 2021. https://www.sn.at/panorama/oesterreich/cybercrime-report-internetbetrug-blieb-2020-topdelikt-107867917 (zugegriffen Nov. 25, 2021).

[23] A. Abrams, „Here’s What We Know So Far About Russia’s 2016 Meddling“, *Time*, Apr. 18, 2019. https://time.com/5565991/russia-influence-2016-election/ (zugegriffen Sep. 23, 2021).

[24] J. Hincks, „British Lawmakers Fear Brexit Vote Website Was Hacked“, *Time*, Apr. 12, 2017. https://time.com/4735665/brexit-vote-foreign-cyber-attack/ (zugegriffen Nov. 25, 2021).

[25] W. Worley, „The FBI are ‚investigating the role of Breitbart in spreading fake news with bots‘“, *The Independent*, März 22, 2017. https://www.independent.co.uk/news/world/americas/us-politics/fbi-breitbart-investigate-alt-right-wing-websites-fake-news-bots-donald-trump-a7641826.html (zugegriffen Nov. 25, 2021).

[26] C. Brooks, „3 Key Cybersecurity Trends To Know For 2021 (and On ...)“, *Forbes*, Apr. 12, 2021. https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/ (zugegriffen Nov. 25, 2021).
[27] A. Blankstein, „U.S. indicts three North Koreans in massive WannaCry, Sony hacks“, *NBC News*, Feb. 17, 2021. https://www.nbcnews.com/politics/justice-department/u-s-indicts-three-north-koreans-massive-wannacry-sony-hacks-n1258096 (zugegriffen Nov. 25, 2021).
[28] US Department of Justice, „North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions“, *The United States Department of Justice*, Sep. 06, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (zugegriffen Nov. 25, 2021).
[29] Center for Stategic and International Studies, „Significant Cyber Incidents“, *Significant Cyber Incidents | Center for Strategic and International Studies*, Okt. 2012. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (zugegriffen Nov. 25, 2021).
[30] N. Grundmeier, „C.I.A. Prinzip | Sicherheitslücken im Internet“, *Informatik Uni Oldenburg*, n.V. http://www.informatik.uni-oldenburg.de/~iug10/sli/indexd917.html?q=node/19 (zugegriffen Nov. 25, 2021).
[31] M. Swanson, J. Hash, und P. Bowen, „Guide for developing security plans for federal information systems“, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-18r1, 2006. doi: 10.6028/NIST.SP.800-18r1.
[32] GDPR.EU, „What is GDPR, the EU’s new data protection law?“, *GDPR.eu*, Nov. 07, 2018. https://gdpr.eu/what-is-gdpr/ (zugegriffen Sep. 08, 2021).
[33] humanrights.ch, „Informationelle Selbstbestimmung - (noch) kein neues Grundrecht“, *humanrights.ch*, Okt. 26, 2017. https://www.humanrights.ch/de/ipf/menschenrechte/privatsphaere/informationelle-selbstbestimmung (zugegriffen Dez. 10, 2021).
[34] Kapersky, „Was ist Social Engineering?“, *www.kaspersky.de*, Jan. 13, 2021. https://www.kaspersky.de/resource-center/definitions/social-engineering (zugegriffen Nov. 25, 2021).
