Jahrbuch zu den Alpbacher Technologiegesprächen 2019
Alpbach Technology Symposium Yearbook 2019

Hannes Androsch, Wolfgang Knoll,
Anton Plimon (Hg. Eds.)

Technologie im Gespräch

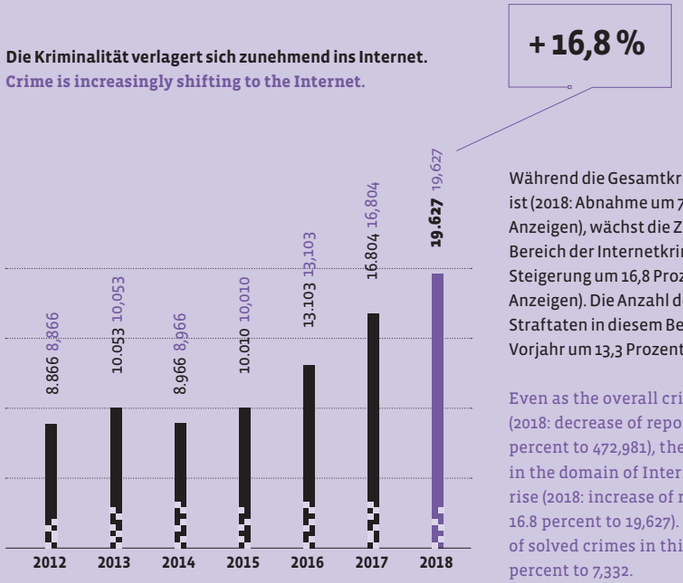
Discussing Technology

Sicherheit im Cyberraum
Cybersecurity

HOLZHAUSEN
Der Verlag

Cyberkriminalität
Cybercrime

1 **Die Kriminalität verlagert sich zunehmend ins Internet.**
Crime is increasingly shifting to the Internet.



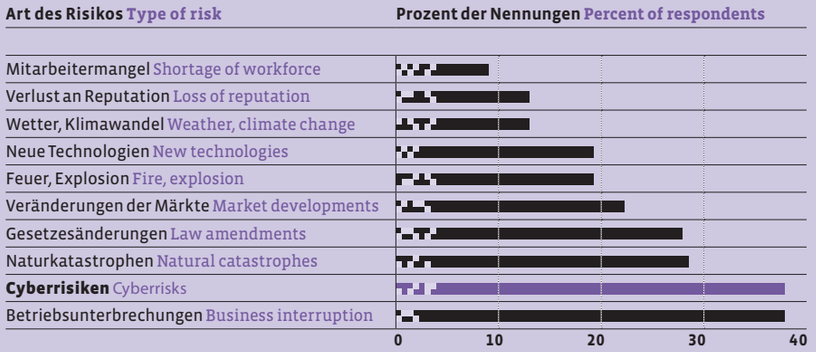
Während die Gesamtkriminalität rückläufig ist (2018: Abnahme um 7,4 Prozent auf 472.981 Anzeigen), wächst die Zahl der Straftaten im Bereich der Internetkriminalität (2018: Steigerung um 16,8 Prozent auf 19.627 Anzeigen). Die Anzahl der geklärten Straftaten in diesem Bereich nahm im Vorjahr um 13,3 Prozent auf 7.332 zu.

Even as the overall crime rate is declining (2018: decrease of reported crimes by 7.4 percent to 472,981), the number of offenses in the domain of Internet crime is on the rise (2018: increase of reported crimes by 16.8 percent to 19,627). Last year the number of solved crimes in this field rose by 13.3 percent to 7,332.

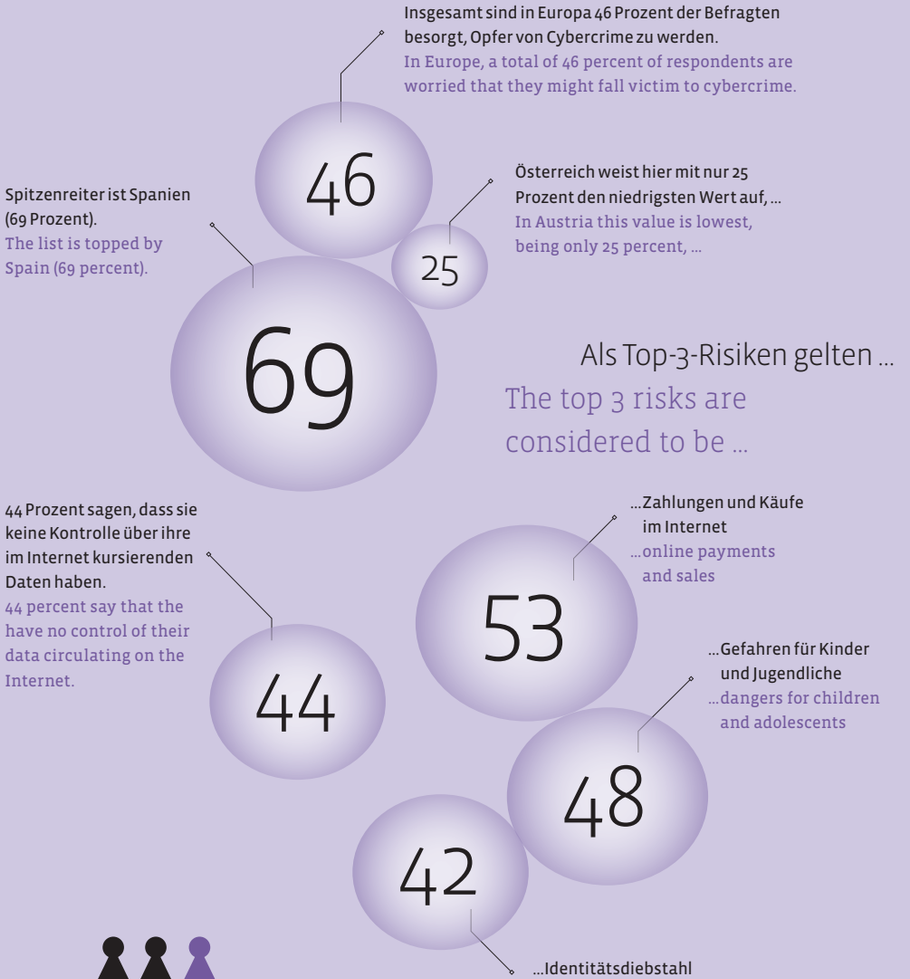
2 **Die zehn größten globalen Geschäftsrisiken 2019**
Top 10 Global Business Risks for 2019

Erstmals landeten Cybervorfälle heuer im Allianz Risk Barometer bei den größten globalen Geschäftsrisiken auf Platz eins – ex aequo mit Betriebsunterbrechungen. 2015 lagen Cyberrisiken noch auf Rang fünf (17 Prozent). Für die Studie wurden 2.415 Experten aus 86 Ländern befragt.

This year it is for the first time that cyberincidents have joined business interruption as leading global risk for companies in the Allianz Risk Barometer. In 2015 cyberrisks were still in fifth place (17 percent). 2,415 experts from 86 countries were interviewed for the study.



3 **Jeder vierte Österreicher sorgt sich wegen Cyberkriminalität.**
Every fourth Austrian is worried about cybercrime.



Jeder dritte Befragte gibt an, Passwörter und digitale Zugangsdaten selten oder nie zu ändern.
Every third respondent states that they rarely or never alter passwords or digital access data.

Quellen Sources

1 Bundesministerium für Inneres/ Polizeiliche Kriminalstatistik 2018
Federal Ministry of the Interior/ Police Crime Statistics 2018

2 Allianz Risk Barometer 2019
Allianz Risk Barometer 2019

3 Lexis im Auftrag von Europ Assistance, Umfrage in neun Ländern – Österreich, Italien, Frankreich, Rumänien, Spanien, Ungarn, USA, Tschechien und Schweiz – bei jeweils 800 Personen (repräsentativ). Lexis on behalf of Europ Assistance, sample survey carried out in nine countries—Austria, Italy, France, Romania, Spain, Hungary, the USA, Czechia and Switzerland,—with 800 persons interviewed per country

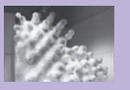
Technologie im Gespräch 2019
Discussing Technology 2019

HOLZHAUSEN
Der Verlag

Inhalt
Contents

ARTTEC zeigt Schnittstellen zwischen Kunst, Technologie und Wissenschaft:

ARTTEC highlights interfaces between art, technology, and science:



…als Teil dieses Jahrbuches und der Alpbacher Technologiegespräche, dieses Jahr in Kooperation mit dem MAK – Museum für angewandte Kunst im Rahmen der **VIENNA BIENNALE FOR CHANGE 2019: SCHÖNE NEUE WERTE.** Unsere digitale Welt gestalten.

…as part of this yearbook and the Alpbach Technology Symposium, this year in cooperation with MAK—Museum of Applied Arts in the context of the **VIENNA BIENNALE FOR CHANGE 2019: BRAVE NEW VIRTUES.** Shaping Our Digital World.

→ viennabiennale.org

Auf den technischen Grundlagen neuronaler Netze entwickelte das Designduo Process Studio speziell für die VIENNA BIENNALE FOR CHANGE 2019 mit *AImoji* und *AIfont* einzigartige Kommunikationswesen, denen man beim Lernen zusehen kann.

Based on the technical foundations of neural networks, the design duo Process Studio developed *AImoji* and *AIfont* especially for the VIENNA BIENNALE FOR CHANGE 2019 as a unique form of communication, which we can watch as it learns.

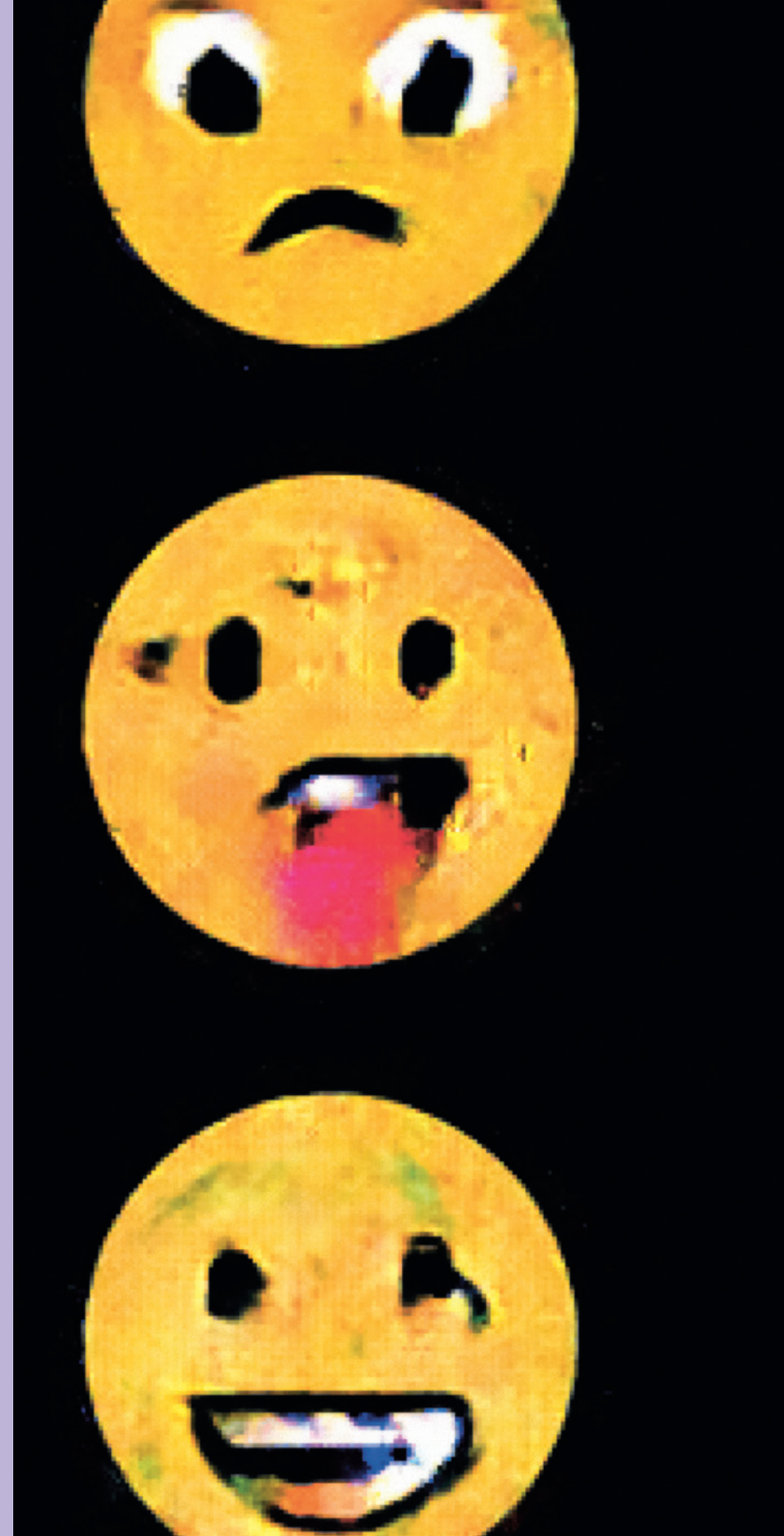
AImoji und *AIfont* sind die Key Visuals der Ausstellung *UNCANNY VALUES. Künstliche Intelligenz & du.*

AImoji and *AIfont* are the key visuals of the exhibition *UNCANNY VALUES. Artificial Intelligence & You.*

→ uncannyvalues.org

CREDITS:
UNCANNY VALUES. Artificial Intelligence & You

Process Studio (Martin Grödl and Moritz Resl), *AImoji,* 2019
Emoji generated by artificial intelligence



Hannes Androsch / Martin Kugler

Neue Spielregeln für die Cyberwelt

Digitalisierung und Vernetzung revolutionieren unsere Welt und bringen dabei auch neue Gefahren und Unsicherheiten mit sich. Wir benötigen dringend neue Rahmenbedingungen, um mit diesen Herausforderungen fertigzuwerden – vor allem Verbesserungen im Bildungssystem, mehr Forschung und Entwicklung sowie neue Regeln im Umgang mit digitalen Technologien.

Seit fast einem Dreivierteljahrhundert leben wir in Österreich in einer Periode des Friedens, der Sicherheit, der Freiheit und des wachsenden Wohlstands. Damit das so bleibt, müssen wir uns den wesentlichen Herausforderungen der Zukunft stellen: vor allem der Überalterung der Gesellschaft, dem Klimawandel und einer immer schneller voranschreitenden Digitalisierung – und das alles in einem Umfeld, in dem sich die Welt inmitten massiver Umbrüche befindet. Die politischen Gewichte auf der Erde werden derzeit neu verteilt: China und andere aufstrebende Staaten bekommen gegenüber den »alten« Weltmächten Europa, USA und Russland immer größere Bedeutung, sie stoßen auch in der Technologie, welche die künftigen Machtstrukturen maßgeblich mitbestimmt, zunehmend an die Weltspitze vor.

Wie seinerzeit der Übergang vom Agrar- ins Industriezeitalter bringt das digitale Zeitalter eine Veränderung aller Lebensbereiche mit sich, allerdings in noch größerem Ausmaß und atemberaubendem Tempo. Auf diese disruptiven Umwälzungen sind wir bislang nur schlecht vorbereitet. Unsere Wahrnehmung ist vielfach noch von rauchenden Schornsteinen geprägt – und noch nicht von »rauchenden Köpfen«, wie sie die Zukunft bestimmen werden.

Auch wenn die Themen der Digitalisierung – von der Roboterisierung über das Internet der Dinge und künstliche Intelligenz bis hin zur Industrie 4.0 – schon seit Längerem diskutiert werden, gilt das nicht in gleichem Ausmaß für die damit verbundenen Veränderungen, etwa in wirtschaftlicher Hinsicht. Schon ein kursorischer Blick auf die Entwicklungen der vergangenen Jahre zeigt jedoch, welch weitreichende Umwälzungen gerade im Unternehmensbereich stattfinden. Sieben der heute zehn wertvollsten Unternehmen der Welt sind Internetgiganten, die fünf

Hannes Androsch / Martin Kugler

New Rules for the Cyberworld Game

Digitization and networking are about to revolutionize our world, but they also have unprecedented dangers and insecurities in store for us. We urgently need a new framework that will enable us to cope with the challenges involved—primarily improvements of the educational system, intensified research and development, as well as new rules for handling the digital technologies.

In Austria we have been living in a period of peace, safety, freedom, and growing wealth for three quarters of a century. For this to remain the same we have to cope with the principal challenges of the future: these include, above all, the aging of society, climate change, and ever more rapidly progressing digitization—in a world that undergoes major ruptures. Currently, the political weights on earth are in a process of redistribution: China and other emerging states are gaining more and more significance compared to the "old" superpowers Europe, the USA, and Russia, and they are also increasingly forging ahead as world leaders when it comes to technology, a field that will substantially codetermine future power structures.

Similar to the transition from the agricultural to the industrial age, the digital age brings about change in all spheres of life, but on an even larger scale and at breathtaking speed. So far we are only inadequately prepared for such a disruptive revolution. In many respects, our perception is still informed by smoking funnels—and not yet by the "storming brains" that will be deciding about our future.

Although the themes of digitization—from robotization and the Internet of things to artificial intelligence and industry 4.0—have been discussed for a while now, this does not hold true to the same degree for the changes they imply, for example in the economic sphere. Even a cursory glance at the developments of recent years shows what far-reaching upheavals have been taking place in the business world. Today seven out of the ten most valuable business corporations in the world are Internet giants; the leading five are headquar-

führenden amerikanische Firmen, dicht gefolgt von chinesischen Technologieriesen. Alle diese neuen IT-Firmen gab es vor 20 Jahren noch nicht – oder sie waren damals bedeutungslos. Das Wirtschaftssystem wandelt sich von einer materiellen Wirtschaft mit riesigen Produktionsanlagen zu einem immateriellen System, das auf geistigem Eigentum, Patenten, Software, Unternehmensprozessen sowie hochqualifizierten Mitarbeitern beruht.

Auch im Bereich der Globalisierung gibt es neue Entwicklungen, die mit Schlagworten wie »Globotics« oder »Slowbalization« umschrieben worden sind. Den Begriff »Globotics Transformation« hat der US-Ökonom Richard Baldwin eingeführt. Seiner Meinung nach entstehen aus der Digitalisierung und der nächsten Welle künstlicher Intelligenz ganz neue Arbeitsformen, die enormen Druck auf die bestehenden Sozial- und Gesellschaftssysteme ausüben. Konkret: eine Telemigration und ein Talentetsunami, denen durch keine Mauer und keinen Stacheldraht oder brutale Abschiebungen begegnet werden kann. Seine Erklärung: Dank Digitalisierung und »machine to machine learning« (M2M) können immer mehr Menschen auf der Welt Dienstleistungen anbieten. Sogenannte »white collar robots« (Maschinen, die fortgeschrittene Dienstleistungen erbringen) werden eine neue Phase der Automation einleiten, welche die Arbeitswelt massiv verändern wird.

Unter »Slowbalization« – ein Wort, das der *Economist* in den Diskurs eingeführt hat – wird die jüngste Verlangsamung des globalen Wachstums bzw. des Welthandels verstanden. Diese ist von einem massiven Rückgang ausländischer Direktinvestitionen – vor allem grenzüberschreitender Investments multinationaler Konzerne – und verstärkten nationalen Ansprüchen im internationalen Handel gekennzeichnet. In dieser Entwicklung spiegle sich wider, dass die goldenen Zeiten der Globalisierung vorbei seien: Es habe eine Zeit der Flaute, der Trägheit und der Renationalisierung begonnen, in der Unternehmen vorsichtig werden und die Politik sich – soweit sie nicht selbst zur »Slowbalization« beiträgt – ratlos zeigt.

Diese Entwicklungen müssen die Welt nicht in den Abgrund führen – ganz im Gegenteil: Sie können die Menschheit weiter voranbringen. Ein positiver Effekt könnte etwa sein, dass die in den vergangenen Jahrzehnten in Billiglohnländer ausgelagerte Produktion nach Europa zurückkehrt. Dafür bedarf es aber entsprechender Rahmenbedingungen. Denn eines ist klar: Ob man will oder nicht, die Zukunft kommt sicher, der Fortschritt ist nicht aufzuhalten.

In der Transformationszeit, die wir gerade erleben, geht es uns freilich ein wenig wie dem Zauberlehrling in der Ballade Johann Wolfgang von Goethes: Wir haben neue Technologien in die Welt gesetzt und nutzen sie auch weidlich, aber wir beherrschen sie nicht. Wir wissen nicht, in welche Richtung die Entwicklung gehen wird und stehen vor vielen ungelösten Problemen – ethischen und juristischen genauso wie ökologischen, ökonomischen, sozialen und politischen.

Zudem drohen neue Gefahren aus der Cyberwelt. Darauf nehmen die Themen des Europäischen Forums Alpbach 2019 »Freiheit und Sicherheit« sowie dieses Jahrbuchs zu den Technologiegesprächen über Cybersecurity Bezug: Je vernetzter die

tered in the United States, closely followed by Chinese technology titans. All of these new IT companies did not exist twenty years ago—or they were insignificant then. The economic system has metamorphosed from a material economy relying on huge production plants into an immaterial system based on intellectual property, patents, corporate processes, and highly qualified employees.

New developments—dubbed "globotics" or "slowbalization"—can also be observed when it comes to globalization. The expression "globotics transformation" was coined by the US economist Richard Baldwin. In his opinion, entirely new forms of work are about to spring from the combination of digitization and the next wave of artificial intelligence, exercising enormous pressure on existing social systems and societies. To be more concrete: a type of telemigration and a tsunami of talent that cannot be countered by any wall, barbed wire fence, or brutal deportations. His explanation: thanks to digitization and machine-to-machine learning (M2M), more and more people across the world will be in a position to offer their services. So-called "white collar robots" (machines performing advanced services) will introduce a new phase of automation that will profoundly change the world of labor.

"Slowbalization"—a term thrown in by the *Economist*—describes the recent slowdown of global economic growth and international commerce. It is marked by a massive decline in foreign direct investment—primarily in multinational corporations' cross-border investment—and more and more national demands made in international trade. This development, it is said, reflects the fact that the Golden Age of globalization is over: a period of depression, stagnancy, and renationalization has begun in which companies have become prudent and politicians—as far as they do not contribute to "slowbalization" themselves—are at a loss.

This does not necessarily mean that these developments will plunge the world into the abyss—quite the contrary is true: they may alternatively bring humankind forward. A positive effect might be that production, which has now been offshored to low-wage countries for decades, will return to Europe. But for this, an appropriate framework will have to be created. For one thing is clear: if you like it or not, the future is certain to arrive, and progress cannot be stopped.

In this period of transition in which we live at the moment, though, it is a bit for us like for the sorcerer's apprentice in Johann Wolfgang von Goethe's ballad: we have brought new technologies into the world and make use of them gleefully without mastering them. We do not know in what direction all of this will develop and are confronted with numerous unsolved problems—not only ethical and legal ones, but also ecological, economic, social, and political ones.

Furthermore, new dangers from the cyberworld are looming. Being on the agenda of the European Forum Alpbach 2019 focusing on "Liberty and Security," these dangers are also discussed in the present yearbook, which

Welt, je komplexer und umfassender IT-Systeme, je mehr Arbeit sie uns abnehmen und Bequemlichkeit in unser Leben bringen, umso mehr sind wir von der Technologie abhängig – und umso schlimmer wird es, wenn diese Systeme ausfallen, mutwillig manipuliert oder gezielt angegriffen werden. Das macht uns extrem verwundbar. Viele dieser Gefahren im Cyberraum sind nicht neu, man kennt ihre Muster auch aus der analogen Welt. Doch die fortschreitende Vernetzung und Digitalisierung machen die Risiken deutlich größer und die Auswirkungen auf Individuen, Unternehmen, Gesellschaften und Staaten dramatischer.

Die Umbrüche und neuen Risiken erzeugen Unsicherheit, und diese löst bei vielen Menschen Skepsis, Sorgen und Ängste aus. Das betrifft u. a. Befürchtungen im Hinblick auf zukünftige Arbeitsplätze. Das war freilich bei allen Modernisierungsschüben so: Die Furcht vor technologiebedingter Massenarbeitslosigkeit ist so alt wie die Wirtschaft selbst. Historisch betrachtet entstanden aber bei wirtschaftlichen Umbrüchen viel mehr neue Stellen, als alte verschwanden. Klar ist: Die neue Maschinenintelligenz macht zwar Menschen Konkurrenz, aber sie macht sie deswegen nicht arbeitslos. Man braucht Spezialisten, die das digitale Zeitalter meistern. Es gibt kein Überangebot an Arbeitskräften, sondern einen Mangel – angesichts des demografischen Wandels erscheint die Angst, diese Entwicklung könnte den Menschen die Arbeit rauben, reichlich übertrieben.

Die Entwicklung hat freilich auch soziale Konsequenzen, welche die Unsicherheit verstärken: Wie bei jeder Transformation gibt es Modernisierungsgewinner und Modernisierungsverlierer – oder zumindest Menschen, die sich bedroht fühlen. Am Beispiel Silicon Valley lässt sich das gut beobachten: Denen, die beim rasanten Aufstieg der Digitalökonomie mit dabei sind, geht es sehr gut, jenen hingegen, die nicht daran beteiligt sind, schlecht – sie müssen, um ein plakatives Bild zu zeichnen, unter einer Brücke oder in einer Garage schlafen, weil sie sich die horrend gestiegenen Mieten in der Boomregion nicht leisten können. Das spaltet die Gesellschaft zunehmend – »America first«, die Wahl Trumps, die fatale Brexitentscheidung, die »Orbanisierung«, die Proteste der Gelbwesten oder die »Salvinisierung« Italiens sind Reaktionen darauf.

Das zunehmende Unsicherheitsgefühl und die damit verbundenen Abstiegs-, Verdrängungs- und Zukunftsängste sind eine Quelle, aus der billiges politisches Kapital geschlagen werden kann. In diesem Klima sind demagogischen und populistischen Akteuren Tür und Tor geöffnet: Diese Gruppen haben zwar keine Lösungen für (angebliche oder auch reale) Gefahren anzubieten, nutzen diesen Pool der Ängste jedoch, um politische Vorteile daraus zu ziehen. Das ist eine sehr gefährliche Entwicklung, die zu einer weiteren Spaltung der Gesellschaften von heute beiträgt. Das äußert sich mancherorts in zunehmender Autokratisierung oder gar gewaltsamen Auseinandersetzungen. Das soziale Gewebe wird immer brüchiger, ohne dass damit irgendetwas zukunftsorientiert gelöst würde.

Vor diesem Hintergrund sind neue Ideen in der Politik ebenso gefragt wie die Umsetzung dringend benötigter Reformen. Zu tun gibt es genug, auch in Österreich: Wir haben an vielen Ecken und Enden Reformbedarf. Unser Bildungswesen ist

accompanies the Technology Symposium on cybersecurity: the more the world is networked, the more complex and comprehensive IT systems will be, and the more work they take away from us and the more convenience they bring into our lives, the more we will depend on technology—and it will become all the worse when these systems break down or when they are deliberately manipulated or strategically attacked. This makes us vulnerable. Many of the dangers in cyberspace are familiar, their patterns known from the analog world. But advanced networking and digitization distinctly add to the risks and render the impact on individuals, corporations, societies, and governments more dramatic.

The ruptures and new risks generate insecurity and cause skepticism, worries, and fears in many people. This also includes concerns about the future job market. As a matter of fact, this was also the case during all the earlier pushes toward modernization: the fear of technology-based mass unemployment is as old as the economy as such. When looked at from a historical perspective, however, in times of economic upheavals always more new jobs were created than old ones disappeared. There can be no doubt: new machine intelligence may well be a rival for humans but it does not make them jobless. Specialists mastering the digital age are and will be in demand. There is no oversupply of labor, but a shortage—given demographic change, the fear that this development could deprive people of their work is more than exaggerated.

Developments admittedly also have social consequences aggravating a sense of insecurity: like in any period of transformation, modernization has its winners and losers—or at least people feeling threatened. This can excellently be observed in the example of Silicon Valley: those being part of the rapid growth of digital economy are extremely well off whereas those not involved are doing badly—drawing a drastic picture, they are forced to sleep under a bridge or in a garage because they cannot afford the booming region's soaring rents. This increasingly splits up society—"America first," Trump's election, the fatal Brexit decision, "Orbanization," the protests of the Yellow Vests, and the "Salvinization" of Italy are all responses to this situation.

This growing sense of insecurity and the resulting fears of social decline, of being made redundant, or of being unable to cope with the future are a source from which political capital can be made. Such a climate opens the floodgates to demagogues and populists: although these groups have no solutions for (alleged or real) dangers at hand, they exploit this pool of fears by taking political advantage from it. This is a very dangerous development that contributes to an ever-wider gap in today's societies. In several countries this manifests itself in growing autocratization or even violent conflict. The social fabric is becoming more and more fragile without any future-oriented solutions being found.

hoffnungslos veraltet, was die erforderlichen Qualifikationen sowie die nötige Flexibilität für das digitale Zeitalter angeht. Der Bildungsstandard der Bevölkerung wird darüber entscheiden, ob wir in einer digitalen Welt bestehen können und wie wir etwa den Herausforderungen von künstlicher Intelligenz und Cyberbedrohungen begegnen. Bildung bringt auch Aufklärung und Ermöglichung, sie kann dadurch die gefühlte Unsicherheit der Menschen bekämpfen. Um den Menschen Sorgen zu nehmen, muss man ihnen Perspektiven geben und Hoffnungen und Aussichten eröffnen. Die Menschen brauchen Optimismus und Selbstvertrauen, damit sie die Zukunft erfolgreich gestalten können. Zeitgemäße Bildung schafft Chancengleichheit, ermöglicht das Ausschöpfen des Talentepools und lässt niemanden zurück.

Man muss den Menschen auch viel mehr als bisher erklären, wie wichtig Wissenschaft und Forschung sind. Man muss vermitteln, dass Innovation dazu dient, ihnen das Leben zu erleichtern. So war es früher z. B. eine mühselige Arbeit, ein Schiff an Seilen einen Fluss hochzuziehen – heute sitzt man dagegen gemütlich in der Kabine eines Schiffs, das von einem Motor angetrieben wird. Europa und insbesondere Österreich sind auf die Herausforderungen der digitalen Zukunft ungenügend vorbereitet. Sie sind in vielen wesentlichen Bereichen Nachzügler. So sind ihnen im Bereich der künstlichen Intelligenz die USA ebenso weit voraus wie China, vielleicht auch Südkorea, sogar Russland, vor allem im militärischen Bereich. Diese Länder konzentrieren ihre Kräfte und investieren in Forschung zur künstlichen Intelligenz: die USA rund 1,7 Milliarden Dollar; auch Deutschland hat angekündigt, drei Milliarden Euro in KI-Forschung zu investieren. Zieht man den bewährten Schlüssel heran, so würde das in Österreich rund 300 Mio. Euro entsprechen – das ist mehr, als der Fonds zur Förderung der wissenschaftlichen Forschung jährlich insgesamt zur Verfügung hat.

Um die immer größer werdende Abhängigkeit von Technologie und damit auch die Verwundbarkeit in den Griff zu bekommen, sind entsprechende Rahmenbedingungen nötig. Wir brauchen für die Cyberwelt neue Ordnungsmaßnahmen, neue Spielregeln. Das war schon immer so: Jeder Technologiesprung erfordert neue Regeln. Als Menschen zum Beispiel noch mit Mauleseln unterwegs waren, war noch keine Straßenverkehrsordnung notwendig. Jetzt bedarf es gleichsam einer Straßenverkehrsordnung für die digitale Welt. Ansonsten werden – weiterhin – Chaos und Anarchie herrschen.

In diesem Jahrbuch zu den Technologiegesprächen Alpbach 2019 unternehmen wir den Versuch, einen aktuellen Schnappschuss der Entwicklungen im Bereich Cybersecurity vorzunehmen – ähnlich wie wir dies in den vergangenen beiden Jahren bei den Themen Digitalisierung und künstliche Intelligenz getan haben. Nach einem Überblick über aktuelle Trends bei Cyberattacken und Angriffswaffen widmen wir uns den Möglichkeiten, sich gegen diese zu wehren. Anhand ausgewählter Forschungsarbeiten am Austrian Institute of Technology (AIT) wird exemplarisch gezeigt, wie sich Wissenschaft sowie Forschung und Entwicklung neuen

Against this background, new political ideas are just as essential as is the implementation of urgently necessary reforms. There is much work to do here, also in Austria: improvement is needed in many areas. Our educational system is hopelessly out of date as far as indispensable qualifications and flexibility called for in the digital age are concerned. The population's educational standard will decide whether we will be capable of standing our ground in a digital world and how we will cope with such challenges as artificial intelligence and cyberthreats. Education also brings enlightenment and empowerment; it can fight the feeling of insecurity in people. In order to take the worries away from people one has to give them hope and open up new perspectives for them. People need optimism and self-confidence so as to be able to successfully shape the future. Modern education creates equal chances, enables us to draw from a pool of talents, and makes sure that no one is left behind.

It is also necessary to point out to people much more comprehensively than before how important science and research really are. It has to be conveyed to them that it is the purpose of innovation to make their lives easier. Formerly, it was tedious work to pull a ship upstream with ropes, for example—nowadays we conveniently sit in the cabin of a ship that is propelled by an engine. Europe in general and Austria in particular are insufficiently prepared for the challenges of a digital future. They lag behind in many crucial areas. When it comes to artificial intelligence, the United States and China are far ahead of them, as are probably also South Korea and even Russia, especially in the military sphere. These countries bundle their strengths and invest in research on artificial intelligence: the USA spends roughly 1.7 billion dollars; Germany has recently announced to invest three billion euros in AI research. Calculating according to the well-tried key, this would correspond to 300 million euros in Austria—which is more than the total yearly amount at the disposal of the Austrian Science Fund.

In order to get a handle on the ever-increasing dependence on technology and the vulnerability that comes along with it, appropriate conditions are called for. We need a new bundle of measures for the cyberworld, a new set of rules for the cybergame. For it has always been like this: each leap in technology requires new guidelines. When people were still en route on muleback, no road traffic regulations were required. Now we need traffic regulations for the digital world, so to speak. Otherwise chaos and anarchy will continue to prevail.

In this yearbook, which is devoted to the 2019 Alpbach Technology Symposium, we attempt to present an up-to-date snapshot of the developments in the sphere of cybersecurity—similar to what we did in the last two years on the subjects of digitization and artificial intelligence. Following an overview of current trends in the categories of cyberattacks and assault weapons, we take

Problemstellungen nähern, um nachhaltige Lösungen für die vielen Bedrohungen bereitzustellen. Die Auseinandersetzung mit dem übergeordneten Forum-Alpbach-Thema »Freiheit und Sicherheit« wird vor allem in ausführlichen Interviews etwa mit der Kriminalsoziologin Hemma Mayrhofer oder der Wirtschaftsethikerin Sarah Spiekermann erweitert. Einen wertvollen Beitrag liefern auch diesmal die Künste – und zwar in Form von Beiträgen unter dem Motto »Schöne neue Werte« der heurigen Vienna Biennale for Change 2019, die auch bei den Technologiegesprächen in Alpbach zu Gast ist. ×

Hannes Androsch, geboren 1938 in Wien, ist Aufsichtsratsvorsitzender des Austrian Institute of Technology (AIT), Vorsitzender des Rats für Forschung und Technologieentwicklung (RFTE) und war bis Juni 2016 Aufsichtsratsvorsitzender der Finanzmarktbeteiligungsgesellschaft des Bundes (FIMBAG). In seiner politischen Tätigkeit (SPÖ) war er u. a. Abgeordneter zum Nationalrat (1966 – 1970), Bundesminister für Finanzen (1970 – 1981) und Vizekanzler (1976 – 1981). Danach war er Generaldirektor der Creditanstalt-Bankverein (1981 – 1988) und Vorsitzender der Österreichischen Kontrollbank AG (1985 – 1986). 1989 gründete er die AIC Androsch International Management Consulting GmbH und begann 1994 den Aufbau einer industriellen Beteiligungsgruppe (Austria Technologie & Systemtechnik AG, Österreichische Salinen AG u. a.). 2004 errichtete er die »Stiftung Hannes Androsch bei der Österreichischen Akademie der Wissenschaften« und ist dort seit 2005 Mitglied des Senats. Ehrendoktorate und Ehrensenator verschiedener österreichischee und internationaler Universitäten (Montanuniversität Leoben, Universität New Orleans, USA, u. a.).

a closer look at what methods can be used to defend ourselves against them. Making reference to selected research projects conducted at the Austrian Institute of Technology (AIT), we give examples of how science and research tackle new problems in order to provide sustainable solutions for a variety of threats. The overall theme of the Forum Alpbach, which is “Liberty and Security,” will above all be elaborated on in extensive interviews with criminal sociologist Hemma Mayrhofer and business ethicist Sarah Spiekermann. This year, valuable input will once again come from the arts—namely in the form of contributions created under the motto “Brave New Virtues” of this year’s Vienna Biennale for Change, which has also been invited to participate at the Alpbach Technology Symposium. ×

Hannes Androsch, born in Vienna in 1938, is Chairman of the Supervisory Board of the Austrian Institute of Technology (AIT) and Chairman of the Austrian Council for Research and Technological Development (RFTE). Until June 2016, he was Chairman of the Supervisory Board of the Finanzmarktbeteiligung-gesellschaft des Bundes (FIMBAG). During his political career (SPÖ), his positions included Member of the National Assembly (1966 – 1970), Federal Minister of Finance (1970 – 1981), and Vice Chancellor (1976 – 1981). After this, he served as Director General of Creditanstalt-Bankverein (1981 – 1988) and as Chairman of Österreichische Kontrollbank AG (1985 – 1986). In 1989, he founded AIC Androsch International Management Consulting GmbH, and in 1994 initiated the establishment of an industrial investment group (Austria Technologie & Systemtechnik AG, Österreichische Salinen AG, etc.). In 2004, he founded the “Hannes Androsch Foundation at the Austrian Academy of Sciences,” where he has been a member of the senate since 2005. He has received honorary doctorates from and is an honorary senator of various Austrian and international universities, including the Montan-universität Leoben and the University of New Orleans, USA.

TEIL 1 / PART 1

Bedrohte Sicherheit

Security at Risk

Die Neuaufstellung des *MAK Design Lab* positioniert Design als Motor eines zukunftsfähigen Wandels und zeigt über Projekte von Designern, Künstlern, Architekten, Programmierern, Aktivisten und Idealisten, wie es gelingen kann, fair, nachhaltig und sinnvoll zusammenzuarbeiten.

The reinstallation of the *MAK Design Lab* presents design as the engine of tenable change and, drawing on projects by designers, artists, architects, programmers, activists, and idealists, shows how it can be possible to work together in a fair, sustainable, and meaningful way.

→ mak.at/makdesignlab

CREDITS:
MAK Design Lab
Reinstallation in the context of the
VIENNA BIENNALE FOR CHANGE 2019

mischer'traxler studio and LWZ, *Prospects*, 2019
© Stefan Lux, MAK

Bedrohte Welt

Durch Vernetzung und Digitalisierung verschieben sich Kriminalität, Spionage und politische Beeinflussung zunehmend in den digitalen Bereich. Ein kurz gefasster Überblick über zentrale Begriffe und Probleme der Cybersicherheit.

Sicherheit ist ein Grundbedürfnis des Menschen. Sie ist allerdings von vielen Seiten bedroht. Auf persönlicher Ebene beispielsweise durch Anfeindung und Hass, Diebstahl, Gewalt und andere Formen von Kriminalität. Aber auch auf gesellschaftlicher und wirtschaftlicher Ebene bestehen zahlreiche Gefährdungen der Sicherheit – beginnend bei Diebstahl und Erpressung von Unternehmen bis hin zu Spionage, Terrorismus, Destabilisierung der Gesellschaft und Krieg. Die riesigen Veränderungen, welche die Menschheit derzeit erlebt – Globalisierung, Digitalisierung und Vernetzung – haben auch immense Auswirkungen auf die Sicherheit: Die Risiken verschieben sich zunehmend in den digitalen Bereich, und das auf allen Ebenen.

Ablesbar ist das beispielsweise an der österreichischen Kriminalstatistik: Während die Gesamtkriminalität seit einigen Jahren stagniert oder sogar sinkt (2018: 472.981 Anzeigen, um 7,4 Prozent weniger als im Jahr zuvor), wuchs die Internetkriminalität auf 19.627 Fälle im Jahr 2018. Das ist eine Steigerung im Jahresvergleich um 16,8 Prozent – und seit 2012 sogar um 126 Prozent. Ähnliches kann man auf globaler Ebene feststellen: Im aktuellen »Cambridge Global Risk Index«, der alljährlich die Gefährdungen von 279 urbanen Regionen der Erde (mit zusammen rund 40 Prozent der globalen Wirtschaftsleistung) bewertet, dominieren zwar weiterhin altbekannte Risiken – nämlich Wirtschaftskrisen, zwischenstaatliche Konflikte, Naturkatastrophen (konkret: Wirbelstürme und Überflutungen) sowie Pandemien; doch auf Platz sechs der Gefährdungen liegen schon Cyberangriffe, die im aktuellen Index das Risiko durch Bürgerkriege überholt haben. Noch dramatischer ist die Entwicklung im Bereich der Wirtschaft. Das alljährlich aus mehr als 2000 Experteninterviews erstellte »Allianz Risk Barometer« weist für das Jahr 2019 erstmals Cybervorfälle auf Platz eins aus – ex aequo mit Betriebsunterbrechungen und relativ weit vor Geschäftsrisiken durch Naturkatastrophen, rechtlichen und regulatorischen Änderungen, Marktentwicklungen, Feuer und Explosion, Technologie- und Klimawandel.

Damit wird Cybersicherheit zu einem der wichtigsten Themen der Zukunft. Allgemein beschreibt der Begriff laut Definition des Kuratoriums Sicheres Österreich (KSÖ) den »Schutz eines zentralen Rechtsgutes mit rechtsstaatlichen Mitteln vor akteursbezogenen, technischen, organi-

A World Under Threat

Networking and digitization make crime, espionage, and political manipulation increasingly encroach on the digital area. This is a brief survey of some of the central notions and problems related to cybersecurity.

Safety and security are basic human needs. They are, however, under threat from many sides. At the personal level, for example, it may be because of hostility and hatred, theft, violence, and other types of crime. But there are numerous safety and security threats also at the social and economic level—from theft and corporate blackmailing to espionage, terrorism, destabilization of society, and war. The huge epochal transformation that humankind is currently going through—globalization, digitization, and networking—also has a tremendous impact on security: risks are shifting more and more to the digital area, and this is true at all levels.

This can be gleaned, for example, from the Austrian crime statistics: while the total crime rate has been staying the same or even slightly dropping for some years now (showing 472,981 reported crimes in 2018, 7.4 percent less than the year before), Internet crime rose to a total of 19,627 cases in 2018. This is an increase of 16.8 percent compared to the previous year—and no less than 126 percent since 2012. A similar trend can be observed at a global scale: in the current "Cambridge Global Risk Index," which annually assesses threats to 279 urban regions in the world (together accounting for some 40 percent of the global economic output), it still is well-known risks—namely, economic crises, national conflicts, natural disasters (specifically, hurricanes and floods) as well as pandemics—that are predominant; however, cyberattacks are already in sixth place and have overtaken the risk from civil wars. Even more dramatic is the development in the field of the economy: The "Allianz Risk Barometer," which is compiled annually from more than 2,000 expert interviews, for the first time shows cyberincidents in first place for 2019—on par with business interruptions and relatively far ahead of business risks arising from natural disasters, legal and regulatory changes, market developments, fire and explosion, technology and climate change.

This makes cybersecurity one of the crucial issues of the future. According to the definition of the Kuratorium Sicheres Österreich (KSÖ), the term generally refers to "the protection of a central legal good by

sations- und naturbedingten Gefahren, die die Sicherheit des Cyberspace (inklusive Infrastruktur- und Datensicherheit) und die Sicherheit der Nutzer im Cyberspace gefährden«. Cybersicherheit trage dazu bei, die Gefährdungen zu erkennen, zu bewerten und zu verfolgen; zudem solle die Fähigkeit gestärkt werden, Störungen im und aus dem Cyberspace zu bewältigen, die damit verbundenen Folgen zu mindern sowie die Handlungs- und Funktionsfähigkeit der davon betroffenen Akteure, Infrastrukturen und Dienste wieder herzustellen.

Drei zentrale Schutzziele

Als Cyberattacken werden Angriffe mit Mitteln der Informationstechnologie (IT) im Cyberraum bezeichnet, die sich gegen ein oder mehrere IT-Systeme richten und darauf abzielen, die Sicherheit von Informations- und Kommunikationstechnologien (IKT-Sicherheit) zu verletzen. Maßnahmen zur Gewährleistung von Cybersicherheit betreffen vor allem die folgenden drei Dimensionen:

- Das Schutzziel »Verfügbarkeit« beschreibt die Anforderung, dass Daten und Systeme zur Verfügung stehen und der Zugriff darauf möglich ist. Störungen, die zu einer Unterbrechung oder vollständigen Abschaltung der Systeme führen können, sollen verhindert werden.
- »Vertraulichkeit« meint, dass Daten nur berechtigten Nutzern zur Verfügung stehen. Daraus ergibt sich die Anforderung, dass Daten von unberechtigten Dritten nicht eingesehen werden dürfen. Ein digitaler Datendiebstahl verletzt dieses Schutzziel genauso wie die unverschlüsselte Übermittlung von Daten über unsichere Netzwerke.
- Das Ziel »Integrität« schließlich beinhaltet die Anforderung, dass Daten richtig und integer sein sollen. Daten dürfen von unberechtigten Dritten nicht verändert werden.

Cyberattacken werden häufig durch Schadprogramme geritten – also durch den Einsatz speziell dafür programmierter oder angepasster Software. Darunter fallen beispielsweise Viren (die sich an Wirtsprogramme hängen und dadurch verbreitet werden), Würmer (die wie Viren funktionieren, sich aber ohne Wirtsprogramme verbreiten) oder Trojaner (die kombinierte Wirtsprogramme mit versteckter Funktion darstellen). Beim »Hacking« werden gezielt Schwachstellen in Programmen und Sicherheitssystemen gesucht, um diese auszunutzen. Dazu zählen das Knacken von Passwörtern, das Scannen von Systemen nach bekannten Verwundbarkeiten, das Mitschneiden bzw. Abhören des Netzwerkverkehrs, die Vorspiegelung von Fakten, die so nicht existieren (»Spoofing«) sowie das aktive Eindringen in Telekommunikationskomponenten wie Telefonnetzwerke (»Phreaking«) und drahtlose Netzwerke (»Wardriving«). Eine häufig eingesetzte Spielart zur Beeinträchtigung der Verfügbarkeit von IT-Systemen ist eine durch

legal means against actor-related, technological, organizational and natural hazards that endanger the security of cyberspace (including infrastructure and data security) and the security of users in cyberspace." Cybersecurity is intended to contribute to the identification, evaluation, and prosecution of threats; also, it is supposed to strengthen the capability of coping with interferences in and from cyberspace, of mitigating the consequences associated, and of restoring the ability to act and functionality of actors, infrastructures, and services affected.

Three central protection objectives

Cyberattacks are assaults using information technology (IT) tools in cyberspace that are directed against one or more IT systems and aim to violate the security of information and communication technologies (ICT security). Measures to ensure cybersecurity mainly apply to the following three dimensions:

- The "availability" protection objective refers to the requirement of keeping data and systems available and accessible. Interferences that can lead to an interruption or complete shutdown of the systems are to be precluded.
- "Confidentiality" means that data are only available to authorized users. This implies the requirement that data may not be viewed by unauthorized third parties. Digital data theft violates this protection objective as does the unencrypted transmission of data through insecure networks.
- Finally, the "integrity" objective consists in the requirement that data must be accurate and consistent. Data may not be altered by unauthorized third parties.

Cyberattacks are often launched through malware—that is, through the deployment of specially programmed or adapted software. This includes viruses (which are spread by attaching themselves to host programs), worms (which work like viruses but do not use host programs to spread), or Trojans (which are combined host programs with hidden functions). "Hacking" is the process of specifically looking for vulnerabilities in programs and security systems in order to exploit them. This includes the cracking of passwords, the scanning of systems for known vulnerabilities, the recording or intercepting of network traffic, the presentation of false facts ("spoofing"), and active intrusion into telecom components such as telephone networks ("phreaking") and wireless networks ("wardriving"). One frequently used variant to hamper the availability of IT systems is to cause an overload-induced non-serviceability in what experts refer to as a

Überlastung herbeigeführte Dienstverweigerung, in der Fachsprache (Distributed) Denial of Service (DDoS). Auch organisatorische Schwachstellen können ausgenutzt werden.

Alte und neue Formen der Kriminalität

Wodurch sind die Cyberschutzziele am meisten gefährdet? Ein prominenter Bereich ist Kriminalität im weitesten Sinne. Unter Cyberkriminalität werden alle rechtswidrigen Angriffe aus dem Cyberraum auf oder mittels IKT-Systemen verstanden, die strafrechtlich oder verwaltungsstrafrechtlich normiert sind. Das umfasst jede Form von Straftaten, die mithilfe von Informationstechnologien und Kommunikationsnetzen begangen werden. Dazu zählt auch die Internetkriminalität. Das beginnt beim Diebstahl von Passwörtern, Identitäten und Daten und reicht bis hin zur Erpressung (etwa durch Ransomware/Verschlüsselungstrojaner). Bei Cyberkriminalität liegt der Schwerpunkt meist auf dem Erzielen von Profit und dem Diebstahl digitaler Identitäten, mit denen ebenfalls Geld erwirtschaftet werden kann. Es kann sich aber auch um Racheakte handeln – etwa weil sich jemand ungerecht behandelt fühlt.

Wirtschaftliche, aber auch politische Motive stehen bei der Industrie- und Wirtschaftsspionage im Vordergrund. Cyberspionage richtet sich gezielt gegen die Vertraulichkeit eines IT-Systems und ist meist eine Form hochorganisierter Kriminalität, hinter der große Unternehmen oder Staaten stehen. Zu den Zielen solcher Cyberangriffe zählt etwa der Zugang zu geschäftsvertraulichen Informationen wie etwa Konstruktionsplänen oder Forschungs- und Entwicklungsergebnissen, zu Informationen über Vertragspartner, Finanzdaten oder Hinweisen zur künftigen strategischen Ausrichtung der Konkurrenz. Die Spionage mit digitalen Mitteln gefährdet nicht nur den Erfolg von Unternehmen, sondern auch die nationale Wettbewerbsfähigkeit und untergräbt damit die nationale Souveränität. Zumindest bei manchen Staaten ist Cyberspionage Teil der Wirtschaftspolitik, um die eigene Wirtschaft zu schützen.

Hinter Cybersabotage, bei der die Integrität und Verfügbarkeit von IT-Systemen angegriffen werden, stehen meist ebenfalls wirtschaftliche und politische Motive. Wie bei allen anderen Bereichen verstärken auch hier die neuen Möglichkeiten durch digitale Technologien die Bedrohungsszenarien. Während früher beispielsweise eine Eisenbahnstrecke durch einen gefällten Baum lahmgelegt werden konnte, reicht heute im Extremfall ein Mausklick, um alle Züge in einer Region stillstehen zu lassen.

Nur mehr ein kleiner Schritt ist es dann zu Cyberterrorismus, dem Missbrauch des Internets für extremistische Zwecke. Das Ziel ist häufig, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens mit dem Vorsatz herbeizuführen, die Bevölkerung einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung

(Distributed) Denial of Service (DDoS) attack. Organizational weaknesses can also be exploited.

Old and new types of crime

What, then, is the greatest threat to cyber protection objectives? One conspicuous area is crime in the broadest sense of the word. Cybercrime is defined as any kind of illegal attack from cyberspace on, or through, ICT systems that is punishable under criminal or administrative criminal law. Covered under this are any and all crimes committed with the help of information technologies and communication networks. This includes Internet crime. It starts with password, identity or data theft and extends all the way to blackmail and extortion (e.g. through ransomware/encryption Trojans). In cybercrime, the focus is mostly on making a profit and on stealing digital identities that can also be used to make money. But it may also be acts of revenge—for example, because someone feels treated unjustly.

Economic as well as political motives are at the forefront of industrial and economic espionage. Cyberespionage is specifically targeted against the confidentiality of IT systems and, in most cases, is a form of highly organized crime, behind which there are large corporations or nation-states. The goals of cyberattacks include gaining access to business secrets such as construction plans or research and development data, information about contractual partners, financial data, or information about competitors' future strategies. Digital espionage puts a threat not only to the success of businesses, but also to national competitiveness, and undermines national sovereignty. At least in some countries, cyberespionage is part of economic policy to protect their own economy.

Cybersabotage, in which the integrity and availability of IT systems are attacked, is usually also driven by economic and political motives. As in all other areas, the new possibilities offered by digital technologies aggravate the threat scenarios. While in the past, for example, a railway line could be blocked by a felled tree placed on the track, a single mouse click can, in extreme cases, be enough today to bring all trains in a region to a standstill.

From there, it is only a small step to cyberterrorism, the abuse of the Internet for extremist purposes. The aim often is to cause a serious or prolonged disruption of public life, or serious damage to economic life, with the intent of intimidating the population, coercing public authorities or an international organization into engaging in, tolerating, or refraining from a certain course of action, or severely shattering or destroying fundamental political, constitutional, economic or social structures of a nation-state or an international organization.

zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören. Mit Cyberterror können aber auch andere Handlungen – zum Beispiel Spionage – verschleiert werden.

Angriffsziel kritische Infrastruktur

Besonders hohes Bedrohungspotenzial durch Cyberkriminalität, -sabotage und -terrorismus besteht für die sogenannte kritische Infrastruktur. Darunter versteht man jene Infrastrukturen oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben. Ihre Störung oder Zerstörung hat schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl der Bevölkerung oder die Funktionsweise von staatlichen Einrichtungen. Das umfasst Sektoren wie Energie, Verkehr, Transport, Finanzen oder die öffentliche Verwaltung. Eine Hauptschwierigkeit beim Schutz kritischer Infrastruktur ergibt sich aus den häufig komplexen Verantwortlichkeiten, Zuständigkeiten und Kompetenzen der verschiedenen beteiligten Organisationen und Unternehmen.

Beeinflussung der Gesellschaft

Ein ganz anderer Bereich der Cybersicherheit betrifft das Funktionieren der Gesellschaft als Ganzes. Durch gezielte Beeinflussung, etwa durch Fake News (Falschmeldungen) und gezielte Lügen, die von unzähligen extra dafür eingerichteten Fake Accounts gestreut werden, kann die öffentliche Meinung beeinflusst werden. Das wird durch die Struktur der sozialen Medien – konkret: durch die »Echokammern« im Netz – begünstigt, durch die der Einzelne nur mehr bestimmte Meinungen und Weltanschauungen serviert bekommt. Auf diese Weise kann beispielsweise die Reputation von Einzelpersonen, von staatlichen Einrichtungen und von Unternehmen nachhaltig gefährdet werden. Überdies können Verwirrung sowie Unruhe im öffentlichen Raum geschaffen werden. Das wiederum kann das Funktionieren demokratischer Systeme beeinträchtigen oder sogar gefährden. Ein großes Thema ist zurzeit die Beeinflussung von Wahlen.

In einem Cyberkrieg – einer kriegerischen Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik – kommen alle bisher beschriebenen Faktoren zusammen. Die Mittel in einem Cyberkrieg sind im Grunde dieselben wie bei zivilen Cyberattacken, allerdings ist das Ausmaß des Konflikts so groß, dass die Situation nur mehr durch das Eingreifen von Armeen zu bewältigen ist. Das beinhaltet auch und vor allem sogenannte heterogene Angriffe, bei denen physische Welt und Cyberwelt gleichzeitig angegriffen werden – wenn etwa die Stromversorgung lahmgelegt und durch gezielte Desinformation ein entstehender Aufruhr angeheizt wird. Staaten haben für einen

Cyberterror may, however, also be employed to conceal other hostile acts, such as espionage.

Targeting critical infrastructure

The potential threat of cybercrime, cybersabotage, and cyberterrorism is particularly high for so-called critical infrastructure. The term refers to infrastructures, or parts of infrastructures, that are of critical importance to maintain important social functions. Their disruption or destruction has severe consequences for public health or public security, for the economic and social well-being of the population, or for the functioning of government institutions. This includes sectors such as energy, traffic, transportation, finance, or public administration. One main difficulty in protecting critical infrastructure arises from the frequently complex responsibilities, jurisdictions, and competences of the various organizations and corporations involved.

Influences on society

A very different area of cybersecurity has an impact on the functioning of society as a whole. Deliberate misinformation, for example, through fake news and targeted lies spread by countless fake social-media accounts that are set up specifically for the purpose can have an influence on public opinion. This is facilitated by the very structure of social media—specifically, the “echo chambers” on the net—which serve individuals only with very specific opinions and worldviews. In this way, lasting damage may, for example, be done to the reputation of individuals, state institutions and corporations. In addition, confusion and unrest may be caused in the public realm. This in turn may impair or even jeopardize the functioning of democratic systems. A major topic at present is the interference in general elections.

In a cyberwar—a warlike confrontation in and around virtual space mainly fought with weaponized information technologies—all the factors described come together. The means of cyberwarfare are basically the same as those for civilian cyberattacks, but the conflict has such an extent that the situation can only be dealt with by army intervention. Above all, this also includes so-called heterogeneous attacks, in which the physical world and the cyberworld come under simultaneous attack—if, for example, the power supply is paralyzed and riots are incited by targeted disinformation. Nation-states have defined rules and established governmental bodies for such cases to decide whether an attack is to be considered as a national crisis and whether the army may be deployed to take military action—beyond “classical” operations by land, sea and air—also in virtual space.

solchen Fall Regeln definiert und Gremien eingerichtet, die entscheiden, ob es sich bei einem Angriff um einen nationalen Krisenfall handelt und das Heer tätig werden darf und – zusätzlich zu »klassischen« militärischen Operationen zu Land, Wasser und Luft –auch militärische Aktionen im virtuellen Raum setzen kann.

Gigantische Schadenspotenziale

Die wirtschaftlichen Schäden, die durch Cyberangriffe verursacht werden, sind immens. Genaue Zahlen hat freilich niemand – nicht zuletzt deshalb, weil der Großteil der Cybervorfälle nicht gemeldet oder bei den Behörden angezeigt wird. Zudem gibt es neben direkten Schäden – etwa bezahlten Erpressungsgeldern, Datenverlust oder Produktionsausfällen – auch zahlreiche indirekte Schäden, die oft erst in größerer zeitlicher Distanz oder in ganz anderen Bereichen anfallen. Dennoch liegen zahlreiche Schätzungen und Umfragen vor, aus denen Größenordnungen abgeleitet werden. Der aktuelle »Cambridge Global Risk Index« zum Beispiel bewertet das Risiko durch Cyberattacken mit 40 Milliarden Dollar pro Jahr – was der Studie zufolge sieben Prozent des globalen Risikos entspricht. Das Beratungsunternehmen Accenture schätzt, dass Cyberkriminalität im Jahr 2017 einen Schaden von 11,7 Milliarden Dollar angerichtet hat. Allein der Schaden durch Erpressungstrojaner (Ransomware) wird mit fünf Milliarden Dollar angegeben.

Auf deutlich höhere Zahlen kam eine Untersuchung des deutschen Digitalverbands Bitkom, der für die Jahre 2016 und 2017 von einem Gesamtschaden für die deutsche Industrie in Höhe von rund 43 Milliarden Euro spricht. Die US-Regierung wiederum veröffentlichte im Vorjahr einen Bericht, laut dem die US-Wirtschaft einen jährlichen Schaden durch Cyberattacken zwischen 57 und 109 Milliarden Dollar erleidet. Das Sicherheitsunternehmen McAfee bezifferte in einer Untersuchung aus dem Vorjahr den weltweiten Schaden durch Cyberkriminalität mit 600 Milliarden Dollar. Bei anderen Organisationen gehen die Schätzungen sogar bis hin zu mehreren Billionen Dollar. ×

Huge potential damage

The economic damage caused by cyberattacks is immense. There are, however, no exact numbers available—not least because the majority of cyberattacks are not made public or reported to authorities. In addition to direct losses—such as extortion money paid, data loss, or production stoppages—there also is a large amount of indirect damage, which only makes itself felt over time or in entirely different areas. Nevertheless, there are numerous estimates and surveys to determine the scale of the problem. The current "Cambridge Global Risk Index," for instance, assesses the risk from cyberattacks to amount to 40 billion dollars per year—which, according to the study, would account for seven percent of the global risk. The consulting firm Accenture estimates that cybercrime caused 11.7 billion dollars in damage in 2017. The damage caused by blackmail Trojans (ransomware) alone is estimated at five billion dollars.

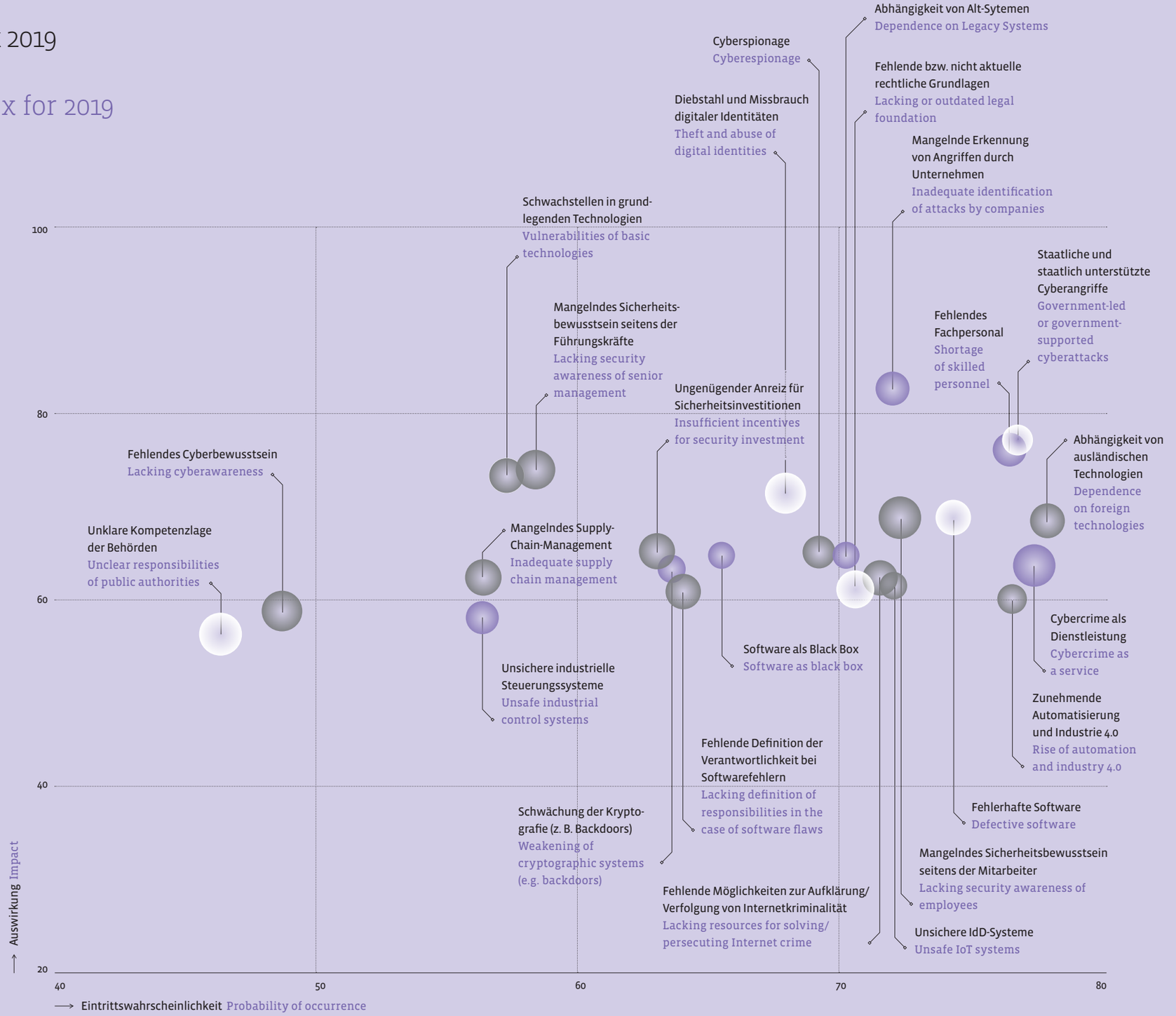
A study published by the German Bitkom Digital Association arrived at significantly higher numbers, estimating the total damage for the German industrial sector at around 43 billion euros for the years 2016 and 2017. The US government published a report last year, according to which the US economy suffered a total annual damage between 57 and 109 billion dollars from cyberattacks. In a survey published last year, the cybersecurity company McAfee puts the global damage caused by cybercrime at 600 billion dollars. Estimates of other organizations even go as high as several trillion dollars. ×

Cybersecurity-Risikomatrix 2019
(vereinfacht)

Cybersecurity Risk Matrix for 2019
(simplified)

Die KSÖ-Cybersecurity-Risikomatrix 2019 zeigt die von Vertretern von Behörden, Wirtschaft und Wissenschaft interpretierte Landschaft von Security-Risiken.

The KSÖ cybersecurity risk matrix for 2019 shows the landscape of security risks as interpreted by representatives of public authorities, industries, and academia.



- sehr hohes Risiko very high risk
- hohes Risiko high risk
- mittleres Risiko medium risk

größere Kreise bedeuten ein geringeres Vorbereitetsein
larger circles mean inadequate preparedness

Aktuelle Situation in Österreich: Cybersecurity-Risikomatrix 2019

Das Kuratorium Sicheres Österreich (KSÖ) befasst sich seit seiner Gründung im Jahr 1975 mit Themen der inneren Sicherheit. Im Jahr 2011 wurde das Themenspektrum um den Bereich der Cybersecurity erweitert, indem gemeinsam mit dem Innenministerium eine Cybersecurity-Initiative ins Leben gerufen wurde. Das erste Produkt dieser Initiative war die Erstellung einer Cybersecurity-Risikomatrix. Von Beginn an wurde dabei ein breiter, gesamtgesellschaftlicher Ansatz verfolgt, der sowohl technische Bedrohungen als auch (wirtschafts-) politische Themen beinhaltete.

2011 war das Thema Cybersecurity noch eine Angelegenheit von Experten. Doch schon damals lag auf der Hand, dass Cybersicherheit nicht nur ein technisches, sondern vor allem ein strategisches Problem ist. Fünf Jahre später, im Jahr 2016, erstellte das KSÖ erneut eine Risikomatrix, und es zeigte sich, dass manche Bedrohungen – wie z. B. mangelndes Sicherheitsbewusstsein – weiterhin bestanden, ohne dass entsprechende Maßnahmen ergriffen worden wären.

Die Cybersecurity-Risikomatrix 2019 zeigt einige sehr interessante Unterschiede zur Matrix von 2016. So ist das größte Risiko von 2016, die Abhängigkeit von ausländischen Sicherheitstechnologien, von der Spitze in das Mittelfeld gerückt. Als neues Toprisiko werden staatliche und staatlich unterstützte Cyberangriffe gesehen, knapp gefolgt von fehlendem Fachpersonal bzw. Sicherheitsexperten.

Cyberkriminalität ist im Vergleich zu 2016 in Bezug auf die Risikoeinschätzung fast unverändert geblieben. Das Gleiche gilt auch für das mangelnde Sicherheitsbewusstsein seitens der Mitarbeiter, unsichere IdD-Systeme und fehlerhafte Software. Deutlich gesteigert hat sich das Risiko der Abhängigkeit von Cloud-Providern. Stark reduziert hat sich hingegen das Risiko, das von DDoS-Angriffen ausgeht.

Staatliche und staatlich unterstützte Cyberangriffe werden als genauso wahrscheinlich, doch von ihrer Wirkung her als bedrohlicher angesehen als andere Spielarten der Cyberkriminalität. In Verbindung mit dem ebenfalls als hochriskant angesehenen Fachkräftemangel hat die Wirtschaft den Ergebnissen der Matrix zufolge diesem Risiko noch nicht genug entgegenzusetzen – was auch das ebenfalls hoch bewertete Risiko der mangelnden Erkennung von Angriffen durch Unternehmen bestätigt. Die Bedrohungslandschaft ist seit 2016 also komplexer geworden. ×

Quelle: *Cyber Security 2019 in Österreich*, hg. von KPMG Security Services GmbH. in Kooperation mit dem Sicherheitsforum Digitale Wirtschaft Österreich des Kuratoriums Sicheres Österreich

Status Quo in Austria: Cybersecurity Risk Matrix for 2019

Since its foundation in 1975, the Kuratorium Sicheres Österreich (KSÖ) has seen to the country's interior security. Cybersecurity was added to its spectrum of tasks in 2011, when a cybersecurity initiative was launched in collaboration with the Federal Ministry of the Interior. The first outcome of their initiative was the establishment of a cybersecurity risk matrix. A more general socio-political approach has been pursued from the very outset, comprising technological, economic, and political themes.

Back in 2011, the subject of cybersecurity was still considered a matter of experts. But even then, it was clear that it was not only a technological, but also and above all a strategic problem. Five years later, in 2016, the KSÖ drew up a new risk matrix. It turned out that some of the threats, such as lacking security awareness, still existed and that no specific measures to fight it had been taken.

The 2019 cybersecurity risk matrix shows some interesting differences compared to the matrix for 2016. For example, the highest risk in 2016, namely the dependence on foreign security technologies, has moved from the leading position to midrange level. Cyperattacks led or supported by governments are regarded as the new top risk, closely followed by a shortage of skilled personnel and security experts.