[35] Kapersky, „What Is an Advanced Persistent Threat (APT)?“, *www.kaspersky.com*, Juni 11, 2021. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats (zugegriffen Dez. 12, 2021).
[36] M. J. Schwartz, „Cybercrime-as-a-Service Economy: Stronger Than Ever“, *Bank Info Security*, Sep. 14, 2016. https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396 (zugegriffen Nov. 25, 2021).
[37] ENISA, „Das Jahr im Rückblick - ENISA Threat Landscape“, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-a-year-in-review-ebook-en-de.pdf (zugegriffen Sep. 08, 2021).
[38] AV-Test, „Sicherheitsreport 2019-2020“. https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2019-2020.pdf (zugegriffen Dez. 10, 2021).
[39] CISCO, „What is Malware? - Definition and Examples“, *Cisco*, n.V. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (zugegriffen Dez. 07, 2021).
[40] ENISA, „Schadprogramme (Malware)“, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-malware-ebook-en-de.pdf (zugegriffen Nov. 25, 2021).
[41] ENISA, „Webbasierte Angriffe“, *ENISA*, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-web-based-attacks-ebook-en-de.pdf (zugegriffen Nov. 25, 2021).
[42] ENISA, „Phishing“, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-phishing-ebook-en-de.pdf (zugegriffen Nov. 25, 2021).
[43] ENISA, „Angriffe auf Webanwendungen“, *ENISA*, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-web-application-attacks-ebook-en-de.pdf (zugegriffen Nov. 25, 2021).
[44] OWASP, „SQL Injection“, n.V. https://owasp.org/www-community/attacks/SQL_Injection (zugegriffen Dez. 13, 2021).
[45] OWASP, „Cross Site Scripting (XSS) Software Attack“, *OWASP*, n.V. https://owasp.org/www-community/attacks/xss/ (zugegriffen Dez. 13, 2021).
[46] ENISA, „Spam“, *ENISA*, 2020. https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-spam-ebook-en-de.pdf (zugegriffen Nov. 25, 2021).
[47] Der Standard, „Starker Anstieg der Cyberkriminalität in Österreich“, *Der Standard*, Aug. 11, 2021. https://www.derstandard.at/story/2000128847102/starker-anstieg-der-cyberkriminalitaet-in-oesterreich (zugegriffen Nov. 25, 2021).
[48] Handelsblatt, „Homeoffice: 52 Milliarden Euro Schaden durch Cyberangriffe“, *Nachrichtenmagazin*, Aug. 23, 2021. https://www.handelsblatt.com/technik/it-internet/studie-52-milliarden-euro-schaden-durch-cyberangriffe-im-homeoffice/27541742.html?ticket=ST-767070-eeGJvwg5mTzCRNHnND94-cas01.example.org (zugegriffen Nov. 25, 2021).
[49] SingCERT, „Social Media And Cybersecurity“, *The Singapore Computer Emergency Response Team*, Mai 03, 2021. https://www.csa.gov.sg/singcert/Publications/social-media-and-cybersecurity (zugegriffen Nov. 25, 2021).