In terms of risk assessment, cybercrime has remained nearly unchanged compared to 2016. The same holds true for the lack of security awareness amongst employees, unsafe IoT systems, and defective software. The risk of dependence on cloud providers has clearly risen, whereas the risk posed by DDoS attacks has considerably declined.

Government-led or government-supported cyberattacks are considered as probable as other variants of cybercrime, but they are felt to be more threatening. According to the findings in the matrix, in combination with the shortage of skilled personnel, which is likewise considered extremely risky, the business world is still insufficiently prepared to counter this hazard—which is reinforced by the risk that companies are only inadequately capable of identifying attacks, which is also classified as high. This means that the threat landscape has grown more complex since 2016. ×

Source: *Cyber Security 2019 in Österreich*, ed. by KPMG Security Services GmbH in collaboration with Sicherheitsforum Digitale Wirtschaft Österreich of the Kuratorium Sicheres Österreich

Der großräumige 3-D-gedruckte biodigitale Prototyp *H.O.R.T.U.S. XL Astaxanthin.g* von ecoLogicStudio zeigt eindrücklich das Potenzial von Cyanobakterien (Blaualgen) auf. Diese lebende Architektur wird über die gesamte Ausstellungsdauer wachsen und kann im MAK-Kunstblättersaal durch Photosynthese Sauerstoff und Biomasse produzieren.

ecoLogicStudio's large-scale 3D-printed biodigital prototype *H.O.R.T.U.S. XL Astaxanthin.g* impressively demonstrates the potential of cyanobacteria (blue-green algae). This living architecture will grow throughout the duration of the exhibition and can produce oxygen and biomass through photosynthesis.

→ mak.at/spaceandexperience

VIENNA BIENNALE FOR CHANGE 2019
Teil der Ausstellung
SPACE AND EXPERIENCE
Architektur für ein besseres Leben

Part of the exhibition
SPACE AND EXPERIENCE.
Architecture for Better Living

CREDITS:
Exhibition view
SPACE AND EXPERIENCE
Architecture for Better Living
center: ecoLogicStudio (Claudia Pasquero and Marco Poletto), *H.O.R.T.U.S. XL Astaxanthin.g*, 2019

MAK Works on Paper Room
© Peter Kainz, MAK

Warum wir so verwundbar sind

Probleme und Schwachstellen, die von Cyberattacken ausgenutzt werden, kann es auf vielen verschiedenen Ebenen geben – von fehlerhafter Hard- und Software über unpassende Betriebsprozesse bis hin zu Fehlern bei der Bedienung. Gerade der Faktor Mensch stellt unverändert ein sehr großes Risiko dar.

Cyberangriffe werden in den allermeisten Fällen dadurch ermöglicht, dass es Schwachstellen in Informationssystemen gibt, die unberechtigten Dritten die Möglichkeit bieten, auf das System zuzugreifen. Solche Verwundbarkeiten kann es auf allen Ebenen geben, aufseiten der Hersteller genauso wie bei Betreibern und Benutzern.

Die Gefahr beginnt bei Fehlern in der Software. Die Ursachen für Programmfehler können vielfältig sein: Das reicht von menschlicher Unachtsamkeit und unscharf festgelegten Spezifikationen bis hin zu unerwarteten Änderungen der Umgebung. Komplexe Software wird typischerweise über längere Zeiträume hinweg entwickelt; es werden regelmäßig Updates durchgeführt, bei denen sich wieder neue Fehler einschleichen können. Es wird zwar viel Zeit und Aufwand in Sicherheitskonzepte, Tests und in die Verifikation investiert, dennoch gibt es in der Praxis wohl keine völlig fehlerfreie Software bzw. keinen Beweis für deren Fehlerfreiheit. Als gute und sichere Software gilt gemeinhin ein Programm, das pro 1000 Programmzeilen im Schnitt nur einen halben Fehler aufweist. Wenn man bedenkt, dass beispielsweise die Software für ein selbstständig fahrendes Auto rund 100 Millionen Programmzeilen umfasst, kann man sich leicht ausrechnen, wie viele Fehler sie wahrscheinlich enthält. Die meisten Softwarefehler führen dazu, dass bestimmte Teile eines Programms nicht richtig funktionieren – das kann zu Beeinträchtigungen der Funktionstüchtigkeit und der Betriebssicherheit führen. Manche Fehler können allerdings auch ein Einfallstor für Cyberattacken von außen sein – sie sind also relevant für die Angriffssicherheit.

Sehr tückisch sind Hardwarefehler. Davon können etwa die Weltmarktführer bei Rechnerchips ein Lied singen: Im Vorjahr fand eine internationale Gruppe unter maßgeblicher Beteiligung von Forschern der Technischen Universität Graz zwei schwerwiegende Designfehler bei Computerchips, durch die es möglich war, gesicherte Daten aus praktisch jedem PC auslesen zu können. Bekannt wurden dabei zwei Angriffsmethoden namens »Meltdown« und »Spectre«. Diese beiden Lücken konnten zwar recht schnell durch Softwareupdates geschlossen werden, allerdings auf

Why We Are so Vulnerable

Problems and weaknesses facilitating cyberattacks can be found on multiple levels—from flawed hard- and software to inadequate operating processes and maloperation. The human factor in particular still poses a major risk.

In most cases, cyberattacks are made possible by weaknesses in information systems that allow intruders to gain unauthorized access. Such vulnerabilities can exist on various levels—on the part of producers as well as on those of operators and users.

The danger begins with flawed software. The reasons for errors in computer programs can be manifold, ranging from human carelessness and inadequately defined specifications to unforeseen changes in the system environment. Complex software is typically developed over longer periods of time; regular updates are carried out, in the course of which new flaws can always creep in. Although a lot of time and effort is invested into security concepts, tests, and verification, there appears to be no completely error-free software or no proof of its faultlessness in practice. Software averaging not more than half a bug per 1,000 program lines is generally considered sound and safe. Taking into account that software for a self-driving car, for example, consists of some 100 million program lines, one can easily calculate how many errors it is likely to contain. Most software bugs cause certain parts of a program to malfunction—which can lead to functional deficiencies or reduce operational safety. Some bugs, however, may also work as backdoors for cyberattacks from outside—and are therefore relevant in terms of security.

Hardware faults are particularly malicious. Global market leaders for computer chips can tell you a thing or two about it. Last year it was with substantial support from researchers of the University of Technology in Graz that an international group discovered two grave design flaws in computer chips that made it possible to read out stored data from practically any PC. Two attack methods known as “Meltdown” and “Spectre” became known. It was possible to close these two security gaps relatively fast thanks to software updates, but at the cost of computing capacity, for the repair of vulnerabilities interferes with the central operation of processors. The maximization of processing speed is also the reason behind two further attack methods, which Graz researchers identified in spring this year (“ZombieLoad” and

Kosten der Rechenleistung, da bei der Behebung der Anfälligkeit in die zentrale Arbeitsweise von Prozessoren eingegriffen wird. Die Maximierung der Rechengeschwindigkeit ist auch der Grund für zwei weitere Angriffsmethoden, die Grazer Forscher heuer im Frühling gefunden haben (»ZombieLoad« und »Store-to-Leak Forwarding«): Dabei wird ausgenutzt, dass in modernen Computern viele Arbeitsschritte und Prozesse parallel ablaufen. Eine saubere Bereinigung dieser Probleme könnte die Rechenleistung glatt halbieren, meinen die Forscher.

Dieses Beispiel zeigt, dass Fehler selbst in den avanciertesten Hardwaretechnologien niemals ausgeschlossen werden können. Als einer der Hauptgründe dafür gilt, dass man sich bei der Entwicklung von Hardware noch stärker als bei jener von Software auf Funktionalität und Design konzentriert. Sicherheitsaspekten wird demgegenüber viel weniger Aufmerksamkeit geschenkt, und das auch deshalb, weil Haftungsfragen in der international stark arbeitsteiligen IT-Branche nicht ausreichend geklärt sind.

Internet der Dinge

Die genannten Probleme potenzieren sich durch das im Aufbau befindliche Internet der Dinge. Darunter versteht man die Vernetzung aller möglichen Geräte – von Autos und Kühlschränken bis hin zu Häusern und Spielsachen. Glaubt man Prognosen, wird die Zahl der über das Internet verbundenen Geräte in den nächsten Jahren auf Dutzende Milliarden anwachsen. Komponenten mit unterschiedlichsten Sicherheitsstandards werden kombiniert, und die ganze Kette ist bekanntlich nur so stark wie das schwächste Glied. Grundsätzlich gilt überdies: Je komplexer ein System ist, umso mehr Möglichkeiten gibt es, dass sich Fehler einschleichen – etwa weil verschiedene Komponenten nicht optimal zueinanderpassen. Dadurch entstehen zahlreiche neue Schwachstellen, die ihrerseits den Weg für immer komplexere Bedrohungsszenarien ebnen.

Eine große Rolle spielen die Betreiber von IT-Systemen. Durch unpassende Betriebsprozesse (etwa bei der Vergabe von Berechtigungen), durch Sparen am falschen Platz (etwa den Verzicht auf regelmäßige Wartung oder auf kostenpflichtige Updates), durch unbedachte Kombination verschiedener Komponenten oder eine ungenügende Trennung kritischer IT-Systeme von der notorisch unsicheren Internetwelt schleichen sich zahlreiche Fehler und Lücken ein, die von findigen Angreifern gefunden und ausgenutzt werden können.

Faktor Mensch

Die nach wie vor größte Schwachstelle von IT-Systemen ist freilich der Mensch. Das Problem beginnt mit dem leidigen Thema Passwörter: Die Empfehlung lautet ja, dass diese möglichst stark sein und regelmäßig gewechselt werden sollen. In vielen Fällen überfordert das die Nutzer,

"Store-to-Leak Forwarding"); they take advantage of the fact that in modern computers many operations and processes run simultaneously. Coming up with clean solutions to these problems could in fact reduce computing power by half, researchers point out.

This example shows that not even in the most advanced hardware technologies can bugs be ruled out. One of the main reasons for this is that in the development of hardware, much more than in the development of software, the focus is on functionality and design. Compared to these two, considerably less attention is paid to security aspects. This is also the case because liability issues in the IT sector, which is strongly based on international labor division, have not yet been sufficiently clarified.

Internet of things

The above-mentioned problems are increasing exponentially through the Internet of things, which is currently on the rise. The term refers to a network consisting of all kinds of physical objects—from cars and fridges to toys and entire buildings. If prognoses can be believed, the number of devices connected to the Internet will be growing to dozens of billions within the next years. Components protected by different security standards are combined here, and it is well known that a chain is only as strong as its weakest link. Moreover, the basic rule applies: the more complex a system is, the more possibilities there are for flaws to worm their way in—for example because the various components are not ideally compatible. This results in numerous new vulnerabilities, which in turn pave the way for ever more complex threat scenarios.

The operators of IT systems play an important role in this. Due to inadequate operating processes (for example, when it comes to the assignment of access rights), because of economizing in the wrong place (such as giving up on regular maintenance or fee-based updates), and through the imprudent combination of various components or an insufficient disconnection of critical IT systems from the notoriously insecure Internet world, countless flaws and gaps will creep in that can then be found and exploited by resourceful attackers.

The human factor

Nevertheless humans still represent the greatest weakness in IT systems. The problem starts with the tedious theme of passwords: it is recommended that they should be as strong as possible and be changed on a regular basis. In many cases, this is more than users can cope with, and so they stick Post-it notes to their computer screens on which they have written down their access codes. Lacking security awareness in both employees and executive staff is still considered

sodass die Zugangscodes etwa als Post-its auf den Bildschirm geklebt werden. Mangelndes Sicherheitsbewusstsein sowohl bei Mitarbeitern als auch bei Führungskräften gilt unverändert als einer der größten Risikofaktoren im Bereich Cybersicherheit. Mit dem neudeutschen Wort »Social Engineering« werden Versuche beschrieben, Menschen in ihrem Verhalten so zu manipulieren, dass sie z. B. Passwörter oder Kontodaten bekannt geben. Sogenannte »Phishing«-Attacken, mit denen Betrüger durch gefälschte E-Mails an sensible Daten kommen wollen, zählen unverändert zu den häufigsten Formen der Internetkriminalität. Viele dieser Probleme, mit denen sich Firmen konfrontiert sehen, können unter anderem durch Benutzungsrichtlinien reduziert werden, die festhalten, welches Verhalten von Mitarbeitern erwartet wird.

Verschärft werden viele Cyberrisiken dadurch, dass es einen immer größer werdenden Fachkräftemangel zur Abwehr von Risiken gibt. So berichten bei Umfragen regelmäßig zwei von drei Unternehmen, dass sie keine geeigneten Mitarbeiter mit dem nötigen Know-how finden.

»Crime as a Service«

Überdies hinken Abwehrtechnologien stets den Angreifern hinterher – Lücken in IT-Systemen können erst geschlossen werden, wenn sie bekannt sind. Weltweit arbeiten unzählige kriminelle Gruppen daran, bisher unbekannte Schwachstellen zu finden und gegen – viel – Geld an Schadsoftware-Entwickler und Cyberkriminelle zu verkaufen. Dafür gibt es im Darknet regelrechte Märkte. Durch diese Szene, die in der Fachsprache »Crime as a Service« genannt wird, muss man als Angreifer über keinerlei technische Expertise verfügen.

Es gibt indes auch Fehler in Computersystemen, die bewusst eingebaut werden – sogenannte »Backdoors« (Hintertüren), durch die sich Behörden in an sich gut gesicherte Systeme einklinken können. So wurde heuer im April beispielsweise durch ein Informationsleck bekannt, dass in die neuen 5G-Handynetze gezielt Schwachstellen eingebaut werden sollen, durch die Behörden kriminellen Machenschaften auf die Spur kommen wollen. Unter Druck stehen derzeit auch so manche Betreiber von Messenger-Diensten, bei denen die Kommunikation zwischen den Nutzern gut verschlüsselt ist. Dadurch werden diese Dienste auch von kriminellen oder terroristischen Netzwerken intensiv genutzt – was den Strafverfolgungsbehörden klarerweise ein Dorn im Auge ist. Solche Hintertüren haben jüngst auch globale Verwerfungen ausgelöst: Einem chinesischen Produzenten von Netzwerktechnik wird von europäischen und US-amerikanischen Politikern und Experten vorgeworfen, Backdoors in ihre Produkte zu integrieren, sodass der chinesische Geheimdienst bei allen Transaktionen über diese Netze mithören kann. ×

one of the major risk factors in the wide field of cybersecurity. The term “social engineering” describes efforts to manipulate people in their behavior in such a way that they will readily pass on information like passwords or account data. So-called “phishing” attacks, by which fraudsters seek to obtain sensitive data through fake e-mails, continue to be among the most frequent occurrences of Internet crime. Many of the problems with which companies see themselves confronted could be reduced, among other things, through user guidelines specifying the behavior expected from employees.

Many cybercrises are aggravated by the fact that the shortage of skilled personnel capable of fighting relevant risks is increasing. In surveys two out of three companies regularly state that they cannot find suitable personnel having the necessary know-how.

“Crime as a service”

Moreover, defense technologies always lag behind resourceful intruders—gaps in IT systems can only be closed when they are known. Innumerable groups of criminals around the globe work at identifying yet unknown vulnerabilities and sell them to cybercriminals and developers of malware—for huge amounts of money. There are actual markets for this on the Dark Net. Thanks to this scene, which experts refer to as “crime as a service,” it is not necessary for an attacker to have any technological expertise.

Meanwhile, computer systems also have bugs that have deliberately been built in—so-called “backdoors” through which government agencies can log onto systems that are actually well protected. In April this year, for example, information leaked through that vulnerabilities are to be systematically built into the new 5G cellular networks. In this way, government agencies wish to track down criminal machinations. Furthermore, many an operator of messenger services, which are known for their efficient encryption of communication amongst users, has come under pressure these days. Their services are therefore also intensively made use of by criminal or terrorist networks, which is clearly a thorn in the side of law enforcement authorities. Such backdoors have recently also been the trigger of global political conflict: European and US politicians and experts have accused a Chinese producer of network technology of integrating backdoors into the company’s products, thereby enabling the Chinese intelligence service to eavesdrop on all transactions via these networks. ×

Alexander Janda im Gespräch

Demokratie als »eine der kritischsten kritischen Infrastrukturen«

Alexander Janda, geboren 1968 in Wien. Studium der Politikwissenschaften in Wien und Los Angeles, USA. Tätigkeit als Wissenschaftler, Meinungsforscher, politischer Konsulent und Vortragender. Seit 2014 Generalsekretär des Kuratoriums Sicheres Österreich (KSÖ).

Alexander Janda, Generalsekretär des Kuratoriums Sicheres Österreich (KSÖ), einer Plattform, die verschiedene Akteure und staatliche Sicherheitsdienstleister vernetzt, über die Wahrnehmung von Risiken und das Verhältnis zwischen Sicherheit, Freiheit und Privatheit.

Wie würden Sie die laufende Debatte um Sicherheit in Österreich beurteilen?

Alexander Janda: Ich nehme Folgendes wahr: Das, was man objektive Sicherheit nennen könnte, und das, was subjektiv wahrgenommen wird, driften immer weiter auseinander. Das trifft zunehmend auch auf die Wissenschaft und den täglichen politischen Diskurs zu.
Die aktuelle Kriminalitätsstatistik bestätigt, dass Österreich eines der sichersten Länder der Welt ist. Gleichzeitig entstehen durch Ableitung aus persönlichen Wahrnehmungen und Medienberichten über Tagesereignisse Sicherheits- oder besser gesagt Unsicherheitsbilder. Bei vielen Menschen herrscht große Verunsicherung. Ich glaube, das hat mit zwei Dingen zu tun: Zum einen steigt die Erwartungshaltung der Bevölkerung in Bezug auf die Gewährleistung von Sicherheit ständig. Zum anderen wird auch das Verständnis von persönlicher Sicherheit zunehmend weiter. Diese Entwicklung verknüpft sich damit, dass wir in einer immer komplexeren und unvorhersehbareren Welt leben. Manche nennen das VUKA-Welt; die Buchstaben stehen für Volatilität, Unsicherheit, Komplexität und Ambiguität. Globalisierung, Migrationsphänomene usw. führen zu zunehmender Desorientierung. Viele Menschen fragen sich, was in ihrem Leben noch stabil und konstant, was in ihrem beruflichen Umfeld noch berechenbar ist.

An interview with Alexander Janda

Democracy as “One of the Most Critical Critical Infrastructures”

Alexander Janda, born in Vienna in 1968. Studied Political Science in Vienna and Los Angeles. Has worked as a scientist, pollster, political consultant, and lecturer. Has held the post of Secretary General of the Kuratorium Sicheres Österreich (KSÖ) since 2014.

Alexander Janda, Secretary General of the Kuratorium Sicheres Österreich (KSÖ), a network bringing together various players and governmental security agencies, on the perception of risks and the relationship between security, freedom, and privacy.

How would you comment upon the current security debate in Austria?

Alexander Janda: I perceive the debate as follows: what could be referred to as objective security and what is perceived subjectively are drifting further and further apart. This increasingly also holds true for science and everyday political discourse. Recent crime statistics confirm that Austria is one of the safest countries in the world. At the same time, however, ideas of security or, better, insecurity develop from what is concluded from personal perception and media coverage of events of the day. Many people feel deeply unsettled. I believe that this has to do with two things: on the one hand, the population’s expectations as to a guarantee of security are constantly rising. On the other hand, people’s understanding of personal security is becoming broader and broader. This development can be associated with the fact that we live in an increasingly complex and unpredictable world, which is sometimes referred to as VUCA world: the letters stand for volatility, uncertainty, complexity, and ambiguity. Globalization, migration phenomena, etc. lead to increasing disorientation. Many people wonder what has remained stable and constant in their lives and in what ways their professional environment is still calculable.

Welche Rolle spielt dabei die virtuelle Welt?

AJ: Die Digitalisierung verstärkt die Dynamik dieses Prozesses. Viele Menschen beteiligen sich bereits an der virtuellen Welt, nutzen die wunderbaren Möglichkeiten des Internets und der sozialen Medien. Aber erst langsam begreifen sie, dass all das, was es an technischen Möglichkeiten gibt, mit denen Dinge schneller, einfacher und bequemer werden, auch mit Risiken verbunden ist. Das ist eine neue Erfahrung. Die Digitalisierung vermehrt außerdem die Zahl der Angriffsmuster und Situationen, in denen man angreifbar ist. Die Angriffsmuster waren bisher eingeschränkt: Früher ist man hin und wieder zur Bank gegangen, um Geld abzuheben. Da war man angreifbar. Heute kann man 24 Stunden lang Bankgeschäfte tätigen – und das kann ausgenutzt werden.

Viele Organisationen, darunter das KSÖ, bemühen sich seit Jahren um mehr Aufklärung der Bevölkerung. War man damit bisher erfolgreich?

AJ: Es wurde zwar in den vergangenen Jahren bereits viel Aufklärungsarbeit betrieben, aber ich stelle fest, dass die Risiken bei vielen erst jetzt ins Bewusstsein rücken. Das geht in die richtige Richtung, aber noch immer fallen viele Menschen z. B. auf die einfachsten E-Mail-Tricks herein – wobei man aber auch sagen muss, dass solche Fake-Mails auch immer besser und überzeugender werden.

Meiner Beobachtung nach tritt das Cyberthema in diversen Risikoanalysen immer mehr in den Vordergrund. Deckt sich das mit Ihrer Wahrnehmung?

AJ:: Ja, vor zehn Jahren war Cybersecurity noch nicht unter den großen fünf Sicherheitsfragen. Nun ist das Thema in die Champions League aufgestiegen. Allerdings darf man nicht übersehen, dass die anderen großen Risikothemen wie Urbanisierung, Globalisierung, Migration oder Klimawandel immer noch da sind.

Das KSÖ hat gemeinsam mit Partnern erstmals im Jahr 2011 eine Cybersecurity-Risikomatrix erstellt, in der systematisch Risiken für verschiedene Bereiche untersucht werden. Nun wurde eine Neufassung vorgelegt. Was hat sich seit 2011 verändert?

AJ: Während früher rein technische Fragen der Absicherung im Inneren von Unternehmen und Organisationen dominierten, stehen nun große systemische Fragestellungen und Risiken im Mittelpunkt. Das sind vor allem drei Bereiche. Erstens der Fachkräftemangel: Wir haben viel

What role does the virtual world play in this?

AJ: Digitization intensifies the dynamics of this process. Many people have already come to participate in the virtual world, making use of the wonderful opportunities offered by the Internet and social media. However, they recognize only gradually that everything there is in terms of technological possibilities, thanks to which things become faster, easier, and more convenient, is also associated with risks. This is a new experience. Digitization also multiplies the number of attack patterns and situations in which one is vulnerable. Attack patterns have so far been limited: we used to go to the bank to withdraw money now and then—in these situations we were vulnerable. Today we can transact banking business around the clock—and this can be taken advantage of.

Many organizations, including the KSÖ, have tried for years to inform the population and raise awareness of problems in this sphere. Have they been successful?

AJ: Although a lot of educational work aimed at counteracting cybercrime has been done I can't help noticing that many people have become aware of risks only now. What is done is going in the right direction, but many people are taken in by the simplest e-mail tricks—although it has to be admitted that such fake mails have become much better and more persuasive.

According to my observations, the cybertheme increasingly pushes to the fore in diverse risk analyses. Does this correspond with your own perceptions?

AJ: Yes, ten years ago cybersecurity was not yet among the big five security issues. Now the topic has been promoted to the Champions League. But one must not overlook that other major risk themes, such as urbanization, globalization, migration, and climate change, still exist.

It was in 2011 that the KSÖ, together with several partners, drew up a cybersecurity risk matrix for the first time, which systematically examines risks in various spheres. Now a new edition has been presented. What has changed in comparison to 2011?

AJ: Whereas formerly purely technological issues concerning the internal security in companies and

zu wenige Menschen, die sich im Bereich der Cybersicherheit auskennen. Zweitens geht es heute nicht mehr nur um die Cyberkriminalität privater Personen oder Gruppen, sondern auch um staatliche Angriffe. Drittens wird die Abhängigkeit von nichteuropäischen Technologien immer entscheidender.

Mit dem Thema Sicherheit hängen auch andere gesellschaftliche Werte eng zusammen – etwa Privatheit oder Freiheit. Wie nehmen Sie dieses Verhältnis wahr?

AJ: Ich nehme eine fundamentale Widersprüchlichkeit wahr. Die Bevölkerung erwartet nicht nur mehr Sicherheit, sondern auch, dass die Polizei immer mehr Delikte aufklärt. Gleichzeitig fürchtet man aber den gläsernen Menschen: Es gibt viel Kritik und Sorge, dass unsere Privatsphäre und unsere Daten nicht gut genug geschützt sind. Das passt nicht zusammen: Man gibt zum Beispiel durch Kundenkarten oder die Nutzung sozialer Medien sehr viel Privates preis – meint aber gleichzeitig, dass die Polizei auf diesen Bereich keinen Zugriff haben sollte. Von Überwachungsvideos im öffentlichen Raum will man schon gar nichts wissen, stellt aber selbst alles Mögliche online. Dieses Spannungsverhältnis ist noch nicht gelöst. Um bei diesem Thema weiterzukommen, bräuchten wir so etwas wie eine Datensicherheitspolitik – so wie wir eine Arbeitsmarktpolitik oder Bildungspolitik haben.

Hat sich diese Widersprüchlichkeit in jüngster Zeit verschärft?

AJ: Ich denke nicht. Aber natürlich: Wenn man heute mehr Möglichkeiten hat, seine Daten preiszugeben, dann manifestiert sich das Problem an zahlreicheren Fronten als früher.

Ein zentraler Punkt im Bereich Cybersecurity ist die kritische Infrastruktur. Welche Tendenzen nehmen Sie bei diesem Thema wahr?

AJ: Seit ein, zwei Jahren beobachte ich, dass zunehmend die Demokratie als eine der kritischsten kritischen Infrastrukturen gesehen wird. Wir haben in jüngster Zeit einige Fälle erlebt, wo durch Fake News und andere Formen der Beeinflussung versucht wurde, die Basis der Demokratie anzugreifen, nämlich Wahlen. Das Vertrauen in die Demokratie ist ein fundamentaler Teil der Sicherheitsherausforderung.

organizations were dominant, now the focus is on major systematic problems and risks. Mainly three areas are concerned. First, the shortage of skilled personnel: we have way too few people with expertise in the field of cybersecurity. Second, this is no longer about cybercrime committed only by private individuals and groups, but also by governmental attackers. Third, the dependence on non-European technologies is becoming increasingly crucial.

The security theme is also linked to other social values—such as privacy or freedom. How do you perceive their relationship?

AJ: I perceive a fundamental inconsistence. The population no longer expects only more security but also that the police will solve more and more crimes. At the same time, a fear of the transparent citizen prevails: there are many worries and much criticism that our private sphere and our data might no longer be protected adequately. This does not go together: for example, by accepting customer loyalty cards or using social media, people reveal a lot of private information—but simultaneously think that the police should not have access to these data. Let alone surveillance videos in public space, which seem out of the question, although people put all kinds of things online. This contradiction has not yet been solved. To make progress here, we would need a data security policy—similar to a job market or education policy.

Have these inconsistencies become worse lately?

AJ: I don't think so. But, of course: there being more opportunities these days to reveal one's data, the problem manifests itself on more fronts than before.

A central point in the sphere of cybersecurity is critical infrastructure. What tendencies can you observe here?

AJ: I have noticed for one or two years now that democracy is increasingly seen as one of the most critical critical infrastructures. Most recently, we have had several cases where attempts have been made to attack the foundation of democracy, namely elections, through fake news and other forms of manipulation. Trust in democracy is a fundamental aspect of the security challenge.

Haben Sie persönlich Sorge, dass wir irgendwann einmal nicht mehr in der Lage sein werden, die Risiken durch die neuen Technologien zu beherrschen?

AJ: Ja und nein. Wie ist man in der Geschichte der Menschheit mit technischen Entwicklungen umgegangen? Es gab immer Ängste vor dramatischen technologischen Brüchen, ein hohes Maß an Skepsis und Vorstellungen von Katastrophenszenarien. Man hat aber immer einen gesellschaftlichen Konsens und Regelwerke gefunden, sodass es zu keiner Katastrophe gekommen ist. Sorgen macht mir allerdings eine Entwicklung, die sich vor allem in den USA und in China beobachten lässt. Dort wird seit einigen Jahren eine Gesichtserkennungsindustrie aufgebaut. In den USA geschieht dies vor dem Hintergrund einer Kommerzialisierung, in China vor dem Hintergrund einer umfassenden staatlichen Kontrolle – Stichwort: »social credit system«. Man liest, dass in China Fotos von 700 Millionen Bürgern gespeichert und kategorisiert sind, was die Entwicklung noch beschleunigt. Da sorge ich mich schon, dass diese Veränderungen das Ringen zwischen Sicherheits- und Kontrollanspruch, zwischen individueller Freiheit und Datenschutz ein für alle Mal entscheiden werden, ohne dass wir in einem demokratischen Diskurs abwägen können, was wir wollen und was nicht. ×

Are you personally worried that one day we will not be capable any more of remaining in control of the risks posed by the new technologies?

AJ: Yes and no. How has mankind coped with technological progress throughout history? There have always been fears of dramatic technological breaks, a high degree of skepticism, and ideas of catastrophic scenarios. But people have always reached a consensus in society and installed a system of rules preventing catastrophes. I am indeed worried, however, about a development we can primarily observe in the USA and China. For several years now, these two countries have been establishing facial recognition industries. In the USA this happens against the background of commercialization, whereas in China it is motivated by an all-encompassing form of governmental control—catchword: "social credit system." You can read that in China photographs of 700 million citizens have meanwhile been stored and categorized, which accelerates progress in this field. I am really anxious that these changes will decide the struggle between security and control, between individual freedom and data protection once and for all, without giving us a chance to deliberate in a democratic discourse what we are in favor of and what not. ×

Überblick über Angriffswaffen in der Onlinewelt

Wie im realen Leben – man denke nur an ein Messer – können auch in der virtuellen Welt viele Dinge für nützliche wie für schädliche Zwecke eingesetzt werden. Selbst so hilfreiche Einrichtungen wie etwa Internetsuchmaschinen dienen manchmal verbrecherischen Absichten. Es gibt freilich auch eine ganze Reihe von Erfindungen und Verfahren, mit denen dezidiert Schaden angerichtet werden soll. Ein kurzer Überblick über Begriffe und Abkürzungen aus der Welt der Cybersicherheit.

Advanced Persistent Threats (APTs)

Bei Angriffen dieser Art kommen verschiedene Techniken und Taktiken in Kombination zum Einsatz. Sie richten sich gezielt gegen bestimmte Organisationen, Firmen und Behörden, bei denen wertvolle Informationen zu holen sind. Meist kann damit sehr hoher Schaden angerichtet werden. Deshalb ist der Angreifer bereit, viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt dazu in der Regel über große Ressourcen. APTs werden auch »fortgeschrittene Malware« (advanced malware) genannt.

Backdoor

Backdoor (Hintertür) bezeichnet einen zusätzlich eingebauten Teil einer Software, der es ermöglicht, unter Umgehung der normalen Zugriffssicherung aus der Ferne Zugang zu einem Computer oder einer geschützten Funktion eines Computerprogramms zu erlangen.

Bot

Ein Bot – das Wort leitet sich vom slawischen Wort für Arbeit, »robota«, ab – ist ein Programm, das nach dem Empfang eines Befehls selbstständig bestimmte Aktionen ausführt. Sogenannte »malicious bots« können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen. Als Botnet (Botnetz) bezeichnet man eine Gruppe solcher automatisierter Schadprogramme.

CEO-Fraud

Von CEO-Fraud oder -Betrug ist die Rede, wenn Täter im Namen des Firmenchefs etwa die Buchhaltung anweisen, eine Zahlung auf ein (typischerweise ausländisches) Konto vorzunehmen.

Overview of Assault Weapons in the Virtual World

Like in real life — just think of a knife! — in the virtual world many things can be employed usefully or detrimentally. Even such helpful features as Internet search engines can sometimes serve criminal intentions. Of course there are also numerous inventions and methods contrived to cause harm deliberately. This is a short overview of expressions and abbreviations from the world of cyber security.

Advanced persistent threats (APTs)

For this type of attacks a combination of various methods and tactics is employed. They are systematically directed toward specific organizations, corporations, and authorities from which valuable information can be stolen. Most of them can cause excessive damage. Intruders are therefore prepared to invest a lot of time, money, and knowledge in their attack, and as a rule have substantial resources at their disposal. APTs are also referred to as “advanced malware.”

Backdoor

Backdoor refers to a feature additionally embedded in software that makes it possible to gain remote access to a computer or protected function of a computer program by circumventing standard access security.

Bot

A bot — the term derives from “robota,” the Slavic word for work — is a program carrying out actions autonomously upon reception of a command. So-called “malicious bots” are capable of remote-controlling compromised systems and triggering arbitrary actions. A botnet is a group of such automated malicious bots.

CEO fraud

When perpetrators, allegedly acting in the name of a company’s CEO, instruct the finance or accounting department to make a payment to a (typically foreign) account, this is called CEO fraud.

DDoS

Mit einer Distributed-Denial-of-Service-Attacke wird der Dienst oder das System des Opfers von vielen verschieden Systemen aus gleichzeitig angegriffen, sodass dieses zum Erliegen kommt und nicht mehr verfügbar ist. Dank gezielter Gegenmaßnahmen sind DDoS-Angriffe in jüngster Zeit rückläufig.

Exploit-Kit

Unter einem Exploit-Kit versteht man einen Baukasten, mit dem kriminelle Programme Scripts oder Codezeilen generieren können, um damit Schwachstellen in Computersystemen auszunutzen.

Malware

Malware – auf deutsch: Schadsoftware – ist ein Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt, wie Viren, Würmer oder Trojanische Pferde.

Man-in-the-Middle-Attacke

Eine Man-in-the-Middle-Attacke ist ein Angriff, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner einschaltet und dadurch deren Datenaustausch mitlesen oder verändern kann.

Phishing

Mittels Phishing versuchen Betrüger, an vertrauliche Daten ahnungsloser Internetnutzer zu gelangen. Dabei kann es sich z. B. um Kontoinformationen für Onlinekäufe oder Zugangsdaten für Onlinebanking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen z. B. E-Mails mit gefälschten Absenderadressen zustellen.

Ransomware

Bei Erpressungs- oder Verschlüsselungstrojanern handelt es sich um Schadprogramme, die Dateien auf der Festplatte und anderen verbundenen Speichern verschlüsseln. Dadurch werden diese Dateien für die Benutzer unbrauchbar und können, glaubt man den von den Kriminellen versendeten Erpressungsschreiben, nur durch Zahlung eines Lösegeldes wieder entschlüsselt werden.

Social Engineering

Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen. Eine bekannte Form von Social Engineering ist Phishing.

DDoS

In a distributed denial-of-service attack, the victim's service or system is attacked by various systems simultaneously so that it breaks down and is no longer available. Thanks to systematic counteractive measures, the number of DDoS attacks has recently declined.