[50] M. von Spreti und P. J. Wirnsperger, „Gefahr durch Fake News“, *Deloitte Deutschland*, n.V. https://www2.deloitte.com/de/de/pages/risk/articles/gefahr-durch-fake-news.html (zugegriffen Nov. 25, 2021).
[51] M. Fisher, „Disinformation for Hire, a Shadow Industry, Is Quietly Booming“, *The New York Times*, Juli 25, 2021. Zugegriffen: Nov. 25, 2021. [Online]. Verfügbar unter: https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html
[52] ENISA, „Aufkommende Trends“, ENISA, 2020. Zugegriffen: Nov. 25, 2021. [Online]. Verfügbar unter: https://www.enisa.europa.eu/publications/report-files/ETL-translations/de/etl2020-emerging-trends-ebook-en-de.pdf
[53] B. Schneier, „Hackers Used to Be Humans. Soon, AIs Will Hack Humanity“, *Wired*. Zugegriffen: Nov. 25, 2021. [Online]. Verfügbar unter: https://www.wired.com/story/opinion-hackers-used-to-be-humans-soon-ais-will-hack-humanity/
[54] W. Rjaibi, S. Muppidi, und M. O'Brien, „Quantum computing and cybersecurity: How to capitalize on opportunities and sidestep risks“, *IBM*, Juli 18, 2018. https://www.ibm.com/report/quantumsecurity (zugegriffen Dez. 10, 2021).
[55] P. H. O'Neill, „The US is worried that hackers are stealing data today so quantum computers can crack it in a decade“, *MIT Technology Review*, Nov. 03, 2021. https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/ (zugegriffen Nov. 25, 2021).
[56] K. Putman, „Deepfakes: Preparing for a New Threat“, *WordPressBlog*, Okt. 06, 2020. https://www.accenture.com/nl-en/blogs/insights/deepfakes-how-prepare-your-organization (zugegriffen Nov. 25, 2021).
[57] KSÖ und KPMG, „Neue KPMG/KSÖ: ‚Cyber Security in Österreich' - Kuratorium Sicheres Österreich“, n.V. https://kuratorium-sicheres-oesterreich.at/studienveroeffentlichung-cyber-security-in-oesterreich/ (zugegriffen Nov. 25, 2021).
[58] Der Standard, „Firmen fehlen mehr als 24.000 IT-Fachkräfte“, *Der Standard*, Apr. 06, 2021. https://www.derstandard.at/story/2000125555479/firmen-fehlen-bis-zu-10-000-it-fachkraefte (zugegriffen Nov. 25, 2021).
[59] F. Kenyon, „China's 'splinternet' will create a state-controlled alternative cyberspace“, *The Guardian*, Juni 03, 2021. Zugegriffen: Nov. 04, 2021. [Online]. Verfügbar unter: https://www.theguardian.com/global-development/2021/jun/03/chinas-splinternet-blockchain-state-control-of-cyberspace
[60] R. Neidinger, „Europa- und verfassungsrechtliche Rahmenbedingungen der Netzneutralität“, *Würzburger Online-Schriften zum Europarecht*, Bd. 10, S. 1283 KB, 53 pages, 2020, doi: 10.25972/OPUS-19829.
[61] Bundesamt für Sicherheit in der Informationstechnik, „Darknet und Deep Web – wir bringen Licht ins Dunkle“, *Bundesamt für Sicherheit in der Informationstechnik*. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deepweb.html;jsessionid=C48C2A936F225C8D5C40E7EC48CBF009.internet082?nn=131942 (zugegriffen Nov. 25, 2021).
[62] T. Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media*. New Haven: Yale University Press, 2018.
[63] J. Haas, „Freedom of the Media and Artificial Intelligence“, 2020, S. 12. [Online]. Verfügbar unter: https://www.osce.org/files/f/documents/4/5/472488.pdf
[64] Amnesty International, „Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights“, 2019. Zugegriffen: Dez. 13, 2021. [Online]. Verfügbar unter: https://www.amnesty.org/en/wp-content/uploads/2021/05/POL3014042019ENGLISH.pdf
[65] N. Maréchal und E. R. Biddle, „It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge“, New America, 2020. [Online]. Verfügbar unter: https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/
[66] M. A. Beam, M. J. Hutchens, und J. D. Hmielowski, „Facebook news and (de)polarization: reinforcing spirals in the 2016 US election“, *Information, Communication & Society*, Bd. 21, Nr. 7, S. 940–958, Juli 2018, doi: 10.1080/1369118X.2018.1444783.
[67] G. Alvarez, „Good News, Bad News: A Sentiment Analysis of the 2016 Election Russian Facebook Ads“, *International Journal of Communication*, Bd. 14, S. 3027–3053, 2020.
[68] I. Dachwitz, „FAQ: Was wir über den Skandal um Facebook und Cambridge Analytica wissen [UPDATE]“, *netzpolitik.org*, März 21, 2018. https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/ (zugegriffen Nov. 25, 2021).
[69] The Guardian, „The Cambridge Analytica Files“. Zugegriffen: Nov. 25, 2021. [Online]. Verfügbar unter: https://www.theguardian.com/news/series/cambridge-analytica-files
[70] A. Stevenson, „Facebook Admits It Was Used to Incite Violence in Myanmar“, *The New York Times*, Nov. 06, 2018. Zugegriffen: Nov. 25, 2021. [Online]. Verfügbar unter: https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html