Exploit kit

An exploit kit is a toolbox enabling criminal programs to generate scripts or lines of code by which they can take advantage of the vulnerabilities of computer systems.

Malware

Malware generally describes software that carries out harmful functions on a computer, such as viruses, worms, or Trojan horses.

Man-in-the-middle attack

A man-in-the-middle attack is an attack by which an intruder secretly enters the communication channel between two parties and eavesdrops on or interferes with their exchange of data.

Phishing

Fraudsters phish to gain confidential data from unsuspecting Internet users, such as account information for online sales or access data for online banking. Fraudsters take advantage of their victims' good faith and helpfulness, for example by sending them e-mails with false sender addresses.

Ransomware

Ransom or encryption Trojans are types of malware encrypting data that is stored on hard disks and connected memories. It is a way to make data useless, and users, believing the blackmail messages sent by the criminals, think the data can only be recuperated against payment of ransoms.

Social engineering

Social engineering attacks take advantage of people's credulity, helpfulness, or insecurity in order to gain access to confidential data and prompt victims to perform certain actions. Phishing is a familiar form of social engineering.

Trojan horses

Trojan horses—simply referred to as "Trojans"—are computer programs pretending to offer useful applications while carrying out other functions in the background without the user's knowledge.

Trojanische Pferde

Als Trojanisches Pferd – kurz »Trojaner« genannt – bezeichnet man ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.

Virus

Ein Computervirus ist ein sich selbst verbreitendes Programm, das sich in das Betriebssystem oder andere Computerprogramme einschleust und sich dabei selbst reproduziert. Einmal gestartet, kann es Änderungen an der Software vornehmen, mittelbar auch zu Schäden an der Hardware führen. Ein Antivirusprogramm aktiviert einen dauerhaften »Wächter«, der verdächtige Programme oder Prozesse meldet und deren Funktionieren unterbindet.

Watering-Hole-Angriffe

Watering-Hole-Angriffe sind gezielte Infektionen durch Schadsoftware über Webseiten, die bevorzugt von einer spezifischen Benutzergruppe besucht werden.

Webseiteninfektion

Bei einer Webseiteninfektion wird ein Computer allein durch den Besuch einer Webseite mit Malware infiziert. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote, die zwecks Verteilung der Schadsoftware zuvor kompromittiert wurden.

Wurm

Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtsprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen oder Anwendungen aus, um sich von Rechner zu Rechner selbstständig auszubreiten. ×

Quellen:
www.melani.admin.ch,
www.onlinesicherheit.
gv.at, Wikipedia

Virus

A computer virus is a self-replicating program that attaches itself to the system software or other computer programs in order to propagate. Once released, it can affect software and indirectly also damage the hard disk. Antivirus software activates a permanent “defender” that reports suspicious programs or processes and blocks their functions.

Watering hole attacks

Watering hole attacks are strategic infections with malware via websites preferably visited by specific user groups.

Website infection

In the case of website infection a computer comes to be infected because a website using malware has been visited. In many instances, the infected websites contain serious offerings that have been compromised in order to spread malicious software.

Worm

Unlike viruses, worms do not require a host program in order to propagate. Instead, they use vulnerabilities or configuration errors in operating systems or applications to spread by themselves from one computer to another. ×

Source:
www.melani.admin.ch,
www.onlinesicherheit.
gv.at, Wikipedia

Betriebliche Auswirkungen einer Erpressung durch Ransomware

Corporate consequences of blackmail with ransomware

Eine Onlineumfrage unter 190 deutschen Unternehmen, die 2016 von Ransomware (Erpressung) betroffen waren, ergab, dass die Schadsoftware in 156 Fällen in E-Mail-Anhängen enthalten war. 95 Prozent der Unternehmen sind nicht auf Lösegeldforderungen eingegangen, nur 18 Prozent haben Strafanzeige erstattet.

An online survey conducted among 190 German companies hit by ransomware attacks in 2016 revealed that in 156 cases the malware was contained in e-mail attachments. 95 percent of the companies ignored demands for ransom payments, while only 18 percent reported them to the police.

Quellen Sources

1 Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Federal Office for Information Security (BSI)

Geschichte und Gegenwart der Cybersicherheit

Das Thema Cybersecurity hat seit den 1970er-Jahren von Jahr zu Jahr an Brisanz zugenommen. Die Bedrohungsszenarien haben sich verändert und vervielfacht. Heute stehen vor allem (welt)politische Fragen im Zentrum der Debatte.

Cybersecurity war schon ein Thema, bevor es das Internet überhaupt gab. Bereits 1971 entdeckte der Arpanet-Entwickler Bob Thomas, dass es für Computerprogramme möglich ist, selbsttätig von einem Computer auf einen anderen überzuspringen. Er experimentierte mit dem Programm »Creeper«, das zwar lästig, aber harmlos war – bei befallenen Rechnen im vor allem wissenschaftlich genutzten Arpanet erschien die Nachricht »I'm the creeper: catch me if you can« auf dem Monitor. Darauf aufbauend entwickelte Ray Tomlinson »Creeper« weiter und verlieh ihm die Fähigkeit, sich selbst zu vermehren, womit der erste Computerwurm geschaffen war. Gleichzeitig konzipierte er eine Software namens »Reaper«, die »Creeper« einzufangen und zu vernichten vermochte – das war das erste Antivirenprogramm.

Große Auswirkungen in der Praxis hatten solche Experimente nicht. Doch im militärischen Bereich wurde die im Aufbau begriffene digitale Welt spätestens in den 1980er-Jahren zu einem Tummelplatz neuer Methoden. Bekannt wurde beispielsweise der deutsche Hacker Markus Hess, der 1986 über das Arpanet in militärische Computer des US-Verteidigungsministeriums eindrang und Daten an den russischen Geheimdienst KGB verkaufen wollte. Er wurde gefasst.

1989, im Geburtsjahr des World Wide Web, kam es schließlich zum ersten wirklich großen Problem: Robert Morris programmierte einen Wurm, mit dem er Lücken im Betriebssystem Unix aufzeigen wollte. Das Programm machte sich allerdings selbstständig und führte zu einer massiven Verlangsamung des frühen Internets – dies war gleichsam der erste größere DDoS-Vorfall. Im selben Jahr kreierte Joseph Popp mit dem Trojaner AIDS die erste Ransomware, die allerdings noch leicht entfernbar war. Dennoch wurden die Behörden auf das Problem aufmerksam, und ab 1990 wurden sukzessive Gesetze und Agenturen zur Abwehr solcher Gefahren ins Leben gerufen.

Spätestens damals wurde Cybersicherheit zu einem Jahr für Jahr brennenderen Thema. Um hier nur einige Meilensteine zu nennen: 2003 startete die Hacktivistengruppe Anonymus mit Angriffen auf Behörden. 2007 begannen Internetangriffe auf Estland, die zeitweise praktisch das

Past and Present of Cybersecurity

Since the 1970s, the subject of cybersecurity has gained in explosiveness year by year. Threat scenarios have changed and multiplied. Today's debates focus primarily on (global) political issues.

Cybersecurity was discussed even before the Internet existed. As early as 1971, Arpanet inventor Bob Thomas discovered that it was possible for computer programs to switch independently from one computer to another. He experimented with the program "Creeper," which was irritating but harmless—in affected computers on the Arpanet, which was mostly used by science and research, the following message appeared on the screen: "I'm the creeper: catch me if you can." Building on this, Ray Tomlinson developed "Creeper" further and gave it the ability to multiply autonomously, thereby creating the first computer worm. Simultaneously, he conceived a type of software called "Reaper," which was able to catch the "Creeper" and destroy it—the first antivirus program.

In practice, these experiments had little impact. But by the 1980s the digital sphere, being on the rise, had become a playground for new methods in the world of the military. The German hacker Markus Hess, for example, became known for breaking into military computers of the United States Department of Defense in 1986 via the Arpanet and for trying to sell data to the Soviet security agency KGB. He was caught.

In 1989, the year of birth of the World Wide Web, the first serious problem finally occurred: Robert Morris programmed a worm with which he wanted to point out holes in the Unix operating system. However, the software took on a life of its own and led to a massive deceleration of the early Internet—this was practically the first major DDoS incident. That same year, Joseph Popp, devising the Trojan AIDS, created the first ransomware, which was still easy to eliminate though. Nevertheless, the problem alarmed government agencies; starting in 1990, a succession of laws and institutions were put in place to fight dangers like this.

It was by then at the latest that cybersecurity had become an ever more burning issue year after year. Let us mention only a few milestones here: in 2003 the hacktivist group Anonymus launched its attacks on government institutions; in 2007 Internet attacks on Estonia began, virtually paralyzing the entire country at times; in 2010 the computer worm "Stuxnet" became known, which had been developed

ganze Land lahmlegten. 2010 wurde bekannt, dass der Computerwurm »Stuxnet« gezielt Steuerungssysteme (von Siemens) angreift, die u. a. in Urananreicherungsanlagen im Iran eingesetzt werden. 2014 wurden bei Yahoo Daten von 500 Millionen Nutzern entwendet. 2016 versuchten Kriminelle mehrfach, in den Datenverkehr des globalen Zahlungssystems SWIFT einzubrechen. 2018 mussten die Fluggesellschaften British Airways und Cathay Pacific Datenlecks einräumen, bei denen 380.000 bzw. 9,4 Millionen Kundendaten entwendet wurden.

Zahl der Angriffe steigt weiter

Mit der unaufhörlichen Expansion der Cyberwelt wächst die Zahl der Angriffe stetig. Dem aktuellen *Internet Security Threat Report* des US-Sicherheitsunternehmens Symantec zufolge ist die Zahl der Attacken über das Internet im Vorjahr um weitere 56 Prozent gestiegen. Jede zehnte Internetsite ist laut dieser Statistik »maliziös« – ein Jahr vorher war es »nur« eine von 16 Sites. Nach einer Erhebung des Beratungsunternehmens KPMG, bei der im Februar und März 2019 342 österreichische Unternehmen aller Größen und Branchen befragt wurden, wurden 66 Prozent der teilnehmenden Firmen in den vergangenen zwölf Monaten Opfer einer Cyberattacke. Zum Vergleich: Bei einer ähnlichen Umfrage im Jahr 2016 waren es 49 Prozent. Im Vorjahr erlitten 41 Prozent der Unternehmen einen finanziellen Schaden durch Cyberangriffe – aber nur 33 Prozent informierten öffentliche Stellen davon.

Weniger Ransomware

Im Detail zeigt dieser Bereich recht unterschiedliche Entwicklungen. Während etwa die Häufigkeit von Cyberangriffen auf mobile Geräte zunimmt und immer mehr Versuche gestartet werden, an Kunden- und Kreditkartendaten zu gelangen, sind Attacken durch Ransomware (Erpressung durch Verschlüsselungssoftware) tendenziell rückläufig. Das wird als Folge der größeren Aufmerksamkeit nach den riesigen Angriffen durch die beiden Schadprogramme »WannaCry« und »NotPeya« im Jahr 2017 angesehen, die einen Schaden von mindestens 300 Millionen Dollar verursachten. Auch mit DDoS-Attacken (Lahmlegen von IT-Systemen durch Überlastung) kommen immer mehr Organisationen wesentlich besser zurecht als noch vor einigen Jahren.

Unverändert zu den größten Cyberrisiken zählen hingegen Identitätsdiebstahl und Phishingangriffe (meist in Form gefälschter E-Mails): So wurden 24 Prozent der von KPMG befragten österreichischen Unternehmen zu Cyberopfern, weil sich Angreifer die Gutgläubigkeit oder die Neugierde von Mitarbeitern zunutze machen konnten. »Unreflektiertes Handeln öffnet Cyberkriminellen nach wie vor Tür und Tor«, fassen die Experten zusammen.

Die Palette der Angriffsmethoden wird indes immer größer, und auch die Professionalität der Attacken steigt unaufhörlich. So berichtete das Sicherheitsunternehmen McAfee Ende 2018 von einer neu entdeckten APT-Kampagne (Advanced Persistent Threat/fortgeschrittene andauernde

to systematically target (Siemens) control systems used, among other things, in uranium enrichment plants in Iran; in 2014 the data of 500 million users was stolen from Yahoo; in 2016 criminals attempted several times to hack into the data traffic of the global payment service SWIFT; in 2018 the airlines British Airways and Cathay Pacific were forced to admit the existence of leaks through which the data of 380,000 and 9.4 million passengers respectively had been stolen.

Growing number of attacks

With the cyberworld constantly expanding, the number of attacks keeps growing. The most recent *Internet Security Threat Report* issued by the US security corporation Symantec says that the number of attacks via the Internet rose by another 56 percent during the last year. According to this statistic, one in ten Internet sites is "malicious"—compared to "only" one in 16 sites the year before. According to a survey conducted by the consulting agency KPMG, for which 342 Austrian companies of diverse sizes and from various industries had been interviewed in February and March 2019, 66 percent of the participating enterprises had fallen victim to cyberattacks over the past twelve months. For comparison: a similar survey carried out in 2016 delivered a rate of 49 percent. Last year, 41 percent of the companies suffered monetary damage caused by cyberattacks—but only 33 percent reported the incidents to public authorities or government agencies.

Less ransomware

When looked at in detail, this field shows diverging developments. Whereas the frequency of cyberattacks on mobile devices is in the process of increasing and more and more attempts are launched to get access to the data stored on customer club and credit cards, attacks through ransomware (blackmail by means of encryption software) show a tendency to decline. This is regarded as a positive result of the heightened attention paid to the problem after the large-scale attacks using the two malicious programs "WannaCry" and "NotPeya" in 2017, which caused a damage of at least 300 million dollars. Organizations also tend to cope much better with DDoS attacks (blockage of IT systems by overloading them) than a few years ago.

However, identity theft and phishing attacks (mostly in the form of fake e-mails) continue to be among the greatest cyberrisks: 24 percent of Austrian enterprises interviewed by KPMG became cybervictims because the attackers successfully managed to take advantage of employees' credulity or curiosity. "Unreflecting action still opens up doors to cybercriminals," experts put the problem in a nutshell.

Bedrohung) gegen Unternehmen in den Bereichen Verteidigung, Energie, Atom und Finanz. Die Kampagne mit Namen »Sharpshooter« begann am 25. Oktober 2018 mit dem Versand verseuchter Dokumente an Personen von 87 Organisationen auf der ganzen Welt, hauptsächlich aber in den USA. Mittels Social Engineering sollten die Empfänger zum Öffnen infizierter Dokumente verleitet werden. Das Schreiben war als Bewerbungsschreiben getarnt und enthielt einen Link zu einem Dokument in einer Dropbox. Die Infektion erfolgte schließlich über ein im Word-Dokument enthaltenes Makro. Die Malware »Sharpshooter« installierte eine Hintertür, trug Informationen über Dokumente, Nutzernamen, Netzwerkkonfiguration und Systemeinstellungen zusammen und versandte diese. Überdies kann die Malware weitere Funktionen nachladen und ihre Spuren im Speicher verwischen, um nicht entdeckt zu werden.

Immer mehr (halb)staatliche Angreifer

Einen klaren Trend stellen viele einschlägige Studien und Berichte bei den Motiven von Cyberattacken fest: Im Vergleich zu reinen Profitmotiven werden demnach zurzeit politische Ziele immer wichtiger. Erstmals einer breiten Öffentlichkeit bewusst wurde das bei den Präsidentschaftswahlen in den USA im Jahr 2016. Seither gibt es kaum eine Wahl, bei der nicht Versuche der Beeinflussung über die Cyberwelt festgestellt wurden. In diese Kategorie dürfte auch der DDoS-Angriff auf Server der Stadt Wien fallen, bei dem im Mai 2019 u. a. die Antragstellung für Wahlkarten für die Wahl zum Europäischen Parlament betroffen war. Vor diesen Wahlen haben die Anbieter von Social-Media-Diensten eigenen Angaben zufolge viele Fake-Accounts stillgelegt.

Eng mit diesem Thema hängt wohl zusammen, dass Staaten bzw. halbstaatliche Akteure als Cybertäter immer bedeutsamer werden. Für das Jahr 2017 zählte das Centre for Risk Studies der Universität Cambridge 91 nationale oder staatlich gesponsorte Gruppen – davon viele aus China, Nordkorea, Russland, den USA und dem Iran, aber auch aus Israel, Palästina, dem Libanon, Syrien und Vietnam. Seither dürfte die Zahl weiter gestiegen sein. Im *Cyber Security Assessment Netherlands – CSAN 2018* werden Sabotage und Störungen durch Nationalstaaten mittlerweile als »bedeutendste Bedrohungen für die nationale Sicherheit« angesehen. Der Anbieter von Sicherheitslösungen CrowdStrike veröffentlichte im Februar 2019 eine interessante Statistik von mehr als 30.000 (entdeckten) Hackingversuchen: Gemessen wurde, wie rasch Eindringlinge in die Tiefen eines IT-Systems vordringen. Am schnellsten sind demnach russische Angreifer, gefolgt von Akteuren aus Nordkorea, China und dem Iran. Im Vergleich dazu relativ langsam agierten »normale« Cyberkriminelle, wobei es einzelne Gruppen durchaus mit den schnellsten staatlichen Akteuren aufnehmen können.

Angriffe durch (halb)staatliche Hacker werden freilich nur in den seltensten Fällen einer breiten Öffentlichkeit bekannt. Für Schlagzeilen sorgte beispielsweise ein Angriff auf die IT-Systeme der US-Stadt Atlanta im

Meanwhile the spectrum of attack methods has become ever more diversified, and attack methods keep improving as they become more and more professional. For example, in late 2018 the security technology company McAfee reported a newly disclosed APT (advanced persistent threat) campaign against companies operating in domains like defense, energy, nuclear power, and finance. The campaign named "Sharpshooter" was launched on October 25, 2018 with the dispatch of infected files to recipients in 87 organizations around the globe, although most of them were based in the United States. Social engineering methods were used to persuade recipients to open the infected documents. The messages, camouflaged as letters of application, contained Dropbox links. The infection was eventually brought about by a macro contained in a Word file. Having installed a backdoor, the malware "Sharpshooter" retrieved information from documents, user names, network configurations, and system preferences, and subsequently sent it off. In addition, this type of malware is capable of reloading further functions and covering its tracks in the memory so that it cannot be discovered.

More and more (semi)governmental attackers

The findings of numerous relevant studies and reports show a clear tendency when it comes to the motives of cyberattacks: compared to pure profit motives, political interests constantly gain in significance these days. A broader public first became aware of this in the US presidential elections in 2016. Since then there has hardly been an election for which no evidence of manipulation attempts via the cyberworld has been found. The DDoS attack on the server of the City of Vienna, which in May 2019 interfered, among other things, with applications for absentee ballot papers for the election of the European Parliament, also seems to fall under this category. By their own accounts, the providers of social media services closed many fake accounts before this election.

That governments and semigovernmental players become increasingly relevant as cybercriminals is apparently closely linked to this topic. For the year 2017, the Centre for Risk Studies at the University of Cambridge counted as many as 91 national or government-funded groups—primarily from China, North Korea, Russia, the USA, and Iran, as well as from Israel, Palestine, Lebanon, Syria, and Vietnam. It can be assumed that this number has grown since then. In the *Cyber Security Assessment Netherlands – CSAN 2018,* sabotage and disruption by nation-states are meanwhile regarded as "the most significant threats for the nation's security." In February 2019, CrowdStrike, a supplier of security solutions, published an interesting statistic of more than 30,000 (identified) hacking attempts: it was measured how rapidly

März 2018, wo das Leben de facto zum Stillstand kam, nachdem die Computer der Stadtverwaltung nach einem Ransomware-Angriff blockiert waren. Ein weiteres spektakuläres Angriffsziel war der amerikanische Hersteller von Atomkraftwerken Westinghouse, der von – mutmaßlich aus Russland gesteuerten – Hackern ausspioniert werden sollte. Auch die italienische Marineindustrie blieb nicht verschont, ebenso wenig französische Regierungsserver, das deutsche Auswärtige Amt oder Schweizer Banken – um nur einige wenige Beispiele zu nennen.

Sorgen wegen des Internets der Dinge und Fachkräftemangel

Die Palette der Angriffsmöglichkeiten ist so groß wie nie zuvor, sodass sich bei vielen Akteuren die Erkenntnis durchsetzt, dass es unmöglich ist, sich vorab gegen alle Risiken abzusichern. In der Debatte treten zwei andere Faktoren in den Vordergrund: Zum einen wird das Monitoring und die Fähigkeit, Angriffe rasch zu erkennen und adäquat darauf zu reagieren, immer wichtiger. Zum anderen sollen die zu schützenden Organisationen etwa durch ein funktionierendes Risikomanagement so gestaltet werden, dass sie gegenüber Cyberangriffen widerstandsfähiger werden – also trotz vermehrter Risiken betriebs- und funktionsfähig bleiben bzw. rasch wieder werden. Informationssicherheit sei »kein Zustand, sondern ein Prozess […], der laufende Evaluierungen, Anpassungen und Überarbeitungen erforderlich macht«, wird im aktuellen österreichischen Bericht *Cyber Sicherheit 2018* betont.

Mit der Ausbreitung des Internets der Dinge wird es zu einer rasanten Zunahme angreifbarer vernetzter Geräte kommen – von denen viele mangelhaft geschützt sind. Ein Beispiel für eine mögliche Bedrohung haben kürzlich Forscher des Georgia Institute of Technology durchgespielt: Wenn Automobile künftig online Daten austauschen, werden sie auch anfällig für Cyberangriffe, die für gezielte Attentate auf die Lenker, aber auch zum Schaffen chaotischer Zustände genutzt werden könnten. In einem Simulationsmodell haben die Forscher untersucht, welche Folgen das für den Verkehr in Manhattan haben könnte. Sie kamen zu dem Ergebnis, dass der Verkehrsfluss völlig zum Erliegen gebracht werden kann, wenn 10 bis 15 Prozent der Fahrzeuge gehackt werden – dann könnte es auch für Einsatzkräfte überhaupt kein Durchkommen mehr geben.

Als umfassendes Zukunftsthema nehmen Experten einen drückenden und immer schlimmer werdenden Fachkräftemangel wahr: So empfinden etwa 65 Prozent der von KPMG befragten österreichischen Unternehmen den Fachkräftemangel als Herausforderung. Laut einer Umfrage von Cisco Austria ist der Mangel an ausgebildeten Mitarbeitern noch vor Budgetrestriktionen die größte Hürde für ein umfassendes IT-Security-Update. Zum einen werden auf Universitäten und Fachhochschulen zu wenige Experten ausgebildet – in der Informatik gelten derzeit Studienplatzbeschränkungen. Zum anderen werden Absolventen sofort von großen Internetkonzernen mit teils aberwitzigen Gehaltsangeboten angeworben, sodass der freie

intruders advance to the depths of IT systems. The Russian attackers worked fastest, followed by those from North Korea, China, and Iran. Compared to them, "ordinary" cybercriminals proceed relatively slowly, although individual groups can easily keep up with the fastest governmental players.

Sure enough, attacks led by (semi)governmental hackers very rarely become known in public. For example, an attack on the IT systems of the US city of Atlanta in March 2018, which in fact caused life to stand still after the computers of the municipal administration had been blocked by an assault with ransomware, made it into the headlines. Another spectacular target of an attack was Westinghouse, an American supplier of nuclear power plants, which should be spied on by hackers (presumably directed from Russia). The Italian marine industry was not spared either, and neither were servers of the French government, the German Foreign Office, or Swiss Banks—to mention only few examples.

Worries about the Internet of things and a shortage of skilled personnel

As there are more possibilities for attacks than ever before, many players have come to the conclusion that it is impossible to guard against all the risks beforehand. In discussions, two factors have pushed to the fore: on the one hand, monitoring and the ability to identify attacks rapidly and respond adequately become ever more important; on the other hand, the organizations to be protected should, among other things, be furnished with an efficient risk management in such a way that they will become more resilient to cyberattacks—i.e., that they will remain operable and functioning or be able to quickly restore their operational reliability despite the existence of higher risks. As is emphasized in the recent *Cyber Security Report 2018* for Austria, information security is "not a state, but a process . . . that requires continuous evaluation, adaptation, and revision."

Due to the expansion of the Internet of things, the number of vulnerable networked devices—many of which are insufficiently protected—will increase rapidly. An example for a possible threat was recently played out by researchers of the Georgia Institute of Technology: if automobiles are going to exchange data online in the future, they will also become more prone to cyberattacks that might be used as targeted assassination attempts on the lives of drivers or as instruments to create chaos. In a simulation model, the researchers examined the consequences this could have for traffic in Manhattan. Findings showed that the flow of traffic could come to a complete standstill with only 10 to 15 percent of the vehicles being hacked—then it would also become impossible for rescue units to get through.

Arbeitsmarkt für Cybersecurity-Spezialisten ausgetrocknet ist. Besonders darunter leiden, wie man immer wieder hört, öffentliche Stellen, die an starre Gehaltsschemata gebunden sind.

Reformen nötig

Wie erwähnt, meldet derzeit nur ein Bruchteil der Unternehmen, die eine Cyberattacke erlitten haben, den Vorfall bei den Behörden. Das soll sich nun – vorerst einmal für Betreiber kritischer Infrastrukturen – durch die Umsetzung der EU-Netzwerk- und Informationssicherheitsrichtlinie (NIS) in nationales Recht ändern: Unternehmen kritischer Infrastruktureinrichtungen bekommen Standards vorgegeben, die Cybersicherheit zu verbessern, und müssen Sicherheitsvorfälle bei den zuständigen Computernotfallteams (CERTs) melden, sodass die Behörden erstmals einen Überblick über das tatsächliche Ausmaß der Bedrohungen bekommen, um darauf aufbauend Gegenmaßnahmen konzipieren und die bedrohten Organisationen bei der Abwehr unterstützen zu können. Das österreichische NIS-Gesetz trat mit Jahresbeginn 2019 in Kraft, viele Details zur Umsetzung, etwa nötige Durchführungsverordnungen, sind noch offen.

Durch die zunehmende Vernetzung auf allen Ebenen – sowohl in der virtuellen als auch in der physischen Welt (etwa durch Zulieferketten) – hängt die Sicherheit einer Organisation mehr denn je auch vom Sicherheitsniveau von Zulieferern, Geschäftspartnern, Technologielieferanten usw. ab. Nur sieben Prozent der von KPMG befragten österreichischen Unternehmen waren der Ansicht, dass ihre Lieferanten ausreichende Sicherheitsmaßnahmen setzen. Wie groß dieses Problem ist, wird etwa bei Automobilherstellern deutlich, die Tausende Komponenten zugeliefert bekommen, wobei die Zulieferer selbst wieder Teile von anderen Unternehmen beziehen. Was Software betrifft, gibt es derzeit so gut wie keine internationalen Vereinbarungen, die die Verantwortung in solchen Lieferketten festschreiben.

Einen Anlauf in diese Richtung unternimmt derzeit die EU: In Dezember 2018 haben sich das Europäische Parlament, der Rat und die Europäische Kommission auf einen neuen Rechtsakt zur Cybersicherheit verständigt, der weit über die bisher schon geregelten kritischen Infrastrukturen hinausgeht. Neben einer Stärkung der EU-Cybersicherheitsagentur ENISA wird darin ein europäischer Rahmen für eine Cybersicherheitszertifizierung geschaffen, der die Cybersicherheit von Onlinediensten und von Endgeräten für Verbraucher stärken soll. Ziel ist es, Sicherheitsmerkmale bereits in der Frühphase der technischen Konzeption und Entwicklung zu berücksichtigen (»eingebaute Sicherheit«). Durch eine europaweit einheitliche Zertifizierung können Unternehmen auch erhebliche Kosten sparen, da sie andernfalls mehrere Zertifikate in mehreren Ländern beantragen müssten. Das soll überdies den Binnenmarkt stärken und Unternehmen Anreize bieten, in die Cybersicherheit ihrer Produkte zu investieren und hieraus einen Wettbewerbsvorteil zu erlangen.

Experts have identified an alarming and deteriorating shortage of skilled workers as a wide-ranging theme of the future: 65 percent of the Austrian companies questioned by KPMG perceive the lack of competent personnel as a challenge. According to a survey conducted by Cisco Austria, the shortage of trained employees is regarded as the biggest obstacle for a comprehensive IT security update, coming even before budget restrictions. On the one hand, far too few future experts are trained at regular universities and universities of applied sciences—currently, places for students wishing to enroll for computer sciences are restricted. On the other hand, graduates are hired on the spot by the big Internet corporations and partly offered ludicrous salaries so that the free job market for cybersecurity specialists has metaphorically dried out. Time and again one can hear that those particularly suffering from the situation are government agencies or public authorities, which are bound to rigid salary schemes.

Reforms required

As has been mentioned earlier, currently only a fraction of the companies that have been hit by a cyberattack report the incident to the authorities. This is about to change—for the time being at least for the operators of critical infrastructures—now that the EU Network and Information Security Directive (NIS) has been transposed into national legislations: operators of critical infrastructural facilities have to adhere to certain standards in order to improve cybersecurity and report security incidents to the competent computer emergency teams (CERTs) so that the authorities will get a comprehensive overview of the actual scope of threats for the first time. This will enable them to develop countermeasures and assist the threatened organizations in their defense. The Austrian NIS Act came into force at the beginning of 2019; many details with regard to its implementation, such as the necessary executive orders, still need to be put in place.

Due to the increase of networking opportunities on all levels—in both the virtual and the physical world (such as through supply chains)—the security of an organization also depends more than ever on the security levels of suppliers, partners, technology providers, etc. Only seven percent of the Austrian companies interviewed by KPMG believed that their suppliers took adequate security measures. The actual scope of this problem is exemplified by the automobile industry: car manufacturers procure thousands of components from their suppliers, while they in turn obtain certain parts from other companies. As far as software is concerned, there are currently practically no international agreements regulating responsibilities in such supply chains.

The EU is presently making an effort in this direction: in December 2018, the European Parliament, the Council, and the European

Cybersicherheit und Weltpolitik

Noch dramatischere Folgen hat die mangelhafte Möglichkeit, Cyberangreifer grenzüberschreitend zur Verantwortung zu ziehen – und das vor allem dann, wenn staatliche Akteure beteiligt sind. Dazu fehlen derzeit jegliche Mittel. Diese Probleme beschäftigen immer mehr auch die Weltpolitik. Das prominenteste Beispiel dafür sind sogenannte Backdoors (Hintertüren) in Telekommunikationsnetzen: Einer der Weltmarktführer, der chinesische Huawei-Konzern, wird verdächtigt, den chinesischen Nachrichtendiensten Zugang zum weltweiten Datentransfer zu ermöglichen. Manche europäischen Staaten – vor allem aber die USA – wehren sich mit Händen und Füßen (und Strafzöllen und Sanktionen) gegen diese Möglichkeit, auch wenn Huawei die Existenz solcher Backdoors vehement in Abrede stellt.

Unmittelbar mit staatlichem Handeln zusammenhängt auch das Thema Staatstrojaner – das hier stellvertretend für eine Vielzahl von Methoden stehen soll, wie Strafverfolgungsbehörden kriminellen Machenschaften auf die Spur zu kommen trachten. Wie bei allen Technologien gilt, dass sie sowohl zum Guten als auch zum Schlechten verwendet werden können – in diesem Fall: zum einen zur Verhinderung von Straftaten, zum anderen für eine mögliche Überwachung der Bürger. Daraus ergibt sich ein immanenter Konflikt zwischen Sicherheit, Transparenz, Privatheit und Freiheit. Aus diesem Grund ist das »Sicherheitspaket«, das die österreichische Bundesregierung 2018 verabschiedet hat, vor dem Verfassungsgerichtshof gelandet.

Durch ein Datenleck wurde kürzlich bekannt, dass EU-Strafverfolger wohldefinierte Sicherheitslücken in den künftigen 5G-Handynetzen fordern – andernfalls seien Polizeibehörden »blind« gegenüber Vorgängen in den Netzen. Wie solche schwierigen Abwägungen zwischen Grundwerten künftig entschieden werden – wer wann unter welchen Umständen in Datenströme Einblick nehmen darf – ist eine der vielen offenen Fragen im Bereich Cybersicherheit. ✖

Commission agreed upon a new legal instrument governing cybersecurity that will go far beyond the current regulation of critical infrastructures. In addition to strengthening the EU cybersecurity agency ENISA, it will provide for a European framework for cybersecurity certification that is meant to improve the cybersecurity of both online services and terminal equipment for consumers. The goal is to take security features into account at an early stage of technological conception and development (“built-in security”). Thanks to a harmonized pan-European certification process companies will also be able to save considerable costs, as they will no longer be forced to apply for multiple certificates in several countries. Moreover, this is also meant to consolidate the single market and offer incentives for companies to invest in the cybersecurity of their products and thus gain a competitive advantage.

Cybersecurity and global politics

The fact that the possibilities to hold cyberattackers responsible across national borders are inadequate has even more dramatic consequences—particularly when governmental attackers are involved. Currently, the means to remedy this shortcoming are lacking completely. These problems also increasingly become a matter of global politics. The most prominent example are so-called backdoors in telecommunication networks: the Chinese Huawei corporation, one of the global market leaders, is suspected of granting Chinese intelligence agencies access to worldwide data transfers. Several European countries and above all the United States fight this with tooth and nail (as well as punitive tariffs and sanctions), even if Huawei vehemently denies the existence of such backdoors.

The subject of government Trojans, which is also directly linked to state action, is mentioned here as one example of a multitude of methods of how law enforcement authorities seek to track down criminal machinations. It goes for all technologies that they can be used for both the good and the bad—in this case: for preventing criminal actions on the one hand and for a potential surveillance of citizens on the other. From this results an immanent conflict between security, transparence, privacy, and freedom. For this very reason, the “security package” the Federal Government of Austria passed in 2018 ended up at the constitutional court.

Recently it became known through some data leak that EU criminal prosecutors demand well-defined security gaps to be installed in the future 5G cellular phone networks—otherwise police authorities would be “blind” to network incidents. How such delicate assessments of fundamental values will be decided in the future—who will be authorized to inspect data flows when and under what circumstances—is one of many open questions in the field of cybersecurity. ✖

Das von EOOS entwickelte *sov – Social Vehicle* ist ein kompaktes Elektroleichtfahrzeug mit drei Sitzplätzen, das mit einer Open-Design-Lizenz in kleinen, lokalen Werkstätten gebaut, verbessert und repariert werden kann. Der Ressourcenverbrauch in der Herstellung beträgt ein Zehntel von dem eines durchschnittlichen Mittelklassewagens.

The sov—Social Vehicle developed by EOOS is a compact, three-seater electric light vehicle that can be built, improved, and repaired in small local workshops with an open design license. Resource consumption in manufacturing is one tenth of that of an average mid-range car.

→ mak.at/klimawandel

VIENNA BIENNALE FOR CHANGE 2019
Teil der Ausstellung
KLIMAWANDEL! Vom Massenkonsum zur nachhaltigen Qualitätsgesellschaft

Part of the exhibition
CLIMATE CHANGE! From Mass Consumption to a Sustainable Quality Society

CREDITS:
Exhibition view
CLIMATE CHANGE! From Mass Consumption to a Sustainable Quality Society

EOOS, *SOV,* 2019
MAK DESIGN LAB

Wer sind die Cyberkriminellen?

Eine Studie der Donau-Universität Krems bringt interessante Einblicke

Wer sind die Menschen, die gezielt Computersysteme angreifen? Sind das gestandene Kriminelle? Oder bösartige Nerds, die von ihrem stillen Kämmerchen aus die Welt mit Chaos überziehen, Menschen ins Unglück stürzen und dabei abcashen? Oder eiskalte Geheimdienstagenten, die einen Gegner vernichten wollen? Oder abgehobene Wissenschaftler, die sich Ergebnisse anderer unter den Nagel reißen wollen? Angeregt durch einschlägige Filme oder auch im Internet aufgeschnappte Informationen haben wohl viele Menschen solche oder ähnliche Bilder im Kopf.

Die Realität ist in vielen Fällen um einiges profaner, wie eine unter der Leitung von Edith Huber durchgeführte Studie von Forschern am Zentrum für Infrastrukturelle Sicherheit der Donau-Universität Krems[1] zeigt – zumindest im engeren Bereich der Cyberkriminalität. Anhand von Akten des Wiener Straflandesgerichtes der Jahre 2006 bis 2016 wurden in der im Rahmen des österreichischen Sicherheitsforschungsprogramms KIRAS[2] geförderten Untersuchung (CERT[3]-Kommunikation II) Muster unter den Angeklagten gesucht. Die Delikte umfassten den gesamten Katalog von laut gültigem Strafgesetzbuch verbotenen Handlungen – von widerrechtlichem Zugriff auf ein Computersystem und der Verletzung des Telekommunikationsgeheimnisses über Datenbeschädigung und Missbrauch von Zugangsdaten bis hin zu Datenfälschung und Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses. Nicht betrachtet wurden z. B. Kinderpornografie und Angriffe aus dem Ausland. In zwei Dritteln der Fälle waren Unternehmen die Opfer.

Die Ergebnisse waren zum Teil erwartbar, zum Teil aber auch äußerst spannend: Im großen Durchschnitt sind Cyberkriminelle männlich (75 Prozent) und zwischen 21 und 30 Jahre alt (36 Prozent). Die meisten Tatverdächtigen wurden in Österreich (47 Prozent) oder in einem EU-Land (25 Prozent) geboren. Überdies leben sie in hohem Ausmaß in keiner festen Beziehung (65 Prozent) und haben keine Kinder (57 Prozent). Der Bildungsstand ist überraschenderweise zumeist gering: 54 Prozent der Angeklagten haben keine Matura. Und nur 20 Prozent sind regulär beschäftigt.

Noch interessanter ist eine Typisierung auf Grundlage der demografischen Merkmale: Die Studie unterscheidet drei Kategorien von Cyberkriminellen.

[1] Edith Huber, Bettina Pospisil (Hg.), *Die Cyber-Kriminellen in Wien,* Edition Donau-Universität Krems 2018; Download unter www.researchgate.net/publication/323486485_Die_Cyber-Kriminellen_in_Wien oder als Kindle-Ausgabe bei Amazon.

[2] Siehe https://www.kiras.at/#category-filter:path=default.

[3] Computer Emergency Response Team.

Who Are the Cybercriminals?

A study by Danube University Krems provides fascinating insights.

Who are the people attacking computer systems purposefully and strategically? Are they fully-fledged criminals? Or malicious nerds spreading chaos in the world and making people unhappy while cashing in from behind closed doors? Or cold-blooded intelligence agents determined to destroy an opponent? Or aloof scientists seeking to steal the findings of others?—These are pictures probably many people have in mind, inspired by relevant films or information picked up on the Internet.

In many cases, reality is much more profane, at least in the narrower field of cybercrime, as has been revealed by a study carried out by researchers at the Center for Infrastructural Security at Danube University Krems[1] under the supervision of Edith Huber. Based on Vienna Criminal Law Court files from the years 2006–2016, a search for recurring patterns amongst accused persons was conducted in the context of a study project supported by the Austrian Security Research Program KIRAS[2] (CERT[3] Communication II). The offenses comprised the entire catalogue of activities prohibited according to currently valid criminal law—ranging from illegal access to computer systems and the violation of the privacy of telecommunications to data corruption, abuse of access data, data forgery, and spying on industrial or company secrets. Child pornography and attacks from abroad have, among other things, not been taken into account. In two thirds of the cases, the victims were business companies.

Although many findings were expectable, some proved really remarkable: on average, cybercriminals are male (75 percent) and between 21 and 30 years old (36 percent). Most suspects were born in Austria (47 percent) or in other EU countries (25 percent). The majority does not live in a permanent relationship (65 percent) and has no children (57 percent). Their educational background is surprisingly poor: 54 percent of the suspects failed to graduate from higher secondary school, and only 20 percent have regular work.

Even more fascinating is a typology established on the basis of demographic features: the study differentiates between three categories of cybercriminals.

[1] Edith Huber, Bettina Pospisil, eds., *Die Cyber-Kriminellen in Wien,* Edition Donau-Universität Krems 2018; download at www.researchgate.net/publication/323486485_Die_Cyber-Kriminellen_in_Wien or as Kindle edition from Amazon.

[2] See https://www.kiras.at/#category-filter:path=default.

[3] Computer Emergency Response Team.

Typ 1: Der Businessman

Dieser Typ umfasst 31 Prozent der Fälle und zeichnet sich dadurch aus, dass er zu 100 Prozent aus Männern besteht und aktuell der gefährlichste Tätertyp ist, denn es handelt sich um höher qualifizierte und strategisch denkende Menschen. Gleichzeitig sind überdurchschnittlich viele berufstätig – nur 22 Prozent sind nicht beschäftigt. Das Alter des »Businessman« liegt im Durchschnitt bei knapp 35 Jahren. Außerdem finden sich bei diesem Typ 100 Prozent der Fälle, die sich durch ein komplexeres Vorgehen beim Begehen des Cyberdelikts auszeichnen. Die meisten Personen dieses Typs haben keine Vorstrafen und sind charakteristischerweise Einzeltäter.

Typ 2: Die Hausfrau

Die zweite Gruppe umfasst 18 Prozent der Fälle und besteht zu 100 Prozent aus Frauen – mit einem Durchschnittsalter von rund 32 Jahren. Der Bildungsstatus ist unterschiedlich: Während die Hälfte eine geringe Bildung hat, weisen 44 Prozent Maturaniveau auf. Der Großteil dieser Personen ist nicht regulär beschäftigt – nur 19 Prozent gehen einer regulären Beschäftigung nach. Die »Hausfrauen« haben mit hoher Wahrscheinlichkeit (69 Prozent) keine Vorstrafe; sie verübten das Delikt zu 56 Prozent als Einzeltäterinnen.

Typ 3: Der Perspektivlose

Der dritte Typ von Cyberkriminellem umfasst den größten Teil (51 Prozent) der Fälle und besteht ausschließlich aus Männern. Diese haben zu 100 Prozent eine geringe Bildung und keine reguläre Beschäftigung. Das Alter des »Perspektivlosen« liegt im Schnitt bei knapp 30 Jahren. Diese Gruppe umfasst auch 80 Prozent der angeklagten Jugendlichen unter 20 Jahren. 57 Prozent haben Vorstrafen; die Delikte wurden zu 73 Prozent von Mitgliedern einer Gruppe begangen. Personen mit schwierigem familiärem Hintergrund machen einen hohen Anteil dieser Kategorie aus.

Welche Motive stehen im Vordergrund? Bei rund zwei Dritteln der Fälle sind es vorwiegend extrinsische Motive – vor allem finanzieller Gewinn. Die Ursachen sind in vielen Fällen Geldmangel wegen Erwerbslosigkeit, aber auch mit Sucht gekoppelte Beschaffungskriminalität. Es gibt aber auch viele Fälle, in denen intrinsische Motive ausschlaggebend sind – und da wiederum allen voran private Motive wie Rache oder mutwillige Schädigung. In nur wenigen Fällen stehen indes das auf Anerkennung erpichte Beweisen von Fähigkeiten, »Hacktivismus« oder das Austesten von Möglichkeiten im Vordergrund. ×

Type 1: Businessman

31 percent of the cases can be allotted to this category, which stands out for the fact that it comprises exclusively males and that it currently represents the most dangerous type of perpetrator, including persons that are better qualified and strategic thinkers. The average "businessman" is barely 35 years old. Moreover, in this category 100 percent of the cases are characterized by the employment of more complex strategies for the commitment of cybercrimes. Most persons of this type have no criminal record and are characteristically lone perpetrators.

Type 2: Housewife

18 percent of the cases can be allotted to the second group, which consists solely of women—their average age being 32 years. Their educational background differs: whereas about half of them are poorly educated, 44 percent have graduated from higher secondary school. The majority in this category has no regular employment—only 19 percent work regularly. "Housewives" most likely have no criminal record (69 percent), with 56 percent acting as lone perpetrators when committing their offenses.

Type 3: Hopeless case

The majority of cybercriminals (51 percent) can be assigned to the third type and comprises exclusively men. 100 percent have poor education and no regular work. The average age of the "hopeless case" type is barely 30 years. This group also includes 80 percent of accused adolescents under 20 years of age. 57 percent of the culprits have a police record, and 73 percent of the offenses were committed by members of a group. Persons with a difficult family background make up a major share of this category.

And what are the most frequent motives? In roughly two thirds of all cases it is primarily extrinsic motives, above all financial gain. In many cases the causes are lack of money due to joblessness and addiction, which is linked to the need to obtain drugs through the commitment of crimes. But there are also numerous cases in which intrinsic motives are crucial—most of all private motives like revenge or willful damage. The wish to gain recognition by proving one's abilities, "hacktivism," or checking out what is possible only plays a role in few cases. ×

Hemma Mayrhofer im Gespräch

»Weder Freiheit noch Sicherheit sind gesellschaftlich gleich verteilte Güter«

Soziologin und wissenschaftliche Geschäftsführerin am Institut für Rechts- und Kriminalsoziologie in Wien, Lehrbeauftragte am Institut für Soziologie der Universität Wien, Redaktionsmitglied der *Österreichischen Zeitschrift für Soziologie* (özs). Forschung u. a. zu den Schwerpunkten soziale Inklusion und Exklusion, soziale Kontrolle und soziale Arbeit, Rechtssoziologie, Gewalt und totale Institutionen.

Hemma Mayrhofer, Forscherin am Institut für Rechts- und Kriminalsoziologie in Wien, über das Sicherheitsempfinden der Menschen, die Rolle von Prävention und das Verhältnis zwischen Freiheit und Sicherheit.

Das Institut für Rechts- und Kriminalsoziologie beschäftigt sich sehr intensiv mit gesellschaftlicher Sicherheit. Wie viel Sicherheit braucht der Mensch?

Hemma Mayrhofer: Das ist sehr unterschiedlich und kommt auf viele Faktoren an. Bemerkenswert ist etwa, dass sich manche Bevölkerungsgruppen, die ein hohes Risiko haben, Opfer einer Straftat zu werden, weniger fürchten. Ältere Menschen hingegen sind real gar nicht so gefährdet, zeigen aber Studien zufolge mehr Furcht vor Kriminalität. Dunkle Straßen und Plätze lösen Unsicherheitsgefühle aus, während die eigene Wohnung als besonders sicher erlebt wird. Dabei ist das Zuhause allen Studien zufolge ein besonders unsicherer Ort, nämlich vor allem durch häusliche Gewalt. Das deutet darauf hin, dass nicht die tatsächliche Wahrscheinlichkeit, Opfer zu werden, das Sicherheitsgefühl bestimmt. Vielmehr sind dafür andere Faktoren wie etwa die subjektiv wahrgenommene eigene Verletzlichkeit von Bedeutung. Die Soziologie fasst den Sicherheitsbegriff ja viel weiter, und gesellschaftliche Sicherheit schließt viel mehr als die Sicherheit vor Kriminalität ein. Wir wissen, dass die Angst vor Jobverlust und sozialem Abstieg eine große Rolle dabei spielt, wie sicher sich jemand fühlt. In der Diskussion darum, wie viel Sicherheit Menschen brauchen, muss also immer auch die Frage gestellt werden, von welcher Sicherheit überhaupt gesprochen wird.

An interview with Hemma Mayrhofer

“Neither freedom nor security are assets that are equally distributed in society”

Sociologist and scientific manager at the Institute for the Sociology of Law and Criminology in Vienna, teaching at the Department of Sociology at the University of Vienna and on the editorial board of the periodical *Österreichische Zeitschrift für Soziologie* (özs). Her research activities focus, among other things, on social inclusion and exclusion, social control and social work, the sociology of law, violence, and total institutions.

Hemma Mayrhofer, researcher at the Institute for the Sociology of Law and Criminology in Vienna, on the human sense of security, the role of prevention, and the relationship between freedom and security.

The Institute for the Sociology of Law and Criminology intensively deals with security in society. How much security do people need?

Hemma Mayrhofer: This can be very different and depends on multiple factors. It is remarkable, for example, that some population groups, namely those with a higher risk of falling victim to a crime, display less fear. Elderly people, on the other hand, are not really that much imperiled, but according to studies are more afraid of crime. Dark streets and squares trigger feelings of insecurity, while one’s own apartment is perceived as a particularly safe place. And yet all of the studies have found that one’s home, due to domestic violence, is actually a particularly unsafe place. This indicates that one’s sense of security does not correlate with the actual probability of becoming a victim. Rather, other factors are relevant, including one’s own subjectively perceived vulnerability. Sociology has a much broader notion of security, and security in society encompasses much more than security against crime. We know that the fear of losing one’s job or of social decline plays an important role in how safe or secure one feels. In discussions about how much security people need we also always have to define what sort of security we are talking about.

Die Kriminalität geht seit einigen Jahren stetig zurück, trotzdem fühlen sich die Menschen zunehmend unsicher. Was sind Ihrer Meinung nach die Ursachen dafür?

HM: Wir wissen aus nationalen und internationalen Studien, dass objektive Sicherheitslage und subjektives Sicherheitsgefühl nur bedingt zusammenhängen. Das Sicherheitsgefühl hat relativ wenig damit zu tun, wie hoch etwa die Kriminalitätsrate ist, die genau genommen lediglich eine Anzeigenstatistik darstellt. Mein Kollege Walter Fuchs hat etwa die Kriminalitätsfurcht in verschiedenen Wiener Gemeindebezirken untersucht. Die Ergebnisse deuten darauf hin, dass ganz andere Faktoren das Sicherheitsgefühl wesentlich beeinflussen, etwa Alter, Bildung oder wahrgenommene Lebenschancen. Entwickelte Wohlfahrtsstaaten gewähren ihren Bürgerinnen und Bürgern überdies ein gewisses Maß an sozialer Sicherheit. Dies ist auch ein wichtiger Baustein für gefühlte Absicherung und ein hohes kriminalitätsbezogenes Sicherheitsempfinden, und zwar interessanterweise relativ unabhängig vom »objektivierbaren« Ausmaß an Kriminalität. Es gibt auch Studien, die Zusammenhänge zwischen einem niedrigeren Sicherheitsgefühl und dem Konsum von Medien, die häufig Kriminalität thematisieren, belegen. Schwere Straftaten sind zudem medial besonders präsent, wodurch sich die Wahrnehmung einstellt, dass diese wesentlich öfter passieren, als es der Realität entspricht. Solche Effekte werden durch die vielzitierten »Echokammern« in sozialen Medien noch verstärkt.

Man hat den Eindruck, dass Gesellschaft und Politik derzeit sehr stark auf Sicherheit fokussiert sind. Teilen Sie diese Einschätzung? Und falls ja: Warum ist das so?

HM: Der Trend, dass Sicherheit ein ganz zentrales Thema nationaler Politik ist, lässt sich europaweit und darüber hinaus schon länger beobachten. Man spricht auch von »Securitization«, also »Versicherheitlichung« von Themen und Angelegenheiten, die bislang vor allem als ein Thema der Sozialpolitik, der Jugendpolitik oder der sozialen Integration diskutiert wurden. Der Verweis auf Sicherheit ist zu einem wesentlichen Legitimationsmuster im politischen Diskurs geworden. Warum das so ist, darauf gibt es unterschiedliche Antworten. Eine solche Antwort hat etwa David Garland, ein bedeutender Kriminalsoziologe

Although the crime rate has been declining steadily for several years now, people feel increasingly insecure. What, in your opinion, are the reasons for this?

HM: We know from national and international studies that the objective security situation and the subjective perception of security correspond with each other only to a limited extent. People's sense of security has relatively little to do with how high the crime rate, which, strictly speaking, only represents a statistic based on police reports, really is. My colleague Walter Fuchs, for example, has analyzed the fear of crime in a number of Viennese districts. His findings reveal that totally different types of factors strongly influence one's sense of security, such as age, educational background, or the perception of chances in life. In addition, developed welfare states offer their citizens a certain extent of social security. This is also an important building block for developing a feeling of safety and a heightened awareness of security with regard to crime, which is interestingly enough relatively independent of the "objectifiable" dimension of crime. We also know studies evidencing a relationship between a low sense of security and the consumption of media frequently dealing with criminal themes. Moreover, serious crimes receive frequent coverage in the media so that one feels that they happen much more often than in reality. Such effects are aggravated by the much-quoted "echo chambers" in the social media.

One has the impression that society and politics are currently extremely focused on security.
Do you agree? And if yes: why is that so?

HM: The tendency that security is an absolutely central theme in national politics can be perceived throughout Europe and has been observed over a longer period of time now. One also speaks of the "securitization" of themes and matters that have previously mostly been discussed as themes of social policy, youth policy, or social integration. Making reference to security has become a basic pattern of legitimation in political discourse. There are various answers to the question why this is the case. David Garland, one of today's leading criminal sociologists,

der Gegenwart, ausgearbeitet. Er beobachtet am Beispiel der USA und Großbritanniens einen grundsätzlichen kulturellen Umbruch im Umgang mit Kriminalität weg von der Orientierung an Resozialisierung straffällig gewordener Personen hin zu einer rigiden Kontrollkultur. Stark verkürzt zusammengefasst steht dieser Umbruch mit der Erosion des Wohlfahrtsstaates im Zusammenhang, mit der steigende soziale Ungleichheit einhergeht. Sozioökonomische Verunsicherung wird als individuelle Bedrohung erlebt und erhöht eine generalisierte Kriminalitätsangst, die wiederum populistisch genutzt, verstärkt und mittels Sicherheitspolitik bearbeitet wird.

Welche Folgen hat das?

HM: Mit diesen Umbrüchen geht auch eine starke Präventionsorientierung einher. Mit der Prävention ist das aber so eine Sache, sie scheint auf den ersten Blick so unzweifelhaft gut und erstrebenswert zu sein, erweist sich aber bei näherem Hinsehen als janusköpfig. Denn man will ja möglichen Gefährdungen vorbeugen, die noch gar nicht eingetreten sind und vielleicht auch ohne Präventionsmaßnahme niemals eintreten würden. Annahmen über Gefährdungen stellen Prognosen über eine ungewisse Zukunft dar. Sie bieten entsprechend große Ermessensspielräume und Prognoseunsicherheiten. Zugleich lässt sich die Wirksamkeit präventiver Sicherheitsmaßnahmen empirisch kaum zuverlässig feststellen, da die Wirkzusammenhänge in solch nichtlinearen, multikausalen und pfadabhängigen Interventionsfeldern nur schwer bis gar nicht zuverlässig nachweisbar sind. Mit dem Argument der Gefahrenprävention lassen sich die Grenzen der legitimierbaren Einschränkungen von Freiheit ausweiten, deshalb benötigt es gerade hier besondere Aufmerksamkeit. Damit will ich keinesfalls sagen, dass Prävention generell zu nichts gut oder gar gefährlich sei – ganz im Gegenteil. Man sollte nur genau hinschauen, welche konkreten Rechte und Freiheiten man für ein vages Sicherheitsversprechen möglicherweise verliert.

Geht Sicherheit auf Kosten der Freiheit? Anders gefragt: Sind Sicherheit und Freiheit Gegensätze – oder bedingen sie einander?

HM: Im österreichischen Verfassungsgesetz über den Schutz der persönlichen Freiheit ist an oberster Stelle festgehalten: »Jedermann hat das Recht auf Freiheit und

has elaborated on one of them. Using the United States and Great Britain as examples, he can observe a fundamental shift in how crime is dealt with, from an orientation toward the social reintegration of delinquents to a rigid control culture. Putting it in a nutshell, this shift or rupture has to do with the erosion of the welfare state, which goes hand in hand with growing social inequality. Socioeconomic insecurity is perceived as an individual threat and contributes to a generalized fear of crime, which is taken advantage of by populism as it is intensified and then attended to by security policy.

What are the consequences?

HM: These ruptures are also accompanied by a strong focus on prevention. But prevention is not as simple as it looks. At first sight there seems to be no doubt that prevention is a good and desirable thing. But when we take a closer look, it turns out to be Janus-faced. For one seeks to prevent possible dangers that have not yet happened and probably never will, even if we take no prevention measures at all. Assumptions made about threats are forecasts about an uncertain future. They come along with accordingly large margins of discretion and forecast uncertainties. At the same time, the efficiency of preventive security measures is difficult to ascertain empirically, as cause-effect correlations in such nonlinear, multicausal, and path-dependent fields of intervention can only be determined with difficulty and little reliability. As the argument of threat prevention permits the limits of a legitimized restriction of freedoms to be pushed, one has to be particularly vigilant here. The least I wish to say is that prevention is generally no good or even dangerous—quite the opposite is true. But one should be aware of the concrete rights and freedoms one will possibly lose in return for a vague promise of security.

Is security bought at the expense of freedom? Or, to put it differently: are security and freedom antipodes—or are they mutually dependent?

HM: In Austrian constitutional law, the passage about the protection of personal freedom begins as follows: "Everyone has the right to freedom and security."

Sicherheit.« Sicherheit soll für alle Menschen Ermöglichungsbedingungen für persönliche Freiheit gewährleisten, so würde ich es in Anlehnung an die rechtsphilosophische Tradition von Locke und Kant formulieren. Und ich muss hinzufügen, dass dies nicht nur staatliche und Rechtssicherheit oder die Sicherheit vor Gewalt meint, sondern auch soziale und materielle Sicherheit als unabdingbare Basis für persönliche Entfaltung. Damit ist Sicherheit kein Selbstzweck. Wer Sicherheit – was auch immer damit dann wirklich gemeint ist – über alles stellt, unterliegt somit einer klassischen Zweck-Mittel-Verkehrung. Daher sollten diese beiden Begriffe auch nicht als Gegensatz konstruiert werden, auch wenn sie mitunter in ein Spannungsverhältnis zueinander geraten mögen. Man darf zudem nicht vergessen, dass wir auch vor überbordenden Sicherheitsinteressen des Staates und der Strafverfolgungsbehörden geschützt werden müssen. Die Freiheit vor staatlichen Eingriffen ist historisch erkämpft und stets prekär, weshalb sie in modernen Verfassungsstaaten als subjektives und klagbares Recht ausgestaltet wird. Weder Freiheit noch Sicherheit sind gesellschaftlich gleich verteilte Güter. Deshalb gilt es auch immer zu fragen: Welche und wessen Freiheit wird zugunsten welcher und zugunsten von wessen Sicherheitsinteressen eingeschränkt?

Als Wissenschaftlerin beschäftigen Sie sich viel mit dem Umgang von Jugendlichen mit digitalen Medien. Sehen Sie einen Trend, dass sich Jugendliche der Risiken und Gefahren der digitalen Welt klarer bewusst werden? Und wo sollte hier angesetzt werden, um die Situation zu verbessern?

HM: Ich beschäftigte mich genau genommen damit, wie Offene Jugendarbeit Jugendliche dabei unterstützen kann, mit den Herausforderungen und Risiken in einer digitalisierten und mediatisierten Lebenswelt zurechtzukommen. Zu diesen Risiken zählt unter anderem, dass Jugendliche im Netz leicht mit gewaltverherrlichenden Inhalten in Berührung kommen. Sie sind auch in besonderer Weise Zielgruppe extremistischer Internetpropaganda. Grundsätzlich ist es wichtig, hier auf verschiedenen Ebenen anzusetzen. Zum einen muss die Verbreitung solcher Propaganda eingeschränkt werden. Da ist in den letzten Jahren viel passiert, die großen Konzerne wie Facebook und Google wurden stärker in die Pflicht genommen. Zum

Security shall guarantee conditions that will enable all people to enjoy personal freedoms—this is how I would put it, following the tradition of Locke's and Kant's legal philosophy. And I should add that this encompasses not only the security of a state, legal security, or security against violence, but also social and material security as an indispensable basis for personal development. Thus, security is not an end in itself. Those placing security—or whatever it really means then—above everything else have succumbed to the classic confusion between means and ends. Therefore, these two terms should not be construed as antipodes, even if their relationship can sometimes be conflicting. Moreover, one should not forget that we also have to be protected from an excessive interest of the state and criminal prosecution. The freedom from government intervention is a historic and hard-won asset and always precarious, which is why in modern constitutional states it is perceived as a subjective and enforceable right. Neither freedom nor security are assets that are equally distributed in society. This is why it is always important to find out which and whose freedom will be restricted in favor of which and whose security interests.

As a scientist you deal a lot with young people's use of the digital media. Can you notice a trend that youngsters are becoming more and more aware of the risks and dangers of the digital world? And where should one actually begin to improve the situation?

HM: Strictly speaking, I deal with how open youth work can support young people in coping with the challenges and risks in a digitized, media-driven environment. These risks include, among others, that youngsters can easily encounter violence-glorifying content on the web. They are also, in a very special way, a target group of extremist Internet propaganda. It is essentially important to take action on different levels here. First, the dissemination of such propaganda has to be restricted. Many important steps have been taken in this direction in recent years, and such big corporations as Facebook and Google have been obligated to accept more responsibility in this respect. On the other hand, meaningful alternatives to the extremist offering are urgently needed. If youngsters

anderen braucht es Alternativen zu extremistischen Sinnangeboten. Wenn ein junger Mensch im Internet Rat sucht und sich beispielsweise über die richtige Lebensweise eines jungen Muslims im Westen informieren will, darf er nicht von salafistischen Predigern abgeholt werden. Es braucht etwa sogenannte alternative Narrative, und zwar mehr noch als die Dekonstruktion der Narrative der Extremisten. Hierzu forscht derzeit etwa meine Kollegin Veronika Hofinger. Und natürlich gilt es digitale Medienkompetenz zu fördern, also Kompetenz im Umgang mit dem Internet und mit sozialen Medien. Hier sind alle Sozialisationsinstanzen gefragt: die Eltern, die Schule und etwa auch außerschulische Jugendarbeit.

Einerseits hat der Staat die Aufgabe, die Freiheit und Sicherheit der Menschen zu garantieren. Andererseits ist ein Teil des Unbehagens der Menschen hinsichtlich Freiheit und Sicherheit auch die (zunehmende) Überwachung durch den Staat. Wie kann der Staat, wie kann die Gesellschaft diesen Widerspruch lösen?

HM: Dieser Widerspruch wird sich nicht völlig auflösen lassen. Wichtig ist, gesellschaftliche Errungenschaften wie Grundrechte und Minderheitenrechte nicht zugunsten von überzogenen und faktisch völlig unrealistischen Sicherheitsfantasien auszuhebeln. Wer sich stark an Sicherheit orientiert, wird auch sein Bewusstsein für Risiken erweitern und immer neue Quellen der Unsicherheit entdecken. Insofern plädiere ich dafür, genau hinzuschauen, um welche Unsicherheit oder Verunsicherung es tatsächlich geht, auf die mit sicherheitspolitischen Maßnahmen wie Überwachung reagiert wird oder werden soll. Und ich will auch nochmals die Tücken präventiver Sicherheitspolitik hervorheben: Freiheit präventiv einzuschränken, um Sicherheit zu versprechen, ist selbst ein höchst gefährliches Unterfangen und muss wohlüberlegt sein. ×

seek information about how young Muslims should live in the West and ask the Internet for advice, it cannot be that they are picked up by Salafist preachers. What is needed is a so-called alternative narrative, even more so than the deconstruction of the narrative of extremists. My colleague Veronika Hofinger is doing research in this field. And, of course, it is essential to improve digital media competence, i.e., competence in dealing with the Internet and social media. All agents of socialization are called upon to contribute here: parents, schools, and extracurricular youth work.

On the one hand, it is the state's duty to guarantee people's freedom and security. On the other hand, part of the people's disquietude with regard to freedom and security has to do with (intensified) surveillance through the state. How can the government and society solve this conflict?

HM: It will not be possible to disperse this contradiction completely. It is important that social achievements such as fundamental rights and minority rights will not be annulled in favor of exaggerated security fantasies that are, in fact, totally unrealistic. Those obsessively concentrating on security will nurture their alertness to risks and discover ever-new sources of insecurity. In this respect, I recommend taking a closer look at the actual insecurities or uncertainties that are or should be fought here with such security-political measures as surveillance. And I would like to point out once more the pitfalls of a preventive security policy: restricting freedom preventively so as to be able to promise security is a highly dangerous undertaking that should be carefully deliberated. ×

Wer sich um mehr Cybersicherheit bemüht

In Österreich hat sich in jüngster Zeit eine Vielzahl von Akteuren herausgebildet, die sich des Themas Cybersicherheit annehmen. Ein Versuch, etwas Klarheit in ein kaum durchschaubares Gestrüpp von beteiligten Institutionen zu bringen.

Die Grundlage vieler in Österreich entfalteter Aktivitäten in Sachen Cybersicherheit ist die Österreichische Strategie für Cybersicherheit (öscs), die im Jahr 2013 gemeinsam von Bundeskanzleramt, Innen-, Außen- und Verteidigungsministerium beschlossen wurde (und zurzeit evaluiert und überarbeitet wird). In der öscs werden systematisch Prinzipien, strategische Ziele, Handlungsfelder und Maßnahmen aufgelistet. Die Initiatoren beschreiben die Strategie als ein »umfassendes und proaktives Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum unter Gewährleistung der Menschenrechte«. Die öscs habe zum Ziel, die Sicherheit und Widerstandskraft der österreichischen Infrastrukturen und Leistungen im Cyberraum zu verbessern. Vor allem aber solle sie auch dazu beitragen, in der österreichischen Gesellschaft Bewusstsein über und Vertrauen in die digitale Sicherheit zu schaffen. Als grundlegende Prinzipien wurden definiert:

- Rechtsstaatlichkeit: Das staatliche Handeln im Bereich Cybersicherheit muss den hohen rechtsstaatlichen Standards der österreichischen Verwaltung entsprechen und die Einhaltung der Menschenrechte, vor allem der Privatsphäre und des Datenschutzes sowie der Meinungsäußerungsfreiheit und des Rechts auf Information, gewährleisten.
- Subsidiarität: Cybersicherheit ist ein Rechtsgut. Der Staat bekennt sich daher zu einem hohen Engagement zum Schutz dieses Rechtsguts, kann und soll aber nicht die alleinige Verantwortung für den Schutz des Cyberraums übernehmen. Die Eigentümer und Betreiber von Informations- und Kommunikationstechnologien sind in erster Linie für den Schutz ihrer Systeme selbst verantwortlich. Dabei gilt der Grundsatz »Selbstverpflichtung wenn möglich, Regulierung wenn notwendig«.
- Selbstregulierung: Grundsätzlich sollte angestrebt werden, über Eigeninitiativen das Schutzniveau durch Codes of Conduct, Standardisierungen und Zertifizierungen zu erhöhen. Es bleibt aber Aufgabe des Staates, den Ordnungsrahmen für den Schutz der Informations- und

Those Seeing to More Cybersecurity

In Austria, numerous players devoting themselves to the subject of cybersecurity have recently appeared on the scene. This is an attempt to bring some clarity into the thicket of institutions involved, which has become more and more impenetrable.

For many activities going on in the field of cybersecurity in Austria, the Austrian Cybersecurity Strategy (ASCS), adopted in 2013 by the Federal Chancellery and the Federal Ministries of the Interior, the Exterior, and Defense (and currently being evaluated and revised), has provided a pertinent basis. The ASCS systematically lists principles, strategic goals, fields of actions, and measures to be taken. The initiators describe their strategy as a "comprehensive and proactive concept for the protection of cyberspace and people in virtual space while guaranteeing the observation of human rights." As they say, it is the goal of the ASCS to improve the security and resilience of Austrian infrastructures and their performance in cyberspace. Above all, it should also contribute to creating an awareness of and trust in digital security amongst the Austrian population. Its fundamental principles have been defined as follows:

- The rule of law: Governance in the area of cybersecurity has to meet the Austrian administration's high standards of the rule of law and guarantee compliance with human rights, in particular privacy and data protection, as well as freedom of expression and the right to information.
- Subsidiarity: Cybersecurity is a legal asset. Therefore, the government pledges its strong commitment to the protection of this legal asset, although it cannot and should not assume sole responsibility for the protection of cyberspace. It is primarily upon the owners and operators of information and communication technology to protect their own systems. Therefore the following principle shall apply: "Self-commitment if possible, regulation if necessary."
- Self-regulation: Efforts should generally be made to increase the level of protection through the actors' own initiatives through codes of conduct, standardization, and certification. However, it remains the task of the government to provide the regulatory framework for protecting the information and communication

Kommunikationstechnologien von Unternehmen und Privaten zu schaffen und die Selbstregulierung im privaten Bereich zu begleiten.
- Verhältnismäßigkeit: Die Maßnahmen und Kosten zur Erhöhung des Schutzniveaus müssen in einem ausgeglichenen Verhältnis zum jeweiligen Risiko und zu den Möglichkeiten der Gefahrenminderung stehen.

Eine zentrale Einrichtung in diesem Zusammenhang ist die **Steuerungsgruppe Cybersicherheit,** die unter Federführung des Bundeskanzleramtes auf politisch-strategischer Ebene die Maßnahmen für Cybersicherheit koordiniert, die Umsetzung der ÖSCS beobachtet und begleitet, einen jährlichen Bericht zur Cybersicherheit erstellt und die Bundesregierung in Angelegenheiten der Cybersicherheit berät. Die Steuerungsgruppe setzt sich u. a. aus den Verbindungspersonen zum Nationalen Sicherheitsrat und Cybersicherheitsexperten der im Nationalen Sicherheitsrat vertretenen Ressorts zusammen.