[71] J. Posetti und K. Bontcheva, „Disinfodemic: Deciphering COVID-19 disinformation“, UNESCO, 2020. Zugegriffen: Nov. 10, 2021. [Online]. Verfügbar unter: https://en.unesco.org/sites/default/files/disinfodemic_deciphering_covid19_disinformation.pdf
[72] S. Ghaffary, „The algorithms that detect hate speech online are biased against black people“, *Vox*, Aug. 15, 2019. https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter (zugegriffen Nov. 25, 2021).
[73] „Apple toughens iCloud security after celebrity breach“, *BBC News*, Sep. 17, 2014. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.bbc.com/news/technology-29237469
[74] Der Standard, „Datenschutz: EU-Abgeordnete erhöhen Druck auf EU-Kommission“, *Der Standard*, Mai 20, 2021. https://www.derstandard.de/story/2000126800248/datenschutz-eu-abgeordnete-erhoehen-druck-auf-eu-kommission (zugegriffen Dez. 12, 2021).
[75] E. Massé, „Three Years under the EU GDPR“, Access Now, Mai 2021. Zugegriffen: Dez. 12, 2021. [Online]. Verfügbar unter: https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf
[76] T. Haar, „Wolkenbruch: US CLOUD Act regelt internationalen Datenzugriff“, *ix*, Bd. 2018, Nr. 7, Heise, S. 106–107, Juni 27, 2018.
[77] EDRi, „Demonstrating gaps in the e-Evidence Regulation“, EDRi - European Digital Rights, 2021. Zugegriffen: Dez. 12, 2021. [Online]. Verfügbar unter: https://edri.org/wp-content/uploads/2021/10/EDRI_eEvidence.pdf
[78] J. Menn, „Exclusive: Apple dropped plan for encrypting backups after FBI complained“, *Reuters*, Jan. 21, 2020. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.reuters.com/article/us-apple-fbi-icloud-exclusive-idUSKBN1ZK1CT
[79] DIGITALEUROPE, „Encryption: finding the balance between privacy, security and lawful data access“, *DIGITALEUROPE*, März 16, 2020. https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/ (zugegriffen Dez. 12, 2021).
[80] M. Manakas, „Apple scannt iPhones künftig auf Darstellungen von Kindesmissbrauch“, *DER STANDARD*, Aug. 06, 2021. https://www.derstandard.at/story/2000128738941/apple-scannt-iphones-kuenftig-auf-darstellungen-von-kindesmissbrauch (zugegriffen Nov. 26, 2021).
[81] L. Kolodny, „Tesla drivers can now request Full Self-Driving Beta with the press of a button, despite safety concerns“, *CNBC*, Sep. 25, 2021. https://www.cnbc.com/2021/09/25/tesla-drivers-can-request-fsd-beta-with-a-button-press-despite-safety-concerns.html (zugegriffen Nov. 26, 2021).
[82] T. Brewster, „Watch A Tesla Have Its Doors Hacked Open By A Drone“, *Forbes*, Apr. 29, 2021. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.forbes.com/sites/thomasbrewster/2021/04/29/watch-a-tesla-have-its-doors-hacked-open-by-a-drone/
[83] O. Solon, „Team of hackers take remote control of Tesla Model S from 12 miles away“, *The Guardian*, Sep. 20, 2016. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes
[84] Futurezone, „BMW-Fahrzeuge können per Mobilfunk gehackt werden“, Mai 23, 2018. https://futurezone.at/digital-life/bmw-fahrzeuge-koennen-per-mobilfunk-gehackt-werden/[node:path] (zugegriffen Nov. 26, 2021).
[85] I. Lommer, „Sicherheitsexperte hackt eigenes Auto: ‚Es war eine wirklich verstörende Erfahrung‘“, *FOCUS Online*. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.focus.de/digital/dldaily/sicherheit-auf-der-strasse-sicherheitsexperte-hackt-eigenes-auto-es-war-eine-wirklich-verstoerende-erfahrung_id_10434312.html
[86] D. Brown, „Where are the cameras in your car and what are they looking for?“, *USA TODAY*. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.usatoday.com/story/tech/2019/04/23/cameras-inside-outside-new-cars/3506205002/
[87] E. Poole Sidell, „What Does Google Do With Your Data?“, *Avast*. https://www.avast.com/c-how-google-uses-your-data (zugegriffen Nov. 26, 2021).
[88] J. R. Reidenberg *u. a.*, „Disagreeable Privacy Policies: Mismatches Between Meaning and Users’ Understanding“, *Berkeley Technology Law Journal*, Bd. 30, Nr. 1, S. 39–68, 2015.
[89] Apple, „AirTag“, *Apple (Österreich)*. https://www.apple.com/at/airtag/ (zugegriffen Nov. 26, 2021).
[90] M. Dölle, „Apple AirTags: Schutz vor Stalking und Überwachung völlig unzureichend“, *c’t Magazin*, Juni 18, 2021. Zugegriffen: Nov. 26, 2021. [Online]. Verfügbar unter: https://www.heise.de/news/Apple-AirTags-Schutz-vor-Stalking-und-Ueberwachung-voellig-unzureichend-6069686.html
[91] Kurier, „Online-Shoppen immer beliebter, aber stationärer Handel führt klar“, *Kurier*, Mai 05, 2021. Zugegriffen: Dez. 02, 2021. [Online]. Verfügbar unter: https://kurier.at/wirtschaft/online-shoppen-immer-beliebter-aber-stationaerer-handel-fuehrt-klar/401372651
[92] Der Standard, „Amazon vorne: Zehn Onlineshops dominieren Hälfte des Marktes“, *Der Standard*, Nov. 17, 2020. Zugegriffen: Dez. 02, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000121762990/amazon-vorne-zehn-onlineshops-dominieren-haelfte-des-marktes