Eine zentrale Stelle zur Erhöhung der Cybersicherheit ist der **Innere Kreis der operativen Koordinierungsstrukturen** (IKDOK), welcher der Koordination auf operativer Ebene dient. Diese Einheit, die 2016 den Betrieb aufgenommen hat, erstellt periodische und anlassbezogene operative Lagebilder für Cybersicherheit, erarbeitet im Anlassfall Maßnahmen und unterstützt und koordiniert gesamtstaatliche Notfallmaßnahmen im Rahmen des Cyberkrisenmanagements. Federführend im IKDOK sind das **Cyber Security Center** (CSC) im Bundesministerium für Inneres sowie das **Cyberverteidigungszentrum** (C_yVZ) im Bundesministerium für Landesverteidigung. Überdies vertreten sind das **Cyber Crime Competence Center** (C4) im Innenministerium, das **Heeresnachrichtenamt,** das **Kommando Führungsunterstützung und Cyber Defence** ($K_{do}F_{ü}U\&CD$) des Österreichischen Bundesheeres samt **Military Computer Emergency Readiness Team** ($_{mil}$CERT), das **Government Computer Emergency Response Team** (G_{ov}CERT) im Bundeskanzleramt sowie das **Außenministerium.**

Das **Cyber Security Center** (CSC) im Innenministerium, das seit Ende des Jahres 2017 den Vollbetrieb aufgenommen hat,
- ist die Behörde für Netz- und Informationssicherheit,
- ist für präventive Maßnahmen im Infrastrukturbereich und den Schutz kritischer Infrastrukturen verantwortlich,
- übernimmt die Koordination von Absicherungsmaßnahmen und des Cyberkrisenmanagements,
- verfügt über technische Kompetenz und fungiert als Ansprechpartner.

Das CSC ist vor allem als Aufsichtsbehörde für die Umsetzung des Netz- und Informationssystem-Sicherheitsgesetzes (NIS-Gesetz) zuständig. Dieses Gesetz basiert auf der NIS-Richtlinie, die im Jahr 2016 von der EU festgeschrieben und per 1. Jänner 2019 in Österreich umgesetzt wurde. Das NIS-Gesetz

technology of corporations and private persons, and to support self-regulation in the private sphere.
- Proportionality: Measures to increase the level of protection and the respective costs have to be proportionate to the respective risk and to the possibilities of limiting these threats.

A key instrument in this context is the **Cybersecurity Steering Group,** which under the auspices of the Federal Chancellery coordinates measures in favor of cybersecurity on a political and strategic level; monitors and supports the implementation of the ÖSCS; compiles annual reports on cybersecurity; and advises the Federal Government in matters of cybersecurity. This steering group consists, among others, of liaison officers acting as links to the National Security Council and of cybersecurity experts from the various departments represented in the National Security Council.

A central facility for the improvement of cybersecurity is the **Inner Circle of Operative Coordination Structures** (ICOOC), which is in charge of coordination on an operative level. This unit, which took up its work in 2016, issues periodic and event-driven operative situation reports for cybersecurity; develops concrete measures on specific occasions; and supports and coordinates general national emergency measures within the framework of cybercrisis management. Primary stakeholders in the ICOOC are the **Cybersecurity Center** (CSC) in the Federal Ministry of the Interior and the **Cyberdefense Center** (C_yDC) in the Federal Ministry of Defense. In addition, further platforms represented in this unit are the Interior Ministry's **Cybercrime Competence Center** (C4), the **Armed Forces' Intelligence Agency**, the Austrian Armed Forces' **Leadership Support and Cyberdefense Commando** (L_{ead}S&CDC) and its **Military Computer Emergency Readiness Team** ($_{mil}$CERT), the Federal Chancellery's **Government Computer Emergency Response Team** (G_{ov}CERT), and the **Federal Ministry of the Exterior**.

The **Cybersecurity Center** (CSC) in the Ministry of the Interior, which began full operation in late 2017,
- is the public agency for network and information security;
- is responsible for preventive measures in the field of infrastructure and for the protection of critical infrastructures;
- is in charge of the coordination of safeguarding measures and cybercrisis management;
- has technological competencies and functions as a contact partner.

As a supervisory authority, the CSC is primarily in charge of the implementation of the Network and Information Security Act (NIS Act). It is based on the NIS Directive, which was codified by the EU

schreibt Betreibern von kritischer Infrastruktur (Kraftwerken, Energienetzen, IKT-Diensten, Wasserversorgungseinrichtungen, Eisenbahnunternehmen, Finanzdienstleistern etc.) verbindliche Mindeststandards in Sachen Cybersicherheit vor und verpflichtet sie, schwere Sicherheitsvorfälle an zentrale Stellen zu melden. Dadurch soll zum einen – erstmals – die Erstellung vollständiger Lagebilder ermöglicht werden. Zum anderen können von einer etwaigen Angriffswelle noch nicht betroffene Organisationen rasch gewarnt und auf mögliche Gegenmaßnahmen vorbereitet werden.

Das **Cyber Crime Competence Center** (C4) im Innenministerium ist die nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung von Cyberkriminalität. Das Zentrum setzt sich aus Spezialisten aus den Bereichen Ermittlung, Forensik und Technik zusammen. Die Cybercrime-Meldestelle des C4 ist zum einen die Kontaktstelle zur Bevölkerung – dadurch können frühzeitig neue Phänomene erkannt werden. Zum anderen ist sie auch die Schnittstelle zum CSC und internationale Kontaktstelle in Cybercrime-Angelegenheiten. Eine weitere wichtige Aufgabe des C4 ist die einer Ansprechstelle für alle Polizeidienststellen im Zusammenhang mit Cybercrime-Vorfällen. Im C4 wird beispielsweise an zentraler Stelle gegen Ransomware (Erpressung durch Verschlüsselungssoftware) ermittelt und die internationale Zusammenarbeit koordiniert. Ein weiterer Schwerpunkt sind durch die automatische maschinengestützte Kommunikation (Internet der Dinge) aufgeworfene Fragen.

Das Verteidigungsministerium bzw. das Österreichische Bundesheer betreibt einige Einrichtungen, die sich mit Cybersicherheit befassen. Das im Abwehramt angesiedelte **Cyberverteidigungszentrum** (CyVZ) ist u. a. für die Erstellung aktueller Lagebilder von Cyberbedrohungen zuständig und bereitet aktive Mittel für Verteidigungsmaßnahmen vor. Im **Heeresnachrichtenamt** werden besonders internationale Entwicklungen beobachtet; die Informationen fließen ebenfalls in Lagebilder ein. Im **Kommando Führungsunterstützung und Cyber Defence** (KdoFüU&CD) im Bundesheer, das 2017 eingerichtet wurde, verbinden sich alle präventiven, operativen und reaktiven Kompetenzen zur Abwehr von Bedrohungen aus dem Cyberraum, so auch die des **milCERT.**

Zentral für die Umsetzung der Cyberverteidigung sind sogenannte **Computer Emergency Response Teams** (CERTs). Diese Teams von Cybersicherheitsexperten werden bei akuten Sicherheitsbedrohungen und Ereignissen aktiv, führen vorbeugende Maßnahmen wie etwa Früherkennungsschritte durch und unterstützen auf Anfrage unterschiedlichste Organisationen. Es gibt in Österreich eine Reihe von Computernotfallteams für bestimmte Institutionen bzw. Branchen; im CERT-Verbund Österreich sind aktuell 13 CERTs vertreten. **GovCERT** heißt das im Bundeskanzleramt angesiedelte nationale CERT für die öffentliche Verwaltung; es schützt gemeinsam mit der Organisation **CERT.at** u. a. die Ministerien vor Cyberangriffen. Überdies fungiert das GovCERT als Anknüpfungspunkt für euro-

in 2016 and implemented in Austria on January 1, 2019. The NIS Act stipulates that operators of critical infrastructure (power plants, energy supply networks, ICT services, water supply facilities, railroad companies, financial services, etc.) have to implement mandatory minimum standards in terms of cybersecurity and obliges them to report serious security incidents to central agencies. On the one hand, this makes it possible for the first time to compile comprehensive situation reports; on the other hand, organizations not yet hit by a possible attack wave can be warned at an early stage and prepared to take pertinent countermeasures.

The **Cybercrime Competence Center** (C4) in the Federal Ministry of the Interior is the national and international coordination and reporting point for the combat of cybercrime. This center is composed of experts from the spheres of criminal investigation, forensic science, and technology. On the one hand, the C4's cybercrime reporting unit is the agency to be contacted by the population so that new phenomena can be identified early on. On the other hand, it also acts as a link to the CSC and is the international contact point in matters of cybercrime. Another chief task of the C4 is that it functions as a reporting point for all police stations when it comes to cybercrime incidents. For example, the C4 is the central agency to investigate in cases of ransomware (blackmailing involving encrypted software) and to coordinate international cooperation. Another focus is on problems associated with automated machine-based communication (Internet of things).

The Federal Ministry of Defense and the Austrian Armed Forces run several agencies concerned with cybersecurity. The **Cyberdefense Center** (CyDC), which is affiliated with the Austrian army's Defense Agency, is, among other things, responsible for compiling updated situation reports about cyberthreats and develops active instruments to be employed as defense measures. The **Armed Forces' Intelligence Agency** is mostly concerned with observing international developments; the information gained is likewise fed into the situation reports. At the Armed Forces' **Leadership Support and Cyberdefense Commando** (LeadS&CDC), all the preventive, operative, and responsive competencies for warding off threats from cyberspace converge, including those of the **milCERT.**

The so-called **Computer Emergency Response Teams** (CERTs) are instrumental for the implementation of cyberdefense. These teams of cybersecurity experts take action in acute incidents involving security threats; they take such preventive measures as early recognition assessment and, upon request, provide assistance for diverse organizations. In Austria there are several computer emergency teams for specific organizations and sectors; currently, the CERT network consists of 13 CERTs. **GovCERT** is the name of the national CERT attached

päische und internationale Organisationen wie etwa die **European GovCERT Group** oder die **Central European Cyber Security Platform.** Das **milCERT** ist maßgeblich am Schutz der Souveränität im Cyberraum beteiligt, in erster Linie am Schutz und an der Verteidigung der einsatzrelevanten kritischen Infrastruktur des Bundesheeres und seiner IKT-Systeme.

Auch andere Institutionen und Unternehmen, etwa das Bundesrechenzentrum, die Stadt Wien, der Telekombetreiber A1 oder der Hauptverband der österreichischen Sozialversicherungsträger, betreiben eigene CERTs. Überdies wurde bereits ein erstes Branchen-CERT eingerichtet, nämlich das Austria Energy CERT (AEC) für die Energiewirtschaft. Weitere Branchen-CERTs sind in Diskussion, etwa für die Finanzwirtschaft. Diese Branchen-CERTs, die ihre Mitglieder bei Abwehr und Prävention unterstützen, fungieren auch als Meldestelle, bei denen Unternehmen der kritischen Infrastruktur gemäß den Vorgaben des NIS-Gesetzes schwerwiegende Cybervorfälle melden müssen; wenn es kein Branchen-CERT gibt, übernimmt CERT.at diese Aufgabe. Die Meldungen werden beim CSC gesammelt und ausgewertet.

Eine wichtige Schnittstelle zwischen dem öffentlichen und dem privaten Sektor, also zwischen Politik, Behörden und Wirtschaft, ist die **Cyber Security Platform** (CSP), die 2015 als Public-Private-Partnership eingerichtet wurde. Sie dient dem Erfahrungs- und Informationsaustausch im Bereich Cybersicherheit mit besonderem Fokus auf kritischen Infrastrukturen. Darüber hinaus berät und unterstützt die CSP die Steuerungsgruppe Cybersicherheit in strategischen Fragen der Cybersicherheit.

Die CSP ist überdies die Dachorganisation für bereits länger bestehende Kooperationsformate, mit denen der Kontakt zwischen verschiedenen Partnern ausgebaut und Informationen ausgetauscht werden sollen; ein übergeordnetes Ziel ist das Schaffen einer Vertrauensbasis, um im Ernstfall gemeinsam agieren zu können. Zu diesen Einrichtungen zählen etwa das **Kuratorium Sicheres Österreich** (KSÖ), das regelmäßig eine Cybersecurity-Risikomatrix erstellt, das Sicherheitsforum Digitale Wirtschaft trägt, an dem wesentliche Vertreter der österreichischen Wirtschaft teilnehmen, und zudem regelmäßig Planspiele veranstaltet, in denen unterschiedlichste Akteure gemeinsam die Abwehr von Cyberangriffen üben. Der **Austrian Trust Circle,** eine Initiative von CERT.at und Bundeskanzleramt, bietet einen formellen Rahmen für praxisnahen Informationsaustausch und gemeinsame Projekte im Sicherheitsbereich. Eine weitere, bereits seit 1999 bestehende Plattform zum Informationsaustausch ist der Verein **A-SIT – Zentrum für sichere Informationstechnologie – Austria,** in dem u. a. das Bundesministerium für Digitalisierung und Wirtschaftsstandort, die Oesterreichische Nationalbank, die Technische Universität Graz oder die Donau-Universität Krems vertreten sind. Der Verein **Cyber Security Austria** veranstaltet seit 2012 gemeinsam mit dem Abwehramt, mit Ministerien und anderen öffentlichen Stellen die jährliche »Cyber Security Challenge Austria«, bei

to the Federal Chancellery, which is in charge of public administration; together with the organization **CERT.at** it is, among other things, responsible for protecting the federal ministries from cyberattacks. Moreover, the GovCERT acts as a contact point for European and international organizations, such as the **European GovCERT Group** or the **Central European Cyber Security Platform.** The **milCERT** substantially contributes to safeguarding the sovereignty of cyberspace, first of all to protecting and defending the Armed Forces' critical infrastructure relevant for action and their ICT systems.

Similarly, other institutions and corporations, including the Federal Computing Center, the City of Vienna, the A1 Telecom Corporation, or the Austrian Social Security Federation, run their own CERTs. By the way, the Austria Energy CERT (AEC) has been established as the first industry-specific CERT, namely for the power industry. Further industry-affiliated CERTs are being discussed, such as for the financial sector. These sector-based CERTs, which support their members in defensive and preventive measures, also function as reporting units to which critical infrastructure companies are obliged to report serious cyberincidents in accordance with the provisions contained in the NIS Act; when there is no sector-specific CERT, these tasks are taken care of by CERT.at. Reported incidents are collected and assessed by the CSC.

An important interface between the public and private sectors, i.e., between policymakers, public authorities, and the business world, is the **Cyber Security Platform** (CSP), which was established in 2015 as a public private partnership. It serves the exchange of experience and information in the field of cybersecurity, with a special focus on critical infrastructures. Moreover, the CSP advises and supports the Cybersecurity Steering Group in strategic matters of cybersecurity.

The CSP is also the umbrella organization for cooperative formats that have already existed for a longer period of time and through which contacts amongst various partners should be intensified and information should be exchanged; a primary goal is to build a basis of trust so as to be able to act concertedly if a serious incident arises. One of these organizations is the **Kuratorium Sicheres Österreich** (BSA) , which regularly compiles a cybersecurity risk matrix; acts as a carrier for the Digital Economy Security Forum, with principal representatives of the Austrian business world as stakeholders; and, on a regular basis, organizes simulation games in which various players take part, thereby practicing a concerted defense against cyberattacks. The **Austrian Trust Circle,** an initiative by CERT.at and the Federal Chancellery, offers a formal framework for a practical exchange of information and joint projects in the security domain. Another platform for information exchange, which has existed since 1999, is the association **A-SIT – Center for Secure Information Technology – Austria,** with

der sich IT-Talente in Sachen »Hacking« auszeichnen können – u. a. in einer österreichischen Staatsmeisterschaft. Daneben gibt es noch in zahlreichen Branchenvereinigungen Arbeitsgruppen für Cybersicherheit; stellvertretend seien hier etwa die Plattform Industrie 4.0, der Österreichische Verband für Elektrotechnik – OVE, die Wirtschaftskammer Österreich – WKO (ARGE Sicherheit & Wirtschaft) oder der Fachverband der Elektro- und Elektronikindustrie – FEEI genannt. Überdies gibt es einen Verband österreichischer Sicherheitsexperten – VÖSI.

Eine interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft ist das IKT-Sicherheitsportal **onlinesicherheit.gv.at:** Auf dieser Website finden sich zahlreiche Informationen rund um die Sicherheit in der digitalen Welt – von Hinweisen auf aktuelle Gefahren aus dem Netz und Warnungen über Maßnahmen zur Prävention bis hin zu Erste-Hilfe-Tipps, falls etwas passieren sollte. Überdies können z. B. Sicherheitshandbücher für Unternehmen und Privatpersonen oder Termine für einschlägige Veranstaltungen abgerufen werden. Die Plattform zielt auf eine Sensibilisierung und Bewusstseinsbildung der betroffenen Zielgruppen sowie auf die Förderung einer Sicherheitskultur in Österreich.

Zentral für die Verbesserung der Lage bei Cyberbedrohungen sind Forschung und Entwicklung. In Österreich hat das Infrastrukturministerium im Jahr 2005 das **Sicherheitsforschungsprogramm KIRAS** eingerichtet, das über die Forschungsförderungsgesellschaft FFG abgewickelt wird. Dieses Programm war damals das erste seiner Art in Europa. Einer der Schwerpunkte von KIRAS war von Anfang an der Schutz der kritischen Infrastruktur in den Sektoren Energie, Wasser, Lebensmittel, Gesundheitswesen, Finanzwesen, öffentliche Sicherheit und Ordnung, Verwaltung, Verkehr und Transport, Wissenschaft sowie Kommunikation und Information. Angestrebt wird ein Forschungs- und Entwicklungskreislauf: Einerseits soll die direkte Einbindung der Bedarfsträger einen anwendungs- und ergebnisorientierten Technologieschub sicherstellen. Andererseits soll durch die Rückmeldung von Infrastrukturbetreibern auch eine reaktive Forschung angestoßen werden, die marktgesteuert ist und idealerweise nach der Laufzeit des Programms aufrechterhalten wird. Die im Rahmen von KIRAS geförderten Forschungsprojekte zielen nicht nur auf die Verhinderung oder Beseitigung von Primärschäden, sondern vor allem auch auf die von Sekundärschäden sozial-psychischer oder volkswirtschaftlicher Art wie Vertrauensverlust, Sparverhalten der Bevölkerung, Zukunftsangst oder Panik ab. Sozial- und geisteswissenschaftliche Forschung muss daher integraler Bestandteil technologieorientierter Forschungsprojekte sein. Seit Programmstart wurden rund 250 Forschungsprojekte gefördert.

Die wichtigsten Einrichtungen in der Sicherheitsforschung in Österreich sind zum einen Hochschulen, konkret die **Technischen Universitäten** in Wien und Graz sowie die **Fachhochschulen** FH Campus Wien, FH Joanneum Kapfenberg, FH OÖ Campus Hagenberg und FH St. Pölten. Höchst aktiv

partners like the Federal Ministry of Digital and Economic Affairs, the Austrian National Bank, Graz University of Technology, Danube University Krems, and others. Since 2012, the association **Cyber Security Austria** has organized the annual "Cyber Security Challenge Austria" in cooperation with the Armed Forces' Defense Agency, a number of federal ministries, and other public agencies, in which IT talents have a chance to prove themselves in the discipline of "hacking"—such as in an Austrian National Championship. In addition, numerous industrial branch associations have cybersecurity task forces, including, for example, the Platform Industry 4.0, the Austrian Association for Electronics, the Austrian Economic Chamber – WKO (task force Security & Economy), or the Trade Association of the Electric and Electronic Industries. Moreover, there is also an Association of Austrian Security Experts.

An interministerial initiative operated in collaboration with Austrian industries is the ICT security portal **onlinesicherheit.gv.at:** on this website one can find plenty of information on security in the digital world—from warnings and signs of dangers currently coming from the World Wide Web to preventive measures and first aid tips in case something should really happen. Moreover, users have access to security manuals compiled for companies and private persons or to calendars with the dates of relevant events. The platform aims at the sensitization of and awareness building within the target groups concerned and seeks to promote and cultivate security in Austria.

Research and development are vital instruments for reducing cyberthreats. In 2005, the Austrian Federal Ministry of Infrastructure installed the **Security Research Program KIRAS,** which is operated by the FFG Research Promotion Agency. This program was the first of its kind in Europe at the time. From the very beginning, one of the focal points of KIRAS has been the protection of critical infrastructures in the sectors of energy, water, food, healthcare, finance, public security and order, administration, traffic and transport, science, and communication and information. The goal is to create a research and development cycle: on the one hand, the direct integration of public agencies is to ensure an application- and result-oriented technology boost; on the other hand, the feedback received from infrastructure operators is to initiate a responsive type of research that is market-driven and ideally kept up when the term of the program has expired. The research projects funded by KIRAS are directed at the prevention or elimination not only of primary damage, but also and above all of secondary damage of a socio-psychological and politico-economic sort, such as loss of trust, the population's savings behavior, fears of the future, or panic. Social and humanistic research therefore has to be an integral part of technology-oriented research projects.

sind auch außeruniversitäre Forschungseinrichtungen, vor allem das **AIT Austrian Institute of Technology,** das ein großes **Center for Digital Safety & Security** betreibt und an zahlreiche europäische und internationale Initiativen angekoppelt ist, das COMET-Kompetenzzentrum **SBA Research** (Secure Business Austria), an dem 15 Forschungsinstitutionen und rund 70 Unternehmen beteiligt sind und das sich als Brücke zwischen Wissenschaft und Wirtschaft versteht, oder das **CD-Labor** für Verbesserung von Sicherheit und Qualität in Produktionssystemen an der TU Wien.

Um die Ausbildung der dringend benötigten Fachkräfte zu stärken, haben sich Fachhochschulen, HTLs, Forschungseinrichtungen wie etwa das AIT, Unternehmen wie Ikarus und die öffentliche Hand zum **Austria IT Security Hub** (www.security-hub.at) zusammengetan. Weitere Initiativen zu Ausbildung und Training sind in Vorbereitung. ×

Since the program was launched, some 250 research projects have been funded.

The principal security research facilities in Austria are institutions of tertiary education, most importantly the **Universities of Technology** in Graz and Vienna and the **Universities of Applied Sciences** FH Campus Wien, FH Joanneum Kapfenberg, FH OÖ Campus Hagenberg, and FH St. Pölten. There are, however, also off-campus research facilities displaying extraordinary activity in this field, most of all the **AIT Austrian Institute of Technology,** which operates a large **Center for Digital Safety & Security** and is involved in numerous European and international initiatives; the COMET competence center **SBA Research** (Secure Business Austria), in which fifteen research institutions and some seventy companies take part and which functions as a bridge between science and the business world; or the **CD Laboratory** for an improvement of security and quality in production systems at the Vienna University of Technology.

In order to intensify the training of urgently needed skilled personnel, the universities of applied sciences, the higher secondary technical schools, such research institutes as the AIT, companies like Ikarus, and government agencies have joined forces in the **Austria IT Security Hub** (www.security-hub.at). Further initiatives concerned with education and training are under preparation. ×

Die raumgreifende Installation *Probably Chelsea* von Heather Dewey-Hagborg und Chelsea E. Manning zeigt dreißig mögliche Porträts der US-amerikanischen Whistleblowerin Manning, die algorithmisch durch eine Analyse ihrer DNA erzeugt wurden. Der unheimlichen Vielzahl an persönlichen Informationen stehen die subjektiven Interpretationen der DNA-Daten gegenüber.

The room-spanning installation *Probably Chelsea* by Heather Dewey-Hagborg and Chelsea E. Manning shows thirty possible portraits of the US-American whistleblower Manning, which were produced algorithmically by means of an analysis of her DNA. The uncanny amount of personal information is contrasted with the subjective interpretations of the DNA data.

→ uncannyvalues.org

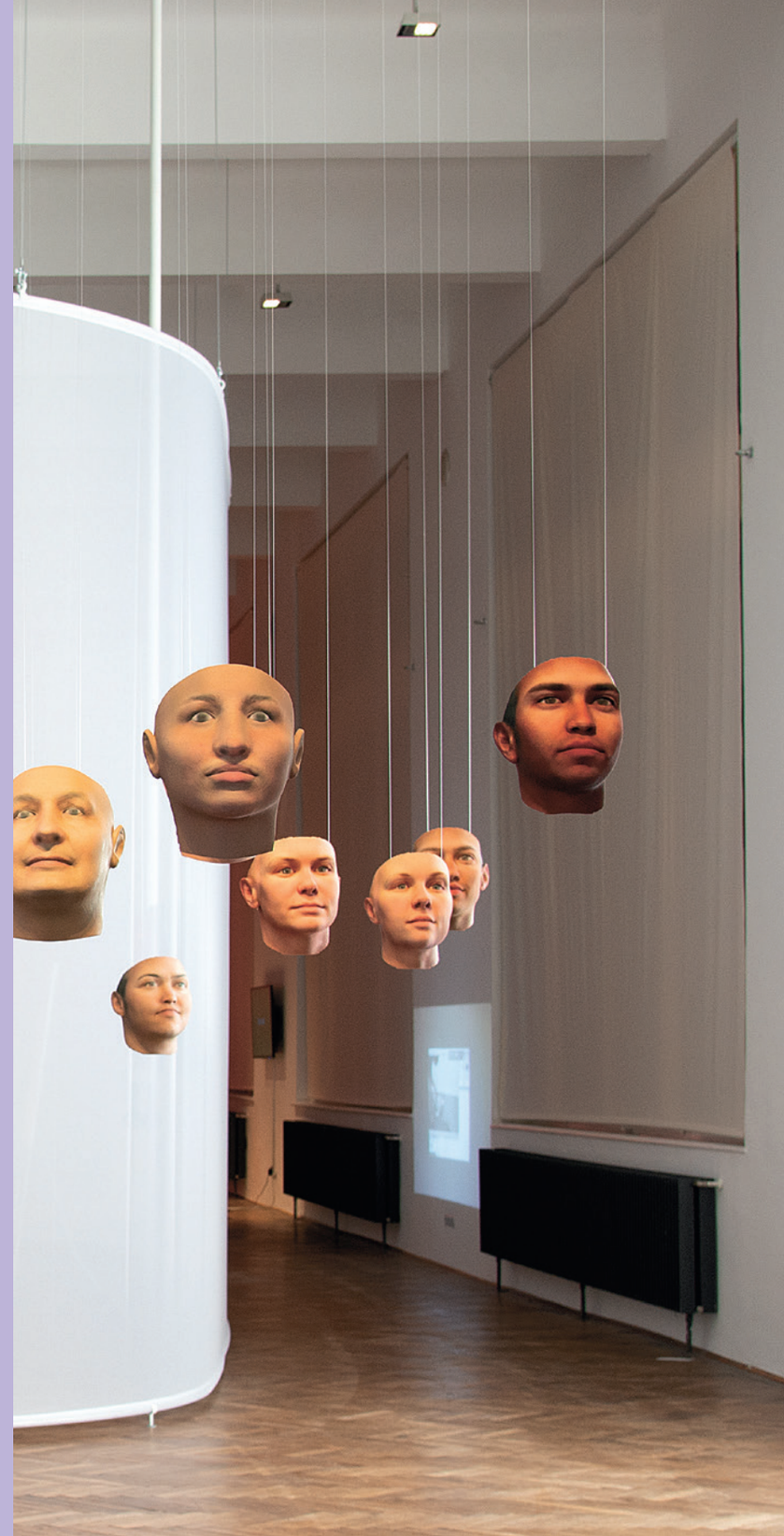
VIENNA BIENNALE FOR CHANGE 2019
Teil der Ausstellung
UNCANNY VALUES. Künstliche Intelligenz & du

Part of the exhibition
UNCANNY VALUES: Artificial Intelligence & You

CREDITS:
Exhibition view
UNCANNY VALUES. Artificial Intelligence & You

Heather Dewey-Hagborg and Chelsea E. Manning, *Probably Chelsea*, 2017

MAK Exhibition Hall
© Kristina Wissik, MAK



Walter Unger im Gespräch

»Ein Cyberangriff kostet viel weniger als ein Angriff mit herkömmlichen Systemen«

Walter Unger ist Leiter der Abteilung »Cyber Defence und IKT-Sicherheit« im Bundesministerium für Landesverteidigung. Er begann seine Tätigkeit für das Österreichische Bundesheer 1982 und befasst sich seit den frühen 2000er-Jahren in verschiedenen Positionen intensiv mit dem Thema Cybersicherheit. Er wurde mit dem Großen Ehrenzeichen für Verdienste um die Republik Österreich ausgezeichnet.

Walter Unger, Leiter der Abteilung »Cyber Defence und IKT-Sicherheit« im Bundesministerium für Landesverteidigung, über die Bedrohung Österreichs und die Möglichkeiten des Staates, darauf angemessen zu reagieren .

Österreich bekennt sich seit Jahrzehnten zur umfassenden Landesverteidigung. Seit wann sind dabei auch die Gefahren aus der Cyberwelt ein Thema?

Walter Unger: Der offizielle Startschuss dafür, auch die Cyberwelt in die Landesverteidigung einzubeziehen, war die Verabschiedung der Cybersicherheitsstrategie im Jahr 2013. Darin ist festgehalten, dass im Fall eines Angriffs auf Österreich die Verantwortung an die Landesverteidigung übergeht und auch im Cyberspace Verteidigungsmaßnahmen zu erfolgen haben. Die Wurzeln der Überlegungen gehen aber weiter zurück. Im Zuge der seinerzeitigen Zilk-Kommission hatte ich den Auftrag, mir den Kopf über die neuen Bedrohungen zu zerbrechen, und zwar im Zusammenhang mit dem Schutz kritischer Infrastruktur. Wir haben u. a. untersucht, wie die Bedrohungen aussehen und was andere Länder tun. 2004 wurde ein erstes Papier vorgelegt, manche Dinge davon sind heute Wirklichkeit.

Was passiert, wenn eine Cyberbedrohung festgestellt wird?

WU: Wir sehen uns heute gleichsam mit einer Pyramide von Bedrohungen konfrontiert. Da sind zum einen alle Bedrohungen, die jeder Person, jedem Unternehmen oder jeder Behörde begegnen können, etwa Erpressung, Phishingangriffe, Manipulation und so weiter. Damit muss im Prinzip jeder Einzelne fertig werden, der dabei allerdings die Hilfe der Kriminalpolizei in Anspruch nehmen kann. Die zweite Stufe in der Bedrohungspyramide wird erreicht, wenn ein Angriff auf eine kritische Infrastruktur erfolgt und dadurch ein krisenhafter Zustand entsteht.

An interview with Walter Unger

"A cyberattack costs much less than an attack with conventional systems"

Walter Unger is head of the department of "Cyber Defence and ICT Security" with the Austrian Federal Ministry of Defence. He started working for the Austrian Armed Forces in 1982 and has, in different positions, been intensely involved in issues of cybersecurity ever since the early 2000s. He has received the Grand Decoration of Honour for Services to the Republic of Austria.

Walter Unger, head of the department of "Cyber Defence and ICT Security" with the Austrian Ministry of Defence, about threats posed to Austria and possibilities of adequate state response.

Austria has subscribed to comprehensive national defense for decades. Since when have the dangers of the cyberworld become an issue in this field?

Walter Unger: What officially kicked off the inclusion of the cybersphere in national defense was the adoption of the Cybersecurity Strategy in 2013. It stated that in the case of an attack on Austria the responsibility devolves on national defense authorities and that defense measures are also to be taken in cyberspace. However, the earliest considerations even go back further. In the course of the then Zilk Commission {a military reform commission installed in 2003/04 chaired by former mayor of Vienna Helmut Zilk} I was assigned to wrap my head around the emergent new threats, particularly in connection with the protection of critical infrastructure. We examined, among other things, what the threats look like and what other countries were doing at the time to protect against them. In 2004, a first paper was submitted, some of the things proposed in it are a reality today.

What happens if a cyberthreat is identified?

WU: Today, we see ourselves confronted with a pyramid, as it were, of threats. There are, for one thing, the threats that each individual, business enterprise, or public institution may encounter at any time, such as blackmail, phishing attacks, manipulation, and so on. This is something that each and every one affected

Dann wird durch den Innenminister eine Cyberkrise ausgerufen. Die Federführung bleibt beim Bundesministerium für Inneres. Für diesen Fall wurde etwa das »Cyber Security Center« eingerichtet. Das Bundesheer leistet im Bedarfsfall, sofern Kräfte frei sind, Assistenz. Gibt es schließlich großangelegte Angriffe gegen die Souveränität Österreichs im Cyberraum, wäre der Zeitpunkt gekommen, nach einer Entscheidung der Politik den Cyberverteidigungsfall auszurufen und zusätzlich zu den zivilen Kräften alle verfügbaren militärischen Mittel aufzubringen. Dabei sind Gremien wie der nationale Sicherheitsrat involviert, das Parlament muss die Maßnahmen genehmigen.

Ist diese Maschinerie schon einmal voll angelaufen?

WU: Im Herbst 2016 hatten wir Angriffe gegen den Flughafen, gegen das Außenministerium, das Parlament und andere Einrichtungen – mit einer mutmaßlich politischen Motivation. Das war ein guter Anlass, die Abläufe einmal zu trainieren. 2017 sind solche Angriffe nur mehr auf schlecht gesicherte Ziele erfolgt, z. B. auf kleinere Unternehmen, die hinsichtlich Cybersecurity nicht so gut aufgestellt sind.

Was ist das schlimmste denkbare Szenario einer Bedrohung aus dem Cyberraum für Österreich?

WU: Das wäre ein konzentrierter Angriff auf die zentralen Infrastrukturen mit digitalen Mitteln – etwa auf Stromversorgung, Kraftwerke, Telekommunikation und Spitäler, aber auch auf Ministerien: Gerade in solchen Situationen müssen die Ministerien funktionieren. Wenn sie lahmgelegt werden, hätten wir einen Super-GAU. Solche Angriffe kommen freilich nicht aus blauem Himmel, sondern resultieren aus einem grundlegenden Konflikt, in dem eine Seite von Österreich politische Zugeständnisse will. So wird Macht ausgeübt. Man muss heute nicht mehr einmarschieren, sondern kann politische Ziele auch anders durchsetzen: Schadprogramme gibt es sonder Zahl, und ein Cyberangriff kostet viel weniger als ein Angriff mit herkömmlichen Systemen.

Wie häufig sind in Österreich Angriffe auf kritische Infrastruktureinrichtungen?

WU: Das wissen wir derzeit nicht genau. Wir werden es sehen, wenn in Österreich die im NIS-Gesetz festgelegte

has to cope with individually, even though they may seek help from police. The second level of the threat pyramid is reached when critical infrastructure comes under attack, leading to a crisis-like situation. The Minister of the Interior will then declare a cybercrisis, with the Ministry of the Interior still staying in command. For a case like this, the Cyber Security Center was established. If needed and if forces are available, the military will provide assistance. If there are large-scale attacks under way against Austria's national sovereignty in cyberspace, this would be the time, following a political decision, to declare the cyberdefense case and to mobilize all military forces available in addition to civilian means. Involved in this are bodies like the National Security Council; the measures taken must be approved by parliament.

Has this machinery ever been fully activated yet?

WU: In fall 2016, we had attacks launched against Vienna airport, the foreign ministry, parliament, and other institutions—presumably with a political motivation behind them. It was a good occasion to train the processes in place. In 2017, attacks of this kind were only launched against a number of ill-protected targets, such as, smaller business companies, which are not really well positioned with respect to cybersecurity.

What would be the worst scenario imaginable for a cyberspace attack on Austria?

WU: This would be a concerted attack on central infrastructures by digital means—for example, on the nation's electricity supply, power stations, telecommunications, and hospitals, but also its federal ministries: ministries need to remain functional particularly in such situations. However, attacks like that do not come out of the blue but are the result of an underlying conflict in which one side wants to coerce Austria into making political concessions. This is how power is exercised. You no longer have to invade a country but can force political goals in other ways: there is malware galore, and a cyberattack costs much less than an attack with conventional systems.

Meldepflicht greift. Dieses Gesetz gilt seit 1. Jänner 2019 und hat das Ziel, die vitalen Dienste so zu schützen, dass sie nie für längere Zeit ausfallen. Diese Maßnahme wird gerade umgesetzt. Den betroffenen Unternehmen wird per Bescheid eine Frist eingeräumt, innerhalb deren der Schutz optimiert werden soll. Dafür werden Standards vorgegeben, die im europäischen Gleichklang entwickelt wurden. Für alle Betreiber kritischer Infrastrukturen ist die Verpflichtung vorgesehen, Cybervorfälle zu melden. Das ist ein wertvoller Beitrag zum Lagebild und die Basis, noch nicht betroffene Unternehmen zu warnen. In Deutschland, wo diese Meldepflicht schon seit zwei Jahren besteht, wurden im letzten Halbjahr 186 Angriffe auf kritische Infrastrukturen registriert. Es ist zu erwarten, dass wir hier nicht mit dem üblichen Faktor 10 bei Vergleichen zwischen Deutschland und Österreich rechnen können, sondern mehr Angriffe zu erwarten haben.

Was kann Österreich gegen Angriffe tun?

WU: Eine Abschreckungsstrategie kommt für uns nicht in Frage. Einige Länder wie etwa die USA oder auch Israel, die bei einem Angriff mit allen Möglichkeiten zurückschießen können, verfahren so. Ein Beispiel: Kurz vor dem heurigen Eurovision Song Contest in Tel Aviv wurden aus dem Gazastreifen nicht nur Raketen auf Israel abgeschossen, sondern auch israelische Webseiten von Hackern angegriffen. Das war – mutmaßlich – der Grund, dass die israelische Armee im Gazastreifen bestimmte Gebäude bombardierte. Schlagartig waren die Cyberangriffe vorbei. Für uns ist das keine Option. Unsere Option ist eine defensive Strategie: Wir müssen die Infrastruktur Österreichs so gut schützen, dass kein letaler »Impact« erfolgt, der Staat nicht lahmgelegt und dazu gezwungen werden kann, Zugeständnisse zu machen. Der Staat gibt dazu Standards vor, die ein hohes Maß an Sicherheit ermöglichen und durch die, wenn etwas passiert, der Dienst in kurzer Zeit wieder verfügbar ist. Man braucht freilich Mittel, um den vorherigen Zustand wiederherzustellen.

Welche Rolle hat das Bundesheer in diesem Fall?

WU: Das Militär hat in Österreich nach wie vor die Rolle einer strategischen Reserve für alle möglichen Bereiche – etwa an der Grenze oder bei Katastrophen. Und es soll auch im Cyberbereich eine strategische Reserve bereitstellen.

How frequent are attacks on critical infrastructure facilities in Austria?

WU: Right now, we don't know precisely. We will know more once that reporting obligation stipulated in the Austrian NIS Act kicks in. This law has been in effect since January 1, 2019, the objective being to protect vital services so as to prevent disruption for any extended period of time. This measure is currently being implemented. The companies affected are being given official notice setting a deadline in which protection ought to be optimized. This includes defining standards which were developed in European agreement. For operators of critical infrastructures, an obligation of disclosure of cyberincidents is made mandatory. This is a valuable contribution to get a picture of the situation and provide a basis for alerting companies that are not yet affected. In Germany, where this obligation has been in effect for two years now, 186 attacks on critical infrastructures were reported within the last half year. It may be expected that in comparing German and Austria we cannot compute by the usual factor of ten but have to reckon with a larger number of attacks.

What can Austria do against such attacks?

WU: A strategy of deterrence is out of the question for us. Some countries, like the United States or Israel, which in the event of an attack are able to fire back with all they have, actually do so. One example: shortly before this year's Eurovision Song Contest in Tel Aviv, not only missiles were fired on Israel from the Gaza Strip, but Israeli websites were also attacked by hackers. That was—probably—the reason why the Israeli army bombed a number of buildings in the Gaza Strip. From one minute to the next, the attacks were over. For us this is not an option. Our option is a defensive strategy: we need to protect Austria's infrastructure so that no lethal impact is suffered, the state is not paralyzed and cannot be coerced into making concessions of some kind. To do so, the state defines standards that enable a high degree of security and make sure that, if anything happens, the service disrupted will be available again shortly. Of course, it takes certain means to return to the previous state.

Zweitens sind Vorkehrungen für die Landesverteidigung zu treffen, damit diese aktive Maßnahmen setzen kann. Das ist derzeit noch nicht im erforderlichen Umfang geschehen, weil noch einige rechtliche Grundlagen ausgearbeitet werden müssen. Es gibt aber z. B. mobile Elemente, die etwa bei Auslandsmissionen eingesetzt werden können. Mit diesen Elementen könnten wir das »Cyber Security Center« im Assistenzeinsatz unterstützen. Das Militär hält auch Mittel bereit, um die Regierungsfähigkeit sicherzustellen, wenn bestimmte Einrichtungen nicht mehr funktionieren – etwa Regierungsbunker und Ausweichmöglichkeiten für das Parlament. Diese sind seit Langem vorhanden und sind, glaube ich, auch in einem sehr aktuellen Zustand. Einmal im Jahr wird der Ernstfall auch durchgespielt. Eine unserer Hauptaufgaben ist das Erstellen aktueller Lagebilder. Unser Nachrichtenamt sammelt strategische Nachrichten. Wir haben einen globalen Fokus und nutzen alle möglichen digitalen Quellen. Wir können von Wien aus die ganze Welt beobachten, ohne etwas Verbotenes zu tun. Diese Lagebilder teilen wir natürlich mit allen anderen, die sie brauchen. Gerade für ein kleines Land ist Prävention wichtig – und dazu gehört die Frühwarnung, damit das eine oder andere Unternehmen Maßnahmen setzen kann, bevor es betroffen ist, und dadurch die Schäden möglichst klein gehalten werden können. Zunächst einmal muss aber das Militär die eigenen Systeme schützen, damit es geordnet und rasch reagieren kann.

Sind auch die Systeme des Bundesheeres regelmäßig Cyberattacken ausgesetzt?

WU: Ja natürlich! Wir erleben das Gleiche wie alle Unternehmen. Auch bei uns gibt es eine sehr hohe Spamrate, wir sehen gezielte Angriffe auf Einzelpersonen aus unterschiedlichsten Motiven. So hat man einmal über einen Attachée versucht, in eine andere Dienststelle einzudringen – das war sehr gezielt geplant und äußerst plausibel angelegt. Es gab auch einmal eine DDoS-Attacke, die aber nicht durchgeschlagen hat, weil sie von aufmerksamen Administratoren abgefangen werden konnte. Das Bundesheer hatte in den letzten 28 Jahren seit Beginn der Digitalisierung aber keinen wirklich schweren Virenvorfall zu verzeichnen. Mir ist auch kein Fall von Ransomware in

What is the role that the army has in such a case?

WU: In Austria, the military still has the role of a strategic reserve in all sorts of different areas—at the border, for example, or in natural disasters. And it is supposed to provide a strategic reserve also in t he area of cyberdefense. Secondly, provisions must be made for national defense to be able to take active measures. At present, this has not yet been done to the degree necessary as a number of legal foundations still need to be worked out. However, there are, for example, mobile elements that are usable for deployments abroad. We can also use those elements to come to the aid of the Cyber Security Center in an assistance deployment.The military also has means available to secure governability in case certain institutions are no longer functionable—for example, a government bunker and emergency quarters for parliament. These have long been available and are, I think, in very good repair. An emergency drill is held once a year. One of our main tasks is to compile up-to-date situation reports. Our Intelligence Office collects strategic intelligence. Our focus is global, and we exploit all possible digital sources. We can observe the entire world from Vienna without doing anything illegal. Of course, we share these situation reports with all the others who need them. For a small country, prevention is particularly important—and this includes early alerts so that one company or the other can take measures before they are hit, keeping the damage as small as possible. But first and foremost the military has to protect its own systems so as to be able to respond in a quick and orderly fashion.

Are the systems of the Austrian Armed Forces also hit by regular cyberattacks?

WU: Yes, of course! We experience the same things as every other company. We, too, have a high spam rate, and we see targeted attacks on individuals for a number of different motives. Once there was an attempt to intrude into a different office through an attaché—a very targeted plan that seemed utterly plausible. There once also was a DDoS attack which, however, did not get through, because it was fended

Erinnerung – wahrscheinlich hat sich herumgesprochen, dass es bei uns kein Geld zu holen gibt. Die Internetwelt ist für uns allerdings nicht entscheidend. Wenn in diesem Bereich etwas passiert, ist das für die Funktionsfähigkeit des Bundesheeres nicht dramatisch. Wir haben eine umfangreiche Sicherheitslandschaft zwischen der unsicheren Welt und unseren Systemen aufgebaut. Mit Beginn der Einführung digitaler Systeme in den frühen 1990er-Jahren haben wir sehr viel Sicherheit mitimplementiert – so sind beispielsweise Festplatten oder Boot-Vorgänge verschlüsselt. Es geht auch um unsere Reputation: Würde ausgerechnet das Bundesministerium, das für Verteidigung zuständig ist, erfolgreich attackiert, wäre man wohl weithin der Ansicht, dass man sich auf das Bundesheer nicht verlassen kann.

Und wie ist das bei den militärischen Systemen? Werden die auch angegriffen?

WU: Solche Systeme sind Hochsicherheitssysteme. Wir haben viele solche Systeme, etwa für die Luftraumverteidigung, für Auslandsdestinationen oder für Funkverbindungen. Meines Wissens hat es da nie einen Vorfall gegeben. Diese Systeme sind völlig abgekoppelt von anderen Systemen, sie sind hochsicher verschlüsselt, Zugang haben nur Einzelpersonen mit speziellen Rechten, es gibt keinen Import von Daten von außen usw. Wenn Daten über das Internet verschickt werden – etwa bei Auslandseinsätzen –, dann sind diese stark verschlüsselt.

Können Sie aufgrund Ihrer Erfahrungen mit hochsicheren Systemen Empfehlungen für die zivile Welt geben?

WU: Die wichtigste Empfehlung ist, für alle möglichen Zwecke eine starke Verschlüsselung einzusetzen. Das allein bietet schon ein hohes Maß an Schutz. Eine zweite wesentliche Maßnahme ist das Trennen von wichtigen Systemen und unsicheren Bereichen: Alles was nicht zwingend das Internet braucht, sollte auch nicht daran angekoppelt sein. Damit hat man einen großen Teil von Schadmöglichkeiten abgehalten.

Woran mangelt es im Bereich Cybersicherheit aus Ihrer Sicht derzeit am meisten?

WU: Daran, dass Soft- und Hardware so viele Schwachstellen haben. Hier müssten sich die EU und große Staaten

off by vigilant administrators. In the past 28 years, ever since the beginning of digitization, the Austrian Armed Forces have not seen a single severe computer virus incident. Also, I cannot recall any case of a ransomware attack—probably word has gotten around that there is no money to be had from us. For us, though, the world of the Internet is not really crucial. If anything happens in this area, the effect on the functional capacity of the Armed Forces is not dramatic. We have built a comprehensive security landscape between the unsafe world and our own systems. From the beginning of the introduction of digital systems in the early 1990s we have been implementing a lot of security—for example, hard disks and boot processes are all encrypted. Our reputation is on the line here: if the very same ministry that is responsible for national defense could be successfully attacked there would be a widespread view that the Austrian Armed Forces cannot be relied upon.

And what about the military systems? Are they being attacked, too?

WU: These are high-security systems. We have many such systems, for example, for the defense of Austria's air space, for destinations abroad, or for radio communications. To my knowledge, there has never been an incident there. These systems are completely disconnected from other systems and have high security encryption, only individuals with special rights have access to them, there is no import of data from outside, etc. If data are sent over the Internet— for example, in cases of foreign deployment—they are strongly encrypted.

Given your experience with high-security systems, what recommendations do you have for the civilian world?

WU: The most important recommendation is to use strong encryption for all sorts of purposes. This alone affords a high amount of protection. Another essential measure is to keep important systems separated from unsafe areas: anything that does not absolutely need the Internet should not be connected to it. Thus, you have already closed out most of the possibilities for damage.

viel stärker einbringen und von den Lieferanten eine höhere Qualität fordern. In allen möglichen Bereichen gibt es Qualitätssicherung, Garantien und Haftung, wenn etwas nicht funktioniert. Man denke an die Autoindustrie: Wenn dort ein Fehler gefunden wird, gibt es sofort große Rückrufaktionen. Und was ist bei der Software? Bei den Apps? Man hat keine Garantie, wie lange es ein Service gibt, man weiß nicht, wie viele Schwachstellen es gibt. Nach wie vor wird nach dem Motto gearbeitet: Wer schneller ist, macht den Gewinn. Hier sollten in ganz großem Rahmen Haftung sowie bestimmte Maßnahmen eingefordert werden, die Konsumenten und Unternehmen vor schlechten Programmen und schlechter Hardware schützen. ✖

In your view, what is the greatest shortcoming in the field of cybersecurity?

WU: The fact that both hard- and software have so many weak spots. Here, the European Union and big states should really put their foot down and demand better quality from suppliers. There is quality control, warranties, and liability in all sorts of fields if things don't work the way they should. Just think of the auto industry: there, if a defect is found, the next thing you know is a large-scale product recall. And what about software? What about apps? You never get a guarantee for how long a service will be available, you never know how many vulnerabilities there are. They still operate on the motto of "Who's faster gets to reap the profit." Here, liability obligations as well as specific measures should be called for on a broad scale to protect consumers and business enterprises from bad software programs and bad hardware. ✖

TEIL 2 / PART 2

Was tun? Forschungs-themen und Maßnahmen

What Next? Research Themes and Measures

Forschung für mehr Cybersicherheit

Bei der Entwicklung von cybersicheren IT-Systemen werden bessere Technologien gesucht. »Allerdings geht es nicht nur um Technik, sondern auch um gesellschaftliche und wirtschaftliche Fragen, um Prozesse und Gesetze, Training und Usability«, betont der Sicherheitsspezialist am AIT Austrian Institute of Technology Helmut Leopold. Eine Tour de Force durch die aktuelle Sicherheitsforschung – die in den folgenden Kapiteln punktuell vertieft wird.

»Sicherheitsaspekte müssen vor allem bei komplexeren Systemen von Anfang an mitgedacht und miteingeplant werden, um effektiv wirken zu können«, lautet das Credo von Helmut Leopold, Head of Center for Digital Safety & Security am AIT. In der Fachsprache nennt man diesen Ansatz »Security by Design«. Der erste Schritt ist eine sorgfältige Risikoanalyse. »Man muss konkrete Bedrohungsszenarien erarbeiten – für das gesamte Unternehmen, für Unternehmensteile, für jeden Staat. Man muss wissen, welche Bereiche gefährdet sind und wie man diese schützen könnte«, so Leopold. Diese Bedrohungsszenarien müssen dann bei der Konzeption und Entwicklung eines Systems entsprechend berücksichtigt werden. Dazu werden zahlreiche Hilfsmittel und neue Verfahren entwickelt – von Standards bei der Programmierung über den gezielten Einsatz digitaler Identitäten bis hin zu neuen Architekturen von IT-Systemen (etwa verteiltem Speichern und Rechnen). Ein eigenes Kapitel ist der Einsatz von innovativen Verschlüsselungsmethoden (siehe Seite 122) und von Quantentechnologien zur sicheren Kommunikation (siehe Seite 130). Überdies können Systeme modelliert und getestet werden, noch bevor sie realisiert werden – »ähnlich wie es ein Architekt macht, bevor er einen Turm baut«, so Leopold.

Nach dieser Systemdesignphase setzt man die jeweils notwendigen Schutzmaßnahmen ein. Darunter fallen etwa die auch Computerlaien bekannte Virenscanner oder Firewalls, aber auch das sogenannte »Security Information and Event Management« (SIEM), also Systeme, die automatisch und blitzschnell nach allerlei (bekannter) Malware und Fehlfunktionen von IT-Systemen suchen – und im Fall des Falles Alarm schlagen. Allerdings: Eine zentrale Erkenntnis der Computerwissenschaften lautet: Man kann niemals absolut sicher sein und sich zu 100 Prozent vor allen möglichen Bedrohungen schützen. Schlussendlich bleibt es eine Frage der wirtschaftlichen Risikobeurteilung.

Research for More Cybersecurity

Developing cyberproof IT systems, research goes in search of improved technologies. "However, this is not only about technology but also about social and economic issues, about processes and laws, training and usability," emphasizes Helmut Leopold, security expert at the AIT Austrian Institute of Technology. A tour de force of state-of-the-art security research—selected topics of which are looked into in more detail in the following chapters.

"Security aspects have to be taken into account and integrated from the very outset, particularly in the case of more complex systems so as to be efficient," is the credo of Helmut Leopold, Head of Center for Digital Safety & Security at the AIT. In technical jargon, this approach is referred to as "security by design." The first step is a thorough risk analysis. "A threat scenario has to be figured out for each individual case—for each company, for each state, for each person. One needs to know what areas are at risk and how they could be protected," Leopold points out. These threat scenarios are subsequently to be taken into consideration in the conception and development of a system. To this end, numerous tools and new methods are devised—from programming standards to the systematic use of digital identities to new architectures of IT systems (such as distributed computing). Another matter are innovative encryption techniques (see pages 123) and quantum technologies for secure communication (see pages 131). Moreover, systems can be modeled and put to the test even before they are realized—"similar to what an architect does before he builds a tower," Leopold says.

After this system design phase, the necessary protective measures are used. These include, for example, virus scanners or firewalls as well as so-called "security information and event management" (SIEM), i.e., systems looking for all kinds of (known) malware and malfunctions in IT systems automatically and at cyberspeed—and sounding the alarm in emergency situations. However: according to a central insight of computer sciences, one can never be absolutely sure safe and 100 percent protected from all sorts of threats. Ultimately, it remains a matter of economic risk assessment..

Active protection and identification of anomalies

However, such systems have their limits. "No doubt the fight against known threats is and will continue to be crucial, but this alone

Aktiver Schutz und Erkennung von Anomalien

Solche Systeme stoßen jedoch an ihre Grenzen. »Der Kampf gegen bekannte Bedrohungen ist und bleibt natürlich wichtig, aber das reicht bei Weitem nicht mehr aus«, erläutert Leopold. Denn zum einen können niemals alle Sicherheitslücken von Systemen bekannt sein; so sind etwa Softwarefehler unvermeidlich, die von Angreifern ausgenutzt werden können. Zum anderen wird die Bedrohungslandschaft zunehmend unübersichtlich, und das unter anderem deshalb, weil die Angreifer immer sorgfältiger ausgeklügelte Waffen einsetzen und zu »advanced persistent threats« (APTs) bündeln, die an mehreren Stellen gleichzeitig angreifen und lange Zeit unbemerkt in IT-Systemen bleiben können, um Systemschwächen für zukünftige Angriffe zu identifizieren. Um diese zu erkennen, müssen völlig neue Wege beschritten werden. Eine Hauptforschungsrichtung sind hier Systeme, die automatisch Anomalien erkennen – also Abweichungen von Systemzuständen, die als »normal« gelten (siehe Seite 138). »Wenn es zum Beispiel noch nie vorgekommen ist, dass auf eine bestimmte IP-Adresse zugegriffen wurde, dann sollte dies automatisch vom System erkannt werden«, nennt Leopold ein einfaches Beispiel. Dann kann man sich umgehend auf die Suche nach der Ursache für die Anomalie machen. Zudem versucht man, dem Verursacher der Cyberattacke auf die Spur zu kommen – dies nennt man in der Fachsprache »Attribution«, Zuschreibung. Wenn das auch schwierig ist, gibt es doch Fortschritte: So gelingt es beispielsweise immer besser, sogar in verteilten Datenbanken, wie etwa in Blockchains, Zusammenhänge zu finden (siehe Seite 144).

Damit solche Maßnahmen greifen können, müssen IT-Systeme mit Sensoren ausgestattet sein, die relevante Informationen sammeln – so wie etwa Virenscanner ständig E-Mails untersuchen. Dieser Ansatz berührt eine gesellschaftlich und juristisch höchst relevante Problematik, nämlich die des Schutzes der Privatheit und vor Überwachung. Durch entsprechende Gestaltung von IT-Systemen können Anforderungen des Datenschutzes von vornherein implementiert werden (»Privacy by Design«).

Der Mensch als Sicherheitsrisiko

Ein System ist bekanntlich nur so sicher wie sein schwächstes Glied – und das schwächste Glied ist in vielen Fällen der Mensch, der mit IT-Systemen arbeitet. Fehler können dabei auf vielen Ebenen passieren. Das beginnt beim Umgang mit Passwörtern und reicht bis zur Aufmerksamkeit, die man E-Mails im Posteingang schenkt; infizierte E-Mails, die unbedacht geöffnet werden, sind unverändert das häufigste Einfallstor für Cyberangriffe. »Security ist nicht nur ein Expertenthema, sondern auch jeder und jede BenutzerIn – als Privatperson als auch als MitarbeiterIn in Unternehmen – hat eine Verantwortung«, betont Leopold. Jeder Einzelne müsse beispielsweise überlegen, wie er seinen Facebook-Account einrich-

is by no means sufficient any longer," Leopold explains. On the one hand, one can never know all security gaps in systems; software flaws, for example, which attackers can take advantage of, are unavoidable. On the other hand, the threat landscape is becoming increasingly confusing, among other things because attackers have come to employ more and more carefully thought-out weapons, bundling them to create advanced persistent threats (APTs) capable of attacking from several directions simultaneously and of making trouble in IT systems while remaining undetected for extensive periods of time to identify system weaknesses for future attacks. In order to identify them, entirely new paths have to be cut out. A main domain of research encompasses systems recognizing anomalies automatically—i.e., deviations from system states considered normal (see pages 139). "If it has never happened before that the computer tries to connect to a specific IP address, the system should detect it," Leopold gives a plain example. Then one will be forced to immediately identify the cause of this anomaly. Moreover, attempts are made to track down those having caused the cyberattack—which is called "attribution" in expert jargon. Although this is difficult, progress has indeed been made: for example, it has gradually become easier to identify connections even in encrypted databases, such as in blockchains (see pages 145).

For such measures to be effective, IT systems have to be equipped with sensors collecting relevant information—such as virus scanners constantly checking e-mails. This method touches a set of problems that are highly relevant from the perspectives of society and law, namely those of the protection of privacy and against surveillance. Through an appropriate design of IT systems, data protection requirements can be implemented from the very beginning ("privacy by design").

Humans as a security risk

As is well known, a system is only as strong as its weakest link—and in many cases this link is a human working with IT systems. Mistakes can happen on multiple levels, ranging from the handling of passwords to the attention paid to e-mails arriving in one's inbox; infected e-mails opened carelessly continue to be the most frequent door for cyberattackers. "Security is not a theme limited to experts, everyone is responsible," Leopold underlines. For example, every individual has to find out how to create a Facebook account in such a way that it cannot be abused or when to use strange USB sticks carelessly. It is also important that companies remind their employees of behaving properly. Organizational measures and the definition of operational processes are equally relevant—such as who is authorized

tet, damit dieser nicht missbraucht werden kann, und wann man fremde USB-Sticks unbekümmert verwendet. Wichtig ist auch, MitarbeiterInnen auf ein richtiges Verhalten aufmerksam zu machen. Nicht weniger bedeutsam sind organisatorische Maßnahmen und die Definition von Betriebsprozessen – etwa wer welche Berechtigungen zum Zugriff auf Daten hat, wer im Fall eines Problems wen informieren muss, wie die Übergabe an die nächste Schicht funktioniert, wie Wartungsprozesse durchgeführt werden, usw.

Sowohl Abläufe und Prozesse als auch das Verhalten von Menschen können in sogenannten Cyberranges getestet und trainiert werden. Darin werden alle wichtigen Aspekte eines konkreten Systems simuliert, sodass Auswirkungen bestimmter Handlungen unmittelbar ausprobiert und Maßnahmen bei Cyberangriffen geübt werden können. In die Gestaltung von Cyberranges fließt aktuell viel Forschungsaufwand (siehe Seite 148). Solche Planspiele werden beispielsweise für Übungen von Betreibern kritischer Infrastruktur und Behörden eingesetzt, um die Cyberskills aller Beteiligten zu trainieren, die Zusammenarbeit verschiedener Akteure zu verbessern oder Abläufe zu optimieren. Immer mehr Unternehmen nutzen diese Möglichkeit, so Leopold. »Denn man kann Sicherheit nicht als Produkt kaufen. Sicherheit muss jedes Unternehmen für sich lernen.«

Schutz kritischer Infrastrukturen

Ein zentrales Forschungsthema im Bereich der Cybersecurity ist – nicht nur am AIT – der Schutz sogenannter »kritischer Infrastrukturen«. Das sind Einrichtungen, die wichtig für das staatliche Gemeinwesen sind und deren Ausfall Versorgungsengpässe, Beeinträchtigungen der nationalen und öffentlichen Sicherheit oder der staatlichen Stabilität mit sich bringen kann – etwa im Bereich der Wasser-, Energie- oder Lebensmittelversorgung, aber auch des Gesundheits-, Verkehrs- und Finanzwesens, der öffentlichen Verwaltung oder der Kommunikationssysteme. Diese Infrastrukturen sind meist sogenannte cyberphysische Systeme, die auf dem Zusammenwirken von physischen Einrichtungen und IT-Systemen beruhen. Daher ist ihr Schutz besonders wichtig und aufwendig – was große Forschungsanstrengungen nach sich zieht (siehe Seite 152).

Ein zentrales Instrument für den Schutz kritischer Infrastrukturen sind Lagebilder, die von den zuständigen Behörden erstellt werden. Diese beinhalten alle relevanten Informationen über den Zustand von Infrastrukturen, die zum Teil von den Behörden selbst erhoben werden und zum Teil von Meldungen der Infrastrukturbetreiber stammen. Erfasst wird in einem Lagebild etwa, welche Bedrohungen und welche Schadsoftware gerade aktuell sind, wer von welchen Vorfällen wie stark betroffen ist und welche Folgen ein Vorfall haben könnte, um daraus weitere Maßnahmen abzuleiten – etwa wer im Krisenfall wen informieren sollte, welche Abwehrmaßnahmen sinnvoll sind oder ob noch nicht betroffene Organisationen präventiv tätig werden können oder sollen. »Dafür braucht man einen umfassenden

to access which data, who has to be informed in the case of a problem, how the system is handed over to
the next shift, how maintenance processes are dealt with, etc.

Both procedures or processes and human behavior can be tested and trained in so-called “cyberranges.” They simulate all relevant aspects of a concrete system so that the consequences of certain actions can immediately be tried out and measures against cyberattacks can be put to the test. Currently, a lot of research goes into the design of these cyberranges (see pages 149). Such simulation games are used, for example, by operators of critical infrastructures and government agencies so as to train the cyberskills of all stakeholders, improve the collaboration of various players, or optimize processes. According to Leopold, more and more companies make use of this possibility. “For one cannot buy security like a product. Security is something each company or organization has to learn individually.”

Safeguarding critical infrastructures

The protection of so-called “critical infrastructures” is a central research topic in the sphere of cybersecurity in general, not only at the AIT. Critical infrastructures are vital facilities for governmental or communal entities, and their breakdown can cause supply shortfalls, interfere with national and public security, or jeopardize governmental stability—in areas like water, energy, or food supply, healthcare, traffic, finance, public administration, or communications. Most of the time, these infrastructures are so-called cyberphysical systems based on the interaction of physical facilities and IT systems. Their protection is thus particularly demanding—and requires an enormous research effort (see pages 153).

Central instruments for the protection of critical infrastructures are situation reports compiled by the governmental agencies in charge. These reports contain all relevant information on the state of infrastructures—information partly gathered by the agencies themselves and partly deriving from reports filed by the operators of infrastructures. For instance, situation reports register what threats and types of malware are prevalent at the moment, who is affected by which incidents and to what extent, and what consequences an incident could have so that further measures can be deduced from it—such as who has to inform whom in an emergency, what defense measures make sense, or if organizations not yet afflicted could or should undertake preventive steps. “This requires a comprehensive exchange of information, which of course must be determined by clear rules and can only be carried out in a space of mutual trust,” Leopold says. The central research problem in this respect: how should information from cyberspace be systematized and presented so that policymakers can

Austausch von Informationen, der natürlich durch klare Regeln bestimmt werden muss und auch nur in einem Raum des gegenseitigen Vertrauens durchgeführt werden kann«, so Leopold. Die hier zentrale Forschungsfrage: Wie bereitet man Informationen aus dem Cyberraum so auf, dass Entscheidungsträger auf ihrer Basis sinnvoll Entscheidungen treffen können, Datenschutzaspekte berücksichtigt werden und Missbrauch ausgeschlossen werden kann?

Internationale Kooperation

Ein weithin ungelöstes Problem ist die internationale Kooperation in Sachen Cybersecurity. Sie hat mehrere Dimensionen. »Früher war nur Krieg international, heute ist das auch Verbrechen«, meint Leopold. Daher sind auch im Kampf gegen Cyberkriminalität internationale Kooperation und grenzüberschreitender Informationsaustausch zwischen Behörden notwendig – etwas, das in der EU bereits existiert. Ein anderer nicht weniger wichtiger Aspekt hängt mit den international verschränkten Lieferketten zusammen. Ein Automobilhersteller etwa bezieht Zehntausende Einzelteile von Tausenden Zulieferern, die ihrerseits wieder zahlreiche Sublieferanten haben. Ohne internationale Standards und Regeln, an die sich alle entlang der Supply Chain halten, sind cybersichere Produkte kaum denkbar. Leopold: »Das beschäftigt derzeit das gesamte globale Zuliefersystem.«

»Wir brauchen ein Minimumset von Regeln und Vereinbarungen sowie internationale Standards für Hersteller, für Prozesse, für Risikomanagement, für den Betrieb von Systemen usw., denen alle vertrauen können«, sagt Leopold. Nachsatz: »Anders geht das nicht – sonst haben wir weiterhin ein Wirrwarr wie heute.« Dieser Aspekt stand auch bei der heurigen »Vienna Cyber Security Week« im Zentrum, die vom AIT und der Wirtschaftskammer Österreich im März veranstaltet wurde und zu der rund 700 Teilnehmer aus rund 70 Ländern anreisten. Diskutiert wurden beispielsweise vertrauensbildende Maßnahmen innerhalb der OSZE oder der EU, die zu effektiven Mechanismen führen sollen, mit denen die Sicherheitslage global verbessert werden kann. Eine der vorgebrachten Visionen ist etwa, dass ein Auto erst dann verkauft werden darf, wenn es – analog dem heutigen CE-Zeichen, das eine gewisse Betriebssicherheit garantiert – eine Art Cybersecurity-Pickerl hat. Nachsatz: »Das kostet natürlich Geld, aber so etwas benötigen wir dringend, um in der globalen Vernetzung und Daten-bestimmten Welt von morgen unsere IT-Systeme sicher und unbedenklich verwenden zu können«, betont Leopold. ×

rely on it for meaningful decisions, privacy aspects are taken into account and abuse can be ruled out?

International cooperation

A multidimensional problem largely unsolved is international cooperation in matters of cybersecurity. “Formerly, only war was international, today this also holds true for crime,” Leopold remarks. This is why international cooperation and a cross-border exchange of information among authorities is an absolute necessity—something that already exists in the EU. Another aspect, no less important, has to do with internationally entwined supply chains. A car manufacturer, for example, receives tens of thousands of separate parts from thousands of suppliers, who in turn work with countless subcontractors. Without international standards and rules generally obeyed along the supply chain, cybersecure products are hardly thinkable. Leopold: “This presently preoccupies the entire global supply system.”

“We need a minimal set of rules and agreements and international standards for manufacturers, for processes, for risk management, for the operation of systems, etc. in which all of us can trust,” Leopold says, adding: “This is the only feasible way—otherwise today’s imbroglio will be prolonged.” This aspect was also in the focus of this year’s “Vienna Cyber Security Week,” which was organized by the AIT and the Austrian Economic Chamber in March, and which was attended by some 700 participants from about 70 countries. They discussed, among other things, confidence-building measures within the OSCE and the EU that should lead to effective mechanisms through which the security situation can be improved on a global level. One of the visions suggested was that a car can only be sold if a certain level of operational security is guaranteed, i.e., if it comes with a kind of cybersecurity label, similar to the CE certification mark. “Of course, that costs money, but we urgently need something like that to be able to use our IT systems safely in the global networking and data-driven world of tomorrowy,” Leopold emphasizes. ×

Gut verschlüsselt

Die Verschlüsselung von Daten gilt als eine der wichtigsten Maßnahmen, um deren Sicherheit zu gewährleisten. Die herkömmlichen Verfahren funktionieren zwar im heutigen Internet sehr gut, doch zunehmende Vernetzung, Cloud Computing und das Internet der Dinge bringen neue Herausforderungen mit sich und erfordern neue Verschlüsselungsmethoden. Überdies bedrohen die künftigen Quantencomputer die Zuverlässigkeit heutiger Verschlüsselungsverfahren.

Die Erfindung der Schrift veränderte den Lauf der Menschheitsgeschichte. Plötzlich wurden Gedanken teilbar, auch ohne dass zwei Kommunikationspartner einander persönlich kennen und treffen mussten. Das schürte schon vor Jahrtausenden Sorgen, dass Nachrichten in unbefugte Hände gelangen könnten, und man machte sich auf die Suche nach Verfahren, um das zu verhindern. Das war die Geburtsstunde zum einen der Steganografie (dem Verbergen von Kommunikationskanälen) und zum anderen der Kryptografie (dem Verschlüsseln von Texten, das verhindert, dass ein unbefugter Dritter die Bedeutung einer Nachricht erfassen kann).

Schon vor rund 5000 Jahren haben die alten Ägypter manche Texte – etwa solche mit kosmologischen Inhalten – in einer Schrift verfasst, die nicht allgemein verständlich war. Bekannt ist auch, dass sich Gaius Iulius Caesar in seiner militärischen Korrespondenz einer Verschlüsselung bediente: Er verwendete dafür ein simples Verfahren, Buchstaben systematisch gegeneinander auszutauschen (konkret: eine Verschiebung des Alphabets um drei Buchstaben). Schon bei dieser frühen Form der Kryptografie war die Verfügung über den Schlüssel entscheidend; man musste den Algorithmus kennen, der die betreffende Nachricht zu dechiffrieren erlaubt. Das Austauschen von Buchstaben oder Buchstabengruppen nach gewissen Regeln blieb (neben dem Erfinden geheimer Schriften) lange Zeit in der europäischen Geschichte das Maß der Dinge – so etwa auch bei der im Zweiten Weltkrieg vom Deutschen Reich eingesetzten ENIGMA-Maschine (die sowohl vom polnischen als auch vom britischen Geheimdienst geknackt wurde).

Diese herkömmlichen Methoden sind allerdings heute veraltet und unsicher: Durch die große Rechenleistung moderner Computer sind sie allesamt problemlos dechiffrierbar (auch wenn manche Handschriften wie etwa das mittelalterliche Voynich-Manuskript bis heute nicht lesbar sind – was bei manchen Forschern Zweifel nährt, ob die Geheimschrift überhaupt sinnvolle Informationen enthält). Heute werden nicht mehr ganze Buchstaben oder Zeichen durch andere ersetzt, sondern Bits (also Teile von Zeichen).

Well-Encrypted

Data encryption is considered to be one of the most important measures to warrant data security. Conventional methods serve their purpose fine on today's Internet, but increased interconnectedness, cloud computing, and the Internet of things bring on new challenges and require new encryption techniques. Also, the quantum computers of the future threaten the sheer reliability of today's encryption methods.

The invention of writing changed the course of human history. All of a sudden, thoughts could be shared without two communication partners having to know each other and meet in person. Already thousands of years ago, this stoked fears that messages might fall into unauthorized hands, and people started looking for ways to prevent this. It was the birth of both steganography (the hiding of communication channels) and cryptography (the encoding of text to prevent unauthorized third parties from grasping the meaning of a message).

Already about 5000 years ago, the ancient Egyptians wrote down certain texts—for example, those containing cosmological contents—in a script that was not generally decipherable. It is also known that Julius Caesar used encryption in his military correspondence: he relied on a simple method of systematically switching letters (specifically, a shift of three in the alphabet). Even in this early form of cryptography, having the key was crucial; one had to know the algorithm that would allow deciphering the message. Switching individual letters or groups of letters with one another according to certain rules remained the yardstick of encryption for a long time in European history—as was the case with the ENIGMA machine used by the German Reich in World War II (which was cracked by both Polish and British secret services).

These conventional methods are, however, outdated and unsafe today: given the great computing power of modern computers, they are all easily decipherable (even if some manuscripts, such as the medieval Voynich manuscript, have remained illegible until today—which has raised doubts among scholars whether the cipher contains any meaningful information at all). Today, it is no longer whole letters or characters that are replaced with others, but bits (i.e., parts of characters). If the rules of such exchange are made sufficiently complicated—that is, if the key is long enough—such encryption systems cannot be cracked within any reasonable period of time.

Wenn man die Austauschregeln hinreichend kompliziert gestaltet – wenn also der Schlüssel lang genug ist –, sind solche Verschlüsselungssysteme in vernünftiger Zeit nicht zu knacken.

Symmetrische und asymmetrische Verfahren

Gebräuchlich sind zwei grundlegende Kryptografiesysteme: Bei »symmetrischen« Systemen haben alle Beteiligten denselben Schlüssel, der sowohl für die Ver- als auch für die Entschlüsselung eingesetzt wird. Der entscheidende Punkt ist, dass die Schlüssel über einen sicheren Weg ausgetauscht werden müssen. 1976 wurde erstmals das Konzept für eine »asymmetrische« Verschlüsselung publiziert, das dieses Problem umgeht. Die Idee dahinter ist, ein Paar zusammenpassender Schlüssel zu verwenden: Zum Verschlüsseln dient ein »öffentlicher« Schlüssel, den alle kennen; zum Entschlüsseln ist hingegen ein »privater« Schlüssel notwendig. Diese beiden Schlüssel sind durch mathematische Verfahren miteinander verknüpft: Aus dem privaten Schlüssel kann man relativ einfach den öffentlichen Schlüssel berechnen – in die andere Richtung geht das aber nur extrem schwer. Gebräuchlich dafür ist beispielsweise die Multiplikation großer Primzahlen: Dieser Schritt ist einfach berechenbar – die Umkehrung, also die Zerlegung in Primfaktoren, dauert hingegen bei großen Zahlen sehr, sehr lang und ist daher in vernünftiger Zeit nicht möglich; selbst heutige Supercomputer benötigen dafür Jahrtausende. Ein anderes weitverbreitetes schwieriges Rechenverfahren zur Schlüsselberechnung nennt sich »diskreter Logarithmus«.

Das heutige Internet basiert sehr stark auf dieser asymmetrischen Verschlüsselung. »Man weiß heute sehr genau, wie man einen sicheren Kanal aufbaut – wie zum Beispiel im Internet eine https-Verbindung. Die Kryptografie funktioniert momentan perfekt, um zum Beispiel Internetbanking abzuwickeln«, kommentiert Thomas Lorünser, Verschlüsselungsexperte am AIT Austrian Institute of Technology. Allerdings: »Diese Kryptografieverfahren wurden für Punkt-zu-Punkt-Verbindungen gebaut. Sie lassen sich nicht mehr einfach auf die neuen Formen des Einsatzes von Informationstechnologien anwenden: auf Cloud Computing, das Internet der Dinge und die immer stärkere Vernetzung.«

Kommunikation findet nicht mehr zwischen zwei definierten Punkten statt, sondern wird in der Cloud geteilt – der Mehrwert wird zunehmend durch das Teilen von Daten und die Kollaboration vieler Beteiligter erzielt. Dafür werden auch Daten von immer mehr miteinander vernetzten Geräten genutzt. Da die Services heute über das Internet laufen, ist die Angriffsfläche größer. »Man kann zwar immer den sicheren Kanal anwenden, aber das hilft nicht mehr, weil die Daten in der Cloud für die Provider einsichtig sind – und damit potenziell auch für jeden Eindringling.«

Symmetric and asymmetric methods

There are two basic cryptographic systems that are common: in "symmetric" systems, all participants have the same key, which is used for both encryption and decryption. The crucial point is that the keys must be passed on in a secure way. The concept for "asymmetric" encryption, which circumvents this problem, was first published in 1976. The idea behind it is to use a pair of matching keys: a "public" key, which is known to everyone, is used for encryption; for decryption, however, a "private" key is needed. Those two keys are linked by mathematical procedures: it is relatively easy to calculate the public key from the private key—but extremely difficult to go the opposite direction. One common procedure, for example, is multiplication of large prime numbers: this step is easily calculable—the inverse process, i.e., the factoring into prime numbers, takes very, very long for large numbers and therefore is not feasible within a reasonable period of time; even today's supercomputers need thousands of years for this. Another widely used intricate method for key computation is called "discrete logarithm."

Today's Internet is based on such asymmetric encryption. "We know exactly how to set up a secure channel today—like an https connection on the Internet. Cryptography works perfectly at the moment, for example to operate Internet banking," says Thomas Lorünser, encryption expert at the AIT Austrian Institute of Technology. However, "these cryptographic procedures were built for point-to-point connections. They can no longer be applied to the new ways of deploying information technologies: cloud computing, the Internet of things, and ever-increasing interconnectedness."

Communication no longer takes place between two defined points but is shared in the cloud—with surplus value being increasingly generated through data sharing and multi-party collaboration. This also involves the use of data from growing numbers of networked devices. With services being run over the Internet, the number of points of attack increases. "You can always use the secure channel, but that doesn't help any longer because the data in the cloud is visible to providers—and hence potentially also to any intruder."

Surplus value through dynamic data sharing

The crucial questions are: How to keep control over one's data? And how can you restore end-to-end security when data is stored and processed on foreign servers? "There is still no satisfactory solution for this today," says Lorünser. But there are plenty of ideas. "We are trying to understand how cryptography must be modified to integrate it with these new systems and support new areas of application." The central problem is how to keep data encrypted in the cloud but still be able to

Mehrwert durch dynamisches Teilen von Daten

Die entscheidenden Fragen lauten: Wie kann man die Kontrolle über seine Daten behalten? Und wie kann man wieder Ende-zu-Ende-Sicherheit herstellen, wenn Daten auf fremden Servern gespeichert und prozessiert werden? »Dafür gibt es heute noch keine zufriedenstellende Lösung«, so Lorünser. Man hat aber bereits viele Ideen. »Wir versuchen zu verstehen, wie man die Kryptografie verändern muss, um sie in diese neuen Systeme einzubauen und die neuen Anwendungsfelder zu unterstützen.« Das zentrale Problem sei, die Daten in der Cloud verschlüsselt zu halten, aber trotzdem kollaborativ zu arbeiten. »Heute will man mit oder auf verschlüsselten Daten rechnen.« Das wird etwa mit einer Methode namens »proxy re-encryption« möglich. »Damit kann man die Daten in der Cloud umschlüsseln, ohne dass man sie auspackt – zum Beispiel auf den Schlüssel eines Partners, an den man Daten weitergeben will, ohne dass die Cloud jemals die Klardaten gesehen hat«, erläutert Lorünser.

Eine andere Methode beruht auf der Dezentralisierung der Daten: Wenn man Daten in mehrere Teile aufteilt, sodass die einzelnen Teile keine Information enthalten, und die Teile auf verschiedene Server verteilt ablegt, bekommt man Sicherheit, ohne dass man einen expliziten Schlüssel hat. »Und man kann damit rechnen«, so Lorünser – das nennt man »multi-party computation«. So interessieren oft zum Beispiel nicht die einzelnen Datenpunkte von Messungen, sondern nur einzelne statistische Größen über eine gewisse Zeit oder auch aggregierte Werte. Dafür können zum Beispiel die Fragmente, die auf einzelnen Servern liegen, addiert werden, übermittelt wird nur das Ergebnis der lokalen Berechnung – und aus diesem kann man die ursprünglichen Daten nicht rekonstruieren. »Man möchte durch solche Verfahren der sogenannten homomorphen Verschlüsselung davon wegkommen, dass man alle Daten offenlegen muss, aber doch Teile der Daten oder Statistiken über die Daten zeigen kann.« Solche Verfahren können auch die Privatheit von Daten verbessern. Ein Beispiel: Wenn es etwa darum geht, Daten eines Schrittzählers am Handy an die Krankenversicherung zu übermitteln, so reicht für diesen Zweck die Offenlegung einer Monatssumme – die täglich zurückgelegten Strecken, aus denen man Rückschlüsse auf viele Faktoren des Privatlebens ziehen könnte, sind irrelevant.

Postquantenverschlüsselung

Während es beim dynamischen Teilen und Berechnen von verschlüsselten Daten also Fortschritte gibt, zeichnet sich am Horizont ein anderes, noch viel grundlegenderes Problem ab: Wann genau sich dieses Problem stellen wird, ist heute unbekannt – aber irgendwann in den nächsten Jahrzehnten werden Quantencomputer so leistungsfähig sein, dass sie auch abseits von Physiklaboren für praktische Zwecke eingesetzt werden können. Auf theoretischer Ebene wurden bereits einige Algorithmen für Quantencomputer entwickelt – etwa einer, der die Primfaktorenzerlegung

do something with them. “Today, we want to compute with encrypted data.” This becomes possible through a method called “proxy re-encryption,” which “allows data in the cloud to be re-encoded without unpacking—for example, to the key of a partner to whom the data is to be passed on without the cloud ever having seen the plain data,” Lorünser explains.

An alternative method is based on the decentralization of data: if data are so split up into several portions that the individual parts do not contain any information and are stored on different servers, you get security without data encryption. “And you can compute with them,” says Lorünser—it is called “multi-party computation.” So, for example, what is of interest in measurements often is not individual data points but a statistical value over a certain period of time. The fragments stored on any one server might be added up; what is transmitted is only the result—from which the original data cannot be reconstructed. “Such processes of so-called homomorphic encryption are used to move away from having to disclose all data, but to stay able to show parts of, or statistics about, the data.” Such methods can also improve data privacy. One example: when it comes to transmitting data from a smartphone step counter to a health insurance, giving a monthly total would suffice to serve the purpose—detailed daily distances covered, which would allow inferences to be drawn about many factors of the person’s private life, would be irrelevant.

Post-quantum encryption

So while there is progress being made in the dynamic sharing and calculation of encrypted data, another, more fundamental problem is on the horizon: when exactly this problem will actually kick in is yet unknown today—but at some point in the next decades, quantum computers will be so powerful that they can be used for practical purposes outside physics labs. At the theoretical level, a number of algorithms have already been developed for quantum computers—for example, one that takes considerably less time to do prime factoring or solve the discrete logarithm problem. As explained above, asymmetric encryption is based on the complex intricacy of such mathematical methods. And with asymmetric encryption being a central privacy technology of today’s Internet, the Internet itself is in jeopardy. What is more: all old data secured through asymmetric encryption in the past will then become accessible by attackers.

The answer that research has to offer is post-quantum encryption. The goal is to identify new mathematical problems that can be used to build asymmetric cryptographic techniques that are hard to solve for quantum computers. To be more precise: “We want to base cryptography on a different set of mathematical problems where we

und das Problem des diskreten Logarithmus in wesentlich kürzerer Zeit lösen kann. Wie oben erläutert, beruht die asymmetrische Verschlüsselung auf der Schwierigkeit solcher mathematischer Verfahren. Da die asymmetrische Verschlüsselung eine zentrale Technologie des heutigen Internets ist, ist damit auch das Internet selbst in Gefahr. Mehr noch: Auch alle alten Daten, die in der Vergangenheit per asymmetrischer Verschlüsselung gesichert wurden, werden dann für Angreifer lesbar.

Die Antwort der Forschung darauf heißt Postquantenverschlüsselung. Dabei geht es darum, neue mathematische Probleme zu finden, mit denen man asymmetrische kryptografische Verfahren bauen kann, die aber gleichzeitig für Quantencomputer schwer zu lösen sind. Genauer gesagt: »Wir wollen die Kryptografie auf andere mathematische Probleme gründen, von denen wir glauben, dass der Quantencomputer keine Beschleunigung bringt«, so Lorünser. Ideen dafür gibt es bereits – z. B. basierend auf Verfahren der Kodierungstheorie oder durch Anwendung von mathematischen Gittermethoden. Durchgesetzt hat sich davon aber noch keine. Viele der neuen Algorithmen wurden beim sogenannten NIST-Wettbewerb eingereicht und werden nun von Experten des US-amerikanischen National Institute of Standards and Technology sowie der weltweiten Community auf Herz und Nieren geprüft. Bis sich ein neuer Standard herauskristallisieren könnte, werden sicher noch Jahre vergehen, meint Lorünser. »Um Vertrauen aufzubauen, müssen die Verfahren intensiv untersucht werden.« Er erinnert daran, dass bei der Faktorisierung, die heute Standard ist, seit mehr als 50 Jahren versucht wurde, einen effizienten Algorithmus zu finden: Da kein deutlich schnelleres Verfahren zur Berechnung gefunden wurde, ist man sich bei diesem Verfahren heute relativ sicher. Ähnliches muss auch bei Algorithmen geschehen, die dann als »quantum-safe« gelten können, allerdings bleibt hier nicht so viel Zeit. In einem Punkt gibt Lorünser dabei bereits Entwarnung: Bei digitalen Signaturen seien schon gute und praktikable Lösungen gefunden worden.

Eine gänzlich andere Variante, um der Bedrohung der Verschlüsselung durch künftige Quantencomputer zu entgehen, ist der Schritt zurück zu symmetrischen Verschlüsselungsverfahren: Diese bleiben auch in Zeiten des Quantencomputers sicher (wenn sie komplex genug sind). Allerdings müsste dafür das Problem der Schlüsselverteilung gelöst werden – und dafür bietet sich eine andere Quantentechnologie an, die sogenannte Quantenschlüsselverteilung.

Doch auch wenn schließlich eine Postquantenverschlüsselung etabliert worden sein sollte, gilt es noch ein weiteres Problem zu lösen: Selbst wenn man alle alten Systeme auf die neuen Verfahren umgestellt hat, so muss danach auch sicher gestellt werden, dass keine alten Daten oder Kommunikationen mehr verfügbar sind. Und das ist im Zeitalter der Cloud eine große Herausforderung. ×

believe the quantum computer won't speed things up much," says Lorünser. There already are ideas for this—for example, methods of coding theory or mathematical grid methods.. However, none of them have yet become established. Many of the new algorithms were submitted to the so-called "NIST competition" and are now being put through their paces by experts from the US National Institute of Standards and Technology and the global community. It will for sure be years before a new standard is established, says Lorünser. "To build trust, processes must be thoroughly scrutinized." He points out that the factoring that is standard today has seen fifty years of trying to find an efficient algorithm: with no significantly faster computation method found, you can feel relatively sure about this procedure today. Something similar must be done with algorithms so that they can be considered "quantum-safe." But there is one point in which Lorünser is already able to give the all-clear: a replacement for digital signatures has already been found.

An entirely different way of avoiding the threat that future quantum computers pose to encryption altogether is taking a step back to symmetric encryption methods: these remain secure even in the age of quantum computers (provided they are complex enough). However, this requires solving the problem of the distribution of keys first—and here, another quantum technology is offering itself, so-called quantum key distribution.

But even once post-quantum encryption is finally established, another problem still remains to be solved: even if all old systems have been adapted to the new procedures, it must be ensured that no old data or communications are available. And that's a big challenge in the age of the cloud. ×

Sicherheit durch Naturgesetze

Die Quantenkryptografie soll in einigen Jahren eine völlig abhörsichere Kommunikation ermöglichen. Bei der Entwicklung dieser Technologie spielen Forscher aus Österreich in der ersten Liga mit.

Die Welt der Quantenphysik enthält vieles, was man sich nur sehr schwer vorstellen kann. Ein Prinzip ist das der Quantenverschränkung: Es besagt, dass zwei miteinander verschränkte Teilchen die exakt gleichen Eigenschaften haben – selbst dann, wenn sie sehr weit voneinander entfernt sind. Eine der Konsequenzen daraus ist nicht weniger verblüffend: Wenn man eines der verschränkten Teilchen verändert (was z. B. auch geschieht, wenn man dessen Eigenschaften misst), wirkt sich das sofort auf das zweite Teilchen aus. In der Physik ist dieses Phänomen – angelehnt an eine Bemerkung Albert Einsteins – als »spukhafte Fernwirkung« bekannt.

Auf dem Phänomen der Verschränkung beruhen zum Beispiel Quantencomputer, die derzeit in vielen Labors der Welt – auch in Österreich – entwickelt werden. Obwohl der Effekt schon Ende der 1960er-Jahre experimentell beschrieben werden konnte, dauerte es ein wenig länger, bis man vorschlug, damit auch Nachrichten sicher zu übermitteln. Die Grundidee dahinter ist folgende: Durch die Verschränkung zweier Teilchen lässt sich ein Kommunikationskanal aufbauen, bei dem man sofort bemerkt, wenn jemand Unbefugter bei einer Transaktion mithört. Damit ist die Kommunikation völlig abhörsicher. Überdies ist auch ein Kopieren von Nachrichten nicht möglich, weil man ein Foton nicht klonen (kopieren) kann.

Erste wissenschaftliche Veröffentlichungen mit konkreten Ideen wurden 1984 vorgestellt. Im Jahr 1989 folgten erste praktische Experimente, etwa beim damaligen Computerriesen IBM. In dieser Zeit begann sich auch der österreichische Quantenphysiker Anton Zeilinger – heute Präsident der Österreichischen Akademie der Wissenschaften – mit solchen Ideen der Quantenkommunikation zu beschäftigen. 1999 gelang es der Gruppe um Zeilinger erstmals, mithilfe von verschränkten Fotonen Schlüssel für eine symmetrische Kodierung auszutauschen; spätestens 2004 war dies über eine Entfernung von 600 Metern zwischen dem Wiener Rathaus und der damaligen Bank Austria-Creditanstalt möglich. Bei einer symmetrischen Verschlüsselung handelt es sich um ein Kryptografieverfahren, das de facto nicht zu knacken ist. Die Voraussetzung dafür ist freilich, dass der Austausch der Schlüssel nicht abgehört wird – wofür eben, wie bewiesen werden konnte, der quantenmechanische Effekt sorgen kann.

Security by Law of Nature

Quantum cryptography is expected to enable totally tap-proof communications within a couple of years from now. Researchers from Austria are at the forefront of the development of this technology.

The world of quantum physics contains many things that are difficult to imagine. One principle obtaining in it is that of quantum entanglement: it says that two entangled particles have exactly the same properties—even if they are very far apart. No less astounding is one of the consequences this has: if one of the entangled particles is modified (which happens, for example, when measuring its properties), it immediately affects the second particle. Based on a remark by Albert Einstein, this phenomenon is known in physics as the "spooky long-distance effect."

For example, the phenomenon of entanglement also makes the basis for quantum computers, which are currently being developed in many laboratories around the world —including Austria. Utilizing this effect for safe transmission of messages was first proposed at the end of the 1960s. The basic idea behind this is as follows: by entangling two particles, a communication channel can be established in which any attempt of unauthorized listening in on a transaction is noticed immediately. This makes communication completely tap-proof. Moreover, the copying of messages is not possible either because photons cannot be cloned (copied).

The earliest research publications with concrete ideas on how to apply this in practice were presented in 1984. First practical experiments followed in 1989, for instance, with then computer giant IBM. It was also the time when Austrian quantum physicist Anton Zeilinger—today President of the Austrian Academy of Sciences—also began to explore ideas of quantum communication. In 1999, Zeilinger's research group first succeeded in using entangled photons to exchange keys for symmetric coding; by 2004, this became possible over a distance of 600 meters. Symmetric encryption is a cryptographic process that can de facto not be cracked, provided, of course, that the exchange of keys itself is not eavesdropped on—which, as has been proven, can be secured using the quantum mechanics effect.

Verteilung von Quantenschlüsseln

Dass ein derartiger Quantenschlüsselaustausch mit verschränkten Fotonen (Quantum Key Distribution/QKD) auch außerhalb eines Physiklabors in realen Kommunikationsnetzen möglich ist, konnte im Rahmen des großen EU-Projekts SEQOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) gezeigt werden, in dem ab 2004 unter der Leitung des damaligen Austrian Research Center, dem Vorläufer des AIT, 41 Partner aus 12 Ländern kooperierten. 2008 gelang es schließlich, in einem rund 200 Kilometer langen Glasfasernetz mit mehreren Netzknoten innerhalb Wiens vertrauliche Daten zu übertragen und verschlüsselte Telefongespräche zu führen, die per Quantenkryptografie abgesichert waren. Die Methoden werden von Wissenschaftlern stetig weiterentwickelt. So ist es Zeilinger und seinen Kollegen im Jahr 2012 gelungen, per QKD abgesicherte Daten über einen Laserstrahl zwischen den kanarischen Inseln La Palma und Teneriffa (143 Kilometer) zu versenden. Ein weiterer Meilenstein wurde im Herbst 2017 genommen: Damals führte Zeilinger über einen chinesischen Satelliten ein durch Quantenkryptografie gesichertes Videotelefonat mit Kollegen an der Chinesischen Akademie der Wissenschaften in Peking.

Kleinere und billigere Geräte

Im Prinzip funktioniert dieses Verfahren also schon seit geraumer Zeit. Doch bis zur routinemäßigen Anwendung ist es noch ein weiter Weg. Denn die Technik dahinter ist extrem aufwendig, wie Hannes Hübel, Forscher am AIT Austrian Institute of Technology, erläutert. »Wir müssen einzelne Quantenzustände erzeugen, manipulieren und messen. Das ist insofern sehr schwierig, weil diese von der Umgebung sehr leicht beeinflusst werden. Man muss sie also sehr gut abschirmen.« Weiters müssen die Eigenschaften einzelner Fotonen gemessen werden. »Es gibt zwar heute Detektoren, die das mit einer Effizienz von fast 99 Prozent können. Das sind aber relativ große Aufbauten, bei denen flüssiges Helium eingesetzt wird«, so Hübel.

Bei einer Reihe von Projekten arbeiten die Forscher am AIT – so wie Kollegen einer Handvoll anderer Organisationen und Unternehmen auf der Welt – an Geräten, die deutlich kleiner und einfacher sind. »Wir bauen Prototypen, welche die gleiche Funktionalität wie große Laboraufbauten haben, aber auf einem optischen Chip integriert sind«, so Hübel. Das Ziel sind kleine und kompakte Endgeräte, die von jedem Nutzer, der über einen Glasfaseranschluss verfügt, problemlos verwendet werden können. Damit die Technologie tatsächlich in der Praxis Fuß fassen kann, spielen drei Faktoren eine Schlüsselrolle: die Robustheit, die Größe und der Preis der Geräte. »Wir versuchen, die technologische Komplexität möglichst zu reduzieren, Standardkomponenten zu benutzen und das Ganze robust, also langzeitstabil, zu gestalten.« Dazu muss auch jede Menge Elektronik und Steuersoftware entwickelt werden.

Quantum Key Distribution

The fact that quantum key transmission by entangled photons—Quantum Key Distribution (QKD)—is also possible in real communication networks outside a physics lab was demonstrated in a large-scale EU project entitled SEQOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography), with forty-one partners from twelve countries cooperating from 2004 under the lead of the then Austrian Research Center. In 2008, it finally became possible to transmit confidential data through an approximately 200-kilometer fiber optic network with several network nodes and to make encrypted telephone calls secured by quantum cryptography. The technology is constantly being further developed by scientists. In 2012, Zeilinger and his fellow scientists succeeded in sending QKD-secured data via laser beam back and forth between the Canary Islands of La Palma and Tenerife (143 kilometers). Another milestone was reached in fall 2017, when Zeilinger made a quantum cryptography secured video call with colleagues at the Chinese Academy of Sciences in Beijing over a Chinese satellite.

Smaller and cheaper devices

In principle, this procedure has been up and running for quite some time now. But there is still a long way to go for it to become a routine application. The technology behind it is extremely complex, as Hannes Hübel, researcher at the AIT Austrian Institute of Technology, explains. “We have to generate, manipulate and measure individual quantum states. This is very difficult because they are highly subject to environmental influences. So they need good shielding.” Furthermore, the properties of individual photons have to be measured. “There are detectors available today that do this with an efficiency of almost 99 percent. However, these are relatively large setups in which you have to work with liquid helium,” says Hübel.

Researchers at the AIT—like their colleagues in a handful of other organizations and companies around the world—are working in a number of projects on devices that are significantly smaller and simpler. “We build prototypes that have the same functionality as large lab setups, but are integrated on a single optical chip,” says Hübel. The goal is small and compact devices for unproblematic use by anybody with a fiber optic connection. In order for the technology to gain traction in practice, three factors play a key role: robustness, size, and device price. “We are trying to reduce technological complexity as much as possible, use standard components and make the whole thing robust, that is, long-term stable.” This also requires developing a lot of electronics and control software.

Bis das Ziel erreicht ist, gilt es noch viele technologische Hürden zu überwinden. Dazu zählen etwa durch Glasfasernetze bedingte Beschränkungen. Bei den in solchen Netzen verwendeten Wellenlängen liegt die Effizienz der Fotonendetektoren bei nur rund zehn Prozent. Das ist mit ein Grund dafür, dass die Übertragung von Photonen durch heutige Glasfasernetze nur über eine Distanz von 100 bis 200 Kilometern möglich ist, weil die Lichtsignale in den Glasfasern mit zunehmender Entfernung schwächer werden.

Zur Überwindung dieser Grenze werden mehrere Ansätze verfolgt, wie Hübel erläutert. Etwa der »trusted repeater approach«, bei dem es ungefähr alle 100 Kilometer einen vertrauenswürdigen Knotenpunkt gibt, der die Signale erneuert und dadurch quasi verstärkt. Ein Problem dabei ist, dass der Besitzer dieser Knoten Zugriff auf die Informationen hat. Das könnte freilich auch ein Vorteil dieser Methode sein, sofern der Knotenbetreiber wirklich vertrauenswürdig ist: Auf diese Art könnten Behörden zwecks Strafverfolgung oder zur Bekämpfung von Terrorismus Zugang zu verdächtigen Datenströmen erlangen. Das ist bei einem anderen Ansatz unmöglich, der 100-prozentige Abhörsicherheit garantieren würde: dem sogenannten Quantenrepeater. In diesem Fall werden nicht Quantenschlüssel verteilt und verstärkt, sondern die Verschränkungen selbst. Die Idee ist, dass an jedem Knotenpunkt erneut verschränkte Fotonen produziert werden; wenn dies entlang des gesamten Übertragungswegs geschieht, sind unterm Strich die Fotonen beim Sender und beim Empfänger miteinander verschränkt. Das würde ermöglichen, dass der zu übertragende Quantenschlüssel an keinem Punkt des Übertragungsweges vorhanden ist – und es daher auch grundsätzlich keine Möglichkeit gibt, den Schlüssel auf dem Weg anzugreifen. »Im Labor wurde bereits gezeigt, dass das funktionieren könnte. Der Nachteil ist allerdings, dass das fast so aufwendig ist wie der Bau eines Quantencomputers«, meint Hübel. »Das scheitert derzeit noch an der Technologie.«

Integration in bestehende IKT-Systeme

Eine andere Idee, die verfolgt wird, um die Quantenkryptografie praktikabel zu machen, heißt in der Fachsprache »CV-Ansatz«. Im Unterschied zur Messung »diskreter Variablen« (DV) mittels Einzelfotonendetektoren bei der herkömmlichen QKD werden dabei übliche Fotodioden verwendet, um kontinuierliche Variablen (CV) zu messen. »Das kann man recht einfach auf einem optischen Chip integrieren«, so Hübel. Die Forscher hoffen, durch diesen Ansatz die Endgeräte der Zukunft wesentlich kompakter und billiger zu machen. Überdies bietet diese Technologie die Möglichkeit, mehr Bits pro Lichtpuls zu übertragen. Hübel: »Mit CV-QKD versuchen wir, die Datenübertragungsrate um den Faktor 1000, also in den Megabit-Bereich, zu erhöhen.« Das ist freilich immer noch um den Faktor 1000 niedriger als die in heutigen IKT-Netzen gebräuchlichen Übertragungsraten.

To reach that goal, many technological hurdles still have to be overcome. These include, for example, limitations inherent in fiber optic networks themselves. With the wavelengths used in such networks, the efficiency of photon detectors is only around ten percent. This is one of the reasons why the transmission of photons through today's fiber optic networks is only possible over a distance of 100 to 200 kilometers, because light pulses in fibers become weaker with distance.

Several approaches are being pursued to overcome this limitation, Hübel explains. One is the "trusted repeater approach," with a trustworthy node approximately every 100 kilometers retransmitting, and thus virtually amplifying, the signal. One problem here is that the owners of these nodes have access to the information. This might, of course, also turn out to be an advantage of the method, provided that the node operator is really trustworthy: thus, authorities could gain access to suspicious data flows for purposes of prosecution or to combat terrorism. This is impossible with another approach that would guarantee 100 percent interception security: the so-called quantum repeater. In this case, it is not quantum keys that are distributed and amplified, but the entanglements themselves, the idea being that entangled photons are reproduced again and again at each nodal point; if this occurs along the entire transmission path, the result is that the photons at the sender and the receiver are entangled. It would allow for the quantum key to be transmitted not to be present at any point of the transmission path—which would basically leave no possibility to attack the key along the way. "Lab tests have already shown that this could work. The downside, however, is that it is almost as complex as building a quantum computer," Hübel says. "Currently, this still founders on technology."

Integration in existing ICT systems

Another idea currently pursued to make quantum cryptography viable is what is called the "CV approach" in tech jargon. In contrast to the measurement of "discrete variables" (DV) by means of single-photon detectors in conventional QKD, conventional photodiodes are used to measure "continuous variables" (CV). "Those can be integrated on an optical chip pretty easily," says Hübel. Researchers hope that this approach will make the terminal equipment of the future a lot more compact and affordable. Also, the technology offers the possibility of transmitting more bits per light pulse. Says Hübel, "With CV-QKD, we are trying to step up data transfer rates by a factor of 1000, that is, to the megabit range." Of course, that still is lower by a factor of 100 than the transfer rates that are common in ICT networks today.

Ein völlig anderer Weg, Distanzbeschränkungen durch Glasfasernetze ganz zu umgehen, ist die Satelliten-QKD. Dabei werden, wie oben bereits erwähnt, die Fotonen von einem Satelliten durch die Luft zu einem Empfänger am Boden übertragen. Dass das praktisch funktioniert, wurde mit dem Quantenvideotelefonat zwischen Wien und Peking erfolgreich demonstriert. Grundsätzlich könnte man über diesen Weg von allen Punkten der Erde aus sicher kommunizieren, an denen eine passende Bodenstation vorhanden ist. Allerdings können wegen der wechselnden Bewölkung nicht zu jeder Zeit Schlüssel erzeugt werden. Aufgrund der Luft- und Lichtverschmutzung in Städten können die Bodenstationen in den meisten Fällen nicht direkt bei den Sendern und Empfängern stehen, sondern etwa auf Bergen außerhalb der Ballungszentren – und die Daten müssen erst recht wieder lokal über Glasfasern weitergeleitet werden.

Aufbau einer europäischen Quantenindustrie

All diese Ideen sollen in dem 2018 gestarteten großen europäischen Quantum-Flagship-Programm weiterentwickelt werden, an dem österreichische Forscher etwa des AIT, der Universität Innsbruck und der Akademie der Wissenschaften – im Rahmen einer Reihe unterschiedlichster Projekte beteiligt sind. Parallel dazu plant die Europäische Weltraumagentur ESA Missionen, die Quantenkommunikation auch auf europäischen Satelliten realisieren – nachdem China jüngst sehr viel in diesen Bereich investiert hat.

Und: In den nächsten Jahren soll ein europäisches QKD-Testbed unter der Leitung des AIT aufgebaut werden, um die Technologie alltagstauglich und die User mit den Möglichkeiten vertraut zu machen. Auch die Einrichtung verschiedener realer Anwendungsfälle (etwa im Gesundheits- oder Energiebereich) ist geplant. Ebenso gezeigt werden soll, dass die Quantenkryptografie nahtlos in bisherige Systeme integriert werden kann. Zudem soll dadurch mittelfristig die Entwicklung eines Marktes für diese Technologie in Europa – inklusive eines ganzen Ökosystems europäischer Hersteller, Lieferanten, Verkäufer usw. – angestoßen werden. »Derzeit ist es für Produzenten schwer, in diesem Segment Fuß zu fassen, weil der Markt noch nicht da ist«, merkt Hübel an. Nachsatz: »Noch scheitert es am Preis, an der verfügbaren Übertragungsrate und an der Überzeugung, dass dieses System wirklich funktioniert und große Vorzüge hat.« ×

A totally different way of circumventing the distance limitations of fiber optic networks altogether is satellite QKD. Here, as mentioned before, the photon-borne information is transmitted over the air to a satellite, which then retransmits it to the desired receiver. The quantum video call between Vienna and Beijing successfully demonstrated that this works in practice. Basically, this channel would make secure communication possible from any point on earth where a suitable ground station is available. However, due to changes in cloud cover, communication is not possible at all times. And due to air and light pollution in cities, the ground stations can in most cases not be located directly with the senders and receivers but on mountains outside urban centers—meaning that data must again be locally retransmitted via fiber optics.

Building a European quantum industry

All of these ideas are to be further developed in the major European Quantum Flagship initiative which was launched in 2018 and in which Austrian researchers—for example, from the AIT, the University of Innsbruck, and the Academy of Sciences—are involved in a number of various projects. In parallel, the European Space Agency ESA is planning missions to implement quantum communication on European space satellites—an initiative that comes after China recently made huge investments in this area.

And: in the coming years, a European QKD testbed is planned to be set up in order to make the technology everyday useable and to make users familiar with the possibilities it offers