[93] Handelsverband, „eCommerce Studie Österreich 2021“, *Handelsverband*. https://www.handelsverband.at/publikationen/studien/ecommerce-studie-oesterreich/ecommerce-studie-oesterreich-2021/ (zugegriffen Dez. 02, 2021).
[94] Der Standard, „Lieferdienste machen Supermärkten zunehmend Konkurrenz“, *Der Standard*, Juni 04, 2021. Zugegriffen: Dez. 02, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000127156417/lieferdienste-machen-supermaerkten-zunehmend-konkurrenz
[95] OECD, „Understanding online consumer ratings and reviews“, OECD Digital Economy Papers 289, Sep. 2019. doi: 10.1787/eb018587-en.
[96] P. U. Blaha, „Fake-Bewertungen auf Amazon und Co.“, *help.ORF.at*, Nov. 14, 2020. https://help.orf.at/stories/3202884/ (zugegriffen Dez. 02, 2021).
[97] M. Fiedler, „London: Wie Fake-Restaurant Nummer eins wurde“, *Der Spiegel*, Apr. 14, 2018. Zugegriffen: Dez. 02, 2021. [Online]. Verfügbar unter: https://www.spiegel.de/spiegel/unispiegel/london-wie-fake-restaurant-nummer-eins-wurde-a-1204771.html
[98] N. Huete-Alcocer, „A Literature Review of Word of Mouth and Electronic Word of Mouth: Implications for Consumer Behavior“, *Frontiers in Psychology*, Bd. 8, S. 1256, 2017, doi: 10.3389/fpsyg.2017.01256.
[99] C. Conner, „9 Online Reputation Management Services Entrepreneurs Can Achieve By Themselves“, *Forbes*, Juni 19, 2016. https://www.forbes.com/sites/cherylsnappconner/2016/07/19/9-online-reputation-management-services-entrepreneurs-can-achieve-by-themselves/ (zugegriffen Dez. 07, 2021).
[100] G. Gürkaynak und Ç. O. Kama, „Navigating the Uncharted Risks of Covert Advertising in Influencer Marketing“, *Business Law Review*, Bd. 39, Nr. 1, Feb. 2018, Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://kluwerlawonline.com/journalarticle/Business+Law+Review/39.1/BULA2018004
[101] L. Matsakis, „The WIRED Guide to Your Personal Data (and Who Is Using It)“, *Wired*, Feb. 15, 2019. Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://www.wired.com/story/wired-guide-personal-data-collection/
[102] M. Al-Youssef, „Jö-Bonusclub soll wegen Datenschutzverstößen Millionenstrafe zahlen“, *DER STANDARD*, Aug. 02, 2021. https://www.derstandard.at/story/2000128639162/joe-bonusclub-soll-millionenstrafe-zahlen (zugegriffen Dez. 07, 2021).
[103] R. M. Weiss und A. K. Mehrotra, „Online Dynamic Pricing: Efficiency, Equity and the Future of E-Commerce“, *Va. J.L. & Tech.*, Bd. 6, S. 1, 2001.
[104] Der Standard, „Wenn das Flugticket über Nacht 300 Euro mehr kostet“, *Der Standard*, Apr. 26, 2019. Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000102018291/wenn-das-flugticket-von-einem-tag-auf-den-anderen-300
[105] N. Lomas, „International coalition joins the call to ban ‘surveillance advertising’“, *TechCrunch*, Juni 23, 2021. Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://social.techcrunch.com/2021/06/23/international-coalition-joins-the-call-to-ban-surveillance-advertising/
[106] N. Schmidt und B. Stephens, „An Introduction to Artificial Intelligence and Solutions to the Problems of Algorithmic Discrimination“, *arXiv:1911.05755 [cs]*, Nov. 2019, Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: http://arxiv.org/abs/1911.05755
[107] Competition and Markets Authority, „Algorithms: how they can reduce competition and harm consumers“, UK Competition and Markets Authority, Jan. 2021. [Online]. Verfügbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/954331/Algorithms_++.pdf
[108] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, und A. L. Toombs, „The Dark (Patterns) Side of UX Design“, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: Association for Computing Machinery, 2018, S. 1–14. Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://doi.org/10.1145/3173574.3174108
[109] H. Brignull, „Dark Patterns“. https://www.darkpatterns.org/ (zugegriffen Dez. 07, 2021).
[110] L. Matsakis, „The Subtle Tricks Shopping Sites Use to Make You Spend More“, *Wired*, Aug. 06, 2020. Zugegriffen: Dez. 07, 2021. [Online]. Verfügbar unter: https://www.wired.com/story/amazon-online-retail-dark-patterns/
[111] New York Times, „Cancel your subscription“, *New York Times*. https://help.nytimes.com/hc/en-us/articles/360003499613-Cancel-your-subscription (zugegriffen Dez. 07, 2021).
[112] Statistik Austria, „Private Internetnutzung erreicht neuen Höchststand“, *Statistik Austria*, Nov. 03, 2021. http://www.statistik.at/web_de/presse/126937.html (zugegriffen Dez. 10, 2021).
[113] A-SIT Zentrum für sichere Informationstechnologie – Austria, „Phishing“, Okt. 08, 2020. https://www.onlinesicherheit.gv.at/Themen/Gefahren-im-Netz/Online-Banking/Phishing.html (zugegriffen Dez. 10, 2021).

[114] Die Presse, „‚Skimming': Wieder mehr manipulierte Bankomaten in Wien", *Die Presse*, Juni 23, 2016. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.diepresse.com/5033179/skimming-wieder-mehr-manipulierte-bankomaten-in-wien
[115] Futurezone, „Wie Bankomaten in wenigen Minuten gehackt werden können", Nov. 17, 2018. https://futurezone.at/digital-life/wie-bankomaten-in-wenigen-minuten-gehackt-werden-koennen/[node:path] (zugegriffen Dez. 10, 2021).
[116] Zeit Online, „Cyberkriminalität: Verdachtsfälle von Geldwäsche mit Kryptowährungen nehmen stark zu", *Die Zeit*, Hamburg, Sep. 02, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.zeit.de/wirtschaft/2021-09/geldwaesche-kryptowaehrungen-zunahme-cyberkriminalitaet-europa?utm_referrer=https%3A%2F%2Fwww.google.com%2F
[117] R. Falterer und J. Oesch, „Eine einzige Überweisung in Bitcoins verbraucht so viel Energie wie ein Schweizer in eineinhalb Monaten", *Neue Zürcher Zeitung*, Apr. 05, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.nzz.ch/technologie/bitcoin-und-co-verbrauchen-schon-jetzt-mehr-energie-als-alle-schweizer-zusammen-so-koennten-sie-gruener-werden-ld.1609815#subtitle-so-viel-strom-fressen-kryptow-hrungen-second
[118] Statista, „Österreich - Inlandstromverbrauch 2020", *Statista*, Nov. 09, 2021. https://de.statista.com/statistik/daten/studie/325788/umfrage/stromverbrauch-in-oesterreich/ (zugegriffen Dez. 10, 2021).
[119] Die Presse, „Pandemie machte Österreichs Unternehmen digitaler", *Die Presse*, Okt. 19, 2021. https://www.diepresse.com/6049329/pandemie-machte-osterreichs-unternehmen-digitaler (zugegriffen Dez. 10, 2021).
[120] R. Karner und O. Suchocki, „Homeoffice nach Corona » New Work", *EY.com*, Jan. 21, 2021. https://www.ey.com/de_at/workforce/wie-viel-homeoffice-bleibt-nach-der-corona-pandemie (zugegriffen Dez. 10, 2021).
[121] Microsoft, „Videokonferenzen, Besprechungen, Anrufe | Microsoft Teams", *Microsoft*. https://www.microsoft.com/de-at/microsoft-teams/group-chat-software (zugegriffen Dez. 10, 2021).
[122] L. Irwin, „The cyber security risks of working from home", *IT Governance Blog*, Aug. 19, 2021. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home (zugegriffen Dez. 11, 2021).
[123] Microsoft, „What info can your company see when you enroll your device?", *Microsoft*, Sep. 28, 2021. https://docs.microsoft.com/en-us/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune (zugegriffen Dez. 10, 2021).
[124] Theo Anders, „Online-Prüfungen an Unis: Videoüberwachung im Wohnzimmer und Verbot von Müsliverpackungen", *DER STANDARD*, Jan. 27, 2021. Zugegriffen: Dez. 11, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000123610987/online-pruefungen-an-unis-videoueberwachung-im-wohnzimmer-und-verbot-von
[125] P. Müller, „Lidar-Sensor im iPhone: Was das ist und wofür", *Macwelt*, Sep. 08, 2021. https://www.macwelt.de/news/Lidar-Sensor-im-iPhone-12-Pro-Was-das-ist-und-wofuer-10899937.html (zugegriffen Dez. 10, 2021).
[126] C. Hall, „Was ist Ultrabreitband und was macht UWB?", *Pocketlint*, Juni 08, 2021. https://www.pocket-lint.com/de-de/gadgets/news/156470-was-ist-ultrabreitband-und-was-macht-uwb (zugegriffen Dez. 10, 2021).
[127] C. Allner, „Smart Home: Chance und Risiko", *Der Standard*, Apr. 24, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000116917030/smart-home-chance-und-risiko
[128] J. Schmidt, „Vom Leben und Sterben der 0days: Gefährliche Sicherheitslücken über viele Jahre ausnutzbar", *c't*, Bd. 2017, Nr. 8, Heise, S. 16–17, März 31, 2017.
[129] Zero Day Initiative, „Published Advisories", *Zero Day Initiative*. https://zerodayinitiative.com (zugegriffen Dez. 10, 2021).
[130] Apple, „Watch - Warum Apple Watch", *Apple (Österreich)*. https://www.apple.com/at/watch/why-apple-watch/ (zugegriffen Dez. 10, 2021).
[131] „Galaxy Watch4", *Samsung.at*. https://www.samsung.com/at/watches/galaxy-watch/galaxy-watch4-classic-silver-lte-sm-r895fzsaeub/ (zugegriffen Dez. 10, 2021).
[132] R. Winkler, „Apple Plans Blood-Pressure Measure, Wrist Thermometer in Apple Watch", *Wall Street Journal*, Sep. 21, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.wsj.com/articles/apple-plans-blood-pressure-measure-wrist-thermometer-in-watch-11630501201
[133] K. Sanchez, „Apple reportedly wants a Watch with more health tracking and could ship one next year", *The Verge*, Sep. 01, 2021. https://www.theverge.com/2021/9/1/22652120/apple-watch-blood-pressure-temperature-sleep-diabetes (zugegriffen Dez. 10, 2021).
[134] Der Spiegel, „Chinesische Firma sammelt Gendaten von Schwangeren", *Der Spiegel*, Juli 09, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.spiegel.de/netzwelt/apps/bgi-group-chinesische-firma-sammelt-gendaten-von-schwangeren-a-ee9dc2e7-afa2-4e8c-9ad2-c26d7ec432a3

[135] „Chinesische Genfirma BGI dementiert Zusammenarbeit mit Militär“, *Die Presse*, Juli 10, 2021. https://www.diepresse.com/6005895/chinesische-genfirma-bgi-dementiert-zusammenarbeit-mit-militar (zugegriffen Dez. 10, 2021).
[136] K.-I. Voigt, „Industrielle Revolution“, *Gabler Wirtschaftslexikon*. https://wirtschaftslexikon.gabler.de/definition/industrielle-revolution-38116 (zugegriffen Dez. 10, 2021).
[137] N. Laufer, „Digitale Landwirtschaft: Drohnen und intelligente Traktoren am Acker“, *DER STANDARD*, Mai 02, 2018. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000078820789/digitale-landwirtschaft-drohnen-und-intelligente-traktoren-am-acker
[138] M. D. Shear, N. Perlroth, und C. Krauss, „Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers“, *The New York Times*, Mai 14, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html
[139] J. Bunge, „WSJ News Exclusive | JBS Paid $11 Million to Resolve Ransomware Attack“, *Wall Street Journal*, Juni 10, 2021. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781
[140] M. A. Mullane, „Cybersecurity für kritische Infrastrukturen“, *DKE.de*, Aug. 03, 2020. https://www.dke.de/de/arbeitsfelder/cybersecurity/news/cybersecurity-fuer-kritische-infrastrukturen (zugegriffen Dez. 10, 2021).
[141] W. Preissl, S. Strauß, und J. Krieger-Lamina, „Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven“, Institut für Technikfolgen-Abschätzung (ITA), 2017. [Online]. Verfügbar unter: http://epub.oeaw.ac.at/ita/ita-projektberichte/2017-01.pdf
[142] M. Z. Gunduz und R. Das, „Cyber-security on smart grid: Threats and potential solutions“, *Computer Networks*, Bd. 169, S. 107094, März 2020, doi: 10.1016/j.comnet.2019.107094.
[143] D. Lee und D. J. Hess, „Data privacy and residential smart meters: Comparative analysis and harmonization potential“, *Utilities Policy*, Bd. 70, S. 101188, Juni 2021, doi: 10.1016/j.jup.2021.101188.
[144] Bundesministerium für Finanzen, „Pflicht zur Abgabe der Einkommensteuererklärung und Einkommensteuerveranlagung“. https://bmf.gv.at/themen/steuern/fuer-unternehmen/einkommensteuer/einkommensteuererklaerungspflicht.html (zugegriffen Dez. 10, 2021).
[145] oesterreich.gv.at, „E-Government: Aktuelle Informationen zu E-Government, elektronische Zustellung, Amtswege etc.“, *oesterreich.gv.at - Österreichs digitales Amt*. https://www.oesterreich.gv.at/themen/dokumente_und_recht/e_government.html (zugegriffen Dez. 10, 2021).
[146] A. Kannenberg, „Hackerangriff in Bulgarien betrifft Millionen Menschen“, *heise online*, Juli 16, 2019. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.heise.de/newsticker/meldung/Hackerangriff-in-Bulgarien-betrifft-Millionen-Menschen-4472405.html
[147] M. Al-Youssef, „Predictive Policing: Wie die Polizei Verbrechen voraussagt“, *Der Standard*, Nov. 23, 2018. Zugegriffen: Dez. 10, 2021. [Online]. Verfügbar unter: https://www.derstandard.at/story/2000091840678/predictive-policing-wie-die-polizei-verbrechen-voraussagt
[148] C. O’Neil, *Weapons of math destruction: how big data increases inequality and threatens democracy*, First edition. New York: Crown, 2016.
[149] BMI, „Österreichische Strategie für Cyber Sicherheit (ÖSCS)“, *Bundesministerium Inneres*, n.V. https://www.bmi.gv.at/504/start.aspx (zugegriffen Sep. 22, 2021).
[150] Bundeskanzleramt, „Nationale Cybersicherheitsstrukturen“, *Nationale Cybersicherheitsstrukturen*. https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/nationale-strukturen.html (zugegriffen Dez. 14, 2021).
[151] Bundeskanzleramt, „Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP)“, *Bundeskanzleramt*, n.V. https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html (zugegriffen Sep. 08, 2021).
[152] Europäischcer Rat, „Cybersicherheit: Wie die EU Cyberbedrohungen begegnet“, n.V. https://www.consilium.europa.eu/de/policies/cybersecurity/ (zugegriffen Sep. 22, 2021).
[153] European Commission, „Cybersecurity Strategy | Shaping Europe’s digital future“, n.V. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (zugegriffen Sep. 22, 2021).
[154] ENISA, „NIS Directive“, *ENISA*, n.V. https://www.enisa.europa.eu/topics/nis-directive (zugegriffen Sep. 08, 2021).
[155] WKO, „Cybersicherheit – Das neue NISG“, März 06, 2019. https://www.wko.at/site/it-safe/cybersicherheit-das-neue-nisg.html (zugegriffen Dez. 10, 2021).
[156] WKO, „EU-Datenschutz-Grundverordnung (DSGVO)“, *WKO*, März 17, 2021. https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html (zugegriffen Sep. 29, 2021).
[157] „GraphSense“, *GraphSense*. https://graphsense.info/ (zugegriffen Dez. 13, 2021).

8. Anhang I: Liste der InterviewpartnerInnen

Name	Organisation
Alexander Janda	Kuratorium Sicheres Österreich
Robert Lamprecht	KPMG
Herbert Leitold	A-SIT
Helmut Leopold	Austrian Institute of Technology
Clemens Möslinger	Bundeskanzleramt
Joe Pichlmayr	Cyber Security Austria
Wolfgang Rosenkranz	CERT.at
Thomas Stubbings	Cyber Security Platform

9. Anhang II: Workshop-Agenda und TeilnehmerInnen

Ein interaktiver Workshop zur Reflexion, Validierung und Diskussion von Handlungsoptionen wurde am 18.11.2021, 10:00-13:00 abgehalten. Der Workshop bestand aus drei Sessions und wurde unter Anwendung partizipativer Methoden als online-Workshop mit mehr als 20 ExpertInnen aus Wirtschaft, Wissenschaft, öffentlicher Verwaltung und Interessensvertretungen umgesetzt. Im Folgenden wird die Agenda sowie die Liste der TeilnehmerInnen dargestellt.

Ziele des Workshops:

- Chancen und Herausforderungen für Österreich im Bereich Cybersecurity reflektieren und priorisieren,
- zukünftige Entwicklungsfelder im Bereich Cybersecurity und Österreichs Positionierung antizipieren und
- Handlungsbedarfe und (FTI-) Maßnahmen zur Unterstützung von österreichischer Forschung und Entwicklung im Bereich Cybersecurity identifizieren.

Agenda

Willkommen

- Begrüßung
- Überblick über die Studie und Ziele des Workshops

Vorstellungsrunde

Bitte stellen Sie sich vor mit Name und Organisation und formulieren jeweils zwei kurze plakative Sätze zu Cybersecurity:

- Was leistet Cybersecurity?
- Woran krankt es aus Ihrer Sicht?

Interaktion I (in Kleingruppen): Begriff Cybersecurity

- Welche Aspekte sind integraler Bestandteil der Cybersecurity und in welcher Beziehung stehen sie zueinander?
- Fehlen Ihnen Aspekte?
- Welche Aspekte sind am wichtigsten?

Interaktion II (in Kleingruppen): SWOT-Analyse Cybersecurity in Österreich

- Welche Stärken/Schwächen/Chancen/Bedrohungen bietet Cybersecurity in Österreich (Wirtschaft, Forschung, öffentliche Verwaltung)?
- Wo hat Österreich eine Themenführerschaft (Stärken)?
- Wo hat Österreich Defizite (Schwächen)?
- Wo sind mögliche Schwerpunkte Österreichs sinnvoll (Chancen)?
- Wo bestehen für Österreich zukünftig Probleme (Risiken)?

Interaktion III (in Kleingruppen): Handlungsbedarf und Maßnahmen

- Welchen Handlungsbedarf sehen Sie für die Politik aus Ihrer persönlichen ExpertInnensicht?
- Decken sich die Handlungsmaßnahmen mit den Stärken/Schwächen/Chancen/Risiken der SWOT?

- Haben Sie Ideen für weitere Maßnahmen?
- Welche Akteure könnten diese Maßnahmen umsetzen?
- Welche Maßnahmen halten Sie für sinnvoll/effektiv in der aktuellen Situation Österreichs (Priorisierung)?

Tabelle 7 Liste der Workshop-TeilnehmerInnen

Name	**Organisation**
Verena Becker	WKÖ
Nikolina Grgic	Plattform Industrie 4.0
Vinzenz Heußler	Bundeskanzleramt
Jeanette Klonk	FFG
Leonhard Kunz	Bundesministerium für Inneres
Helmut Leopold	Austrian Institute of Technology
Thomas Masicek	T-Systems
Nenad Milanovic	Erste Group
Walter Peissl	Österreichische Akademie der Wissenschaften – Institut für Technikfolgenabschätzung
Georg Petzl	Magenta
Bernd Pichlmayer	Bundeskanzleramt
Joe Pichlmayr	Cyber Security Austria
Wolfgang Rosenkranz	CERT.at
Ingrid Schaumüller-Bichl	IT-Sicherheitsberatung
Anton Sepper	Wiener Linien
Thomas Stubbings	Cyber Security Platform
Johanna Ullrich	SBA Research
Elisabeth Veit	FFG
Edgar Weippl	Universität Wien
Christian Zec	Bundeskanzleramt

www.oeaw.ac.at/ita

www.ait.ac.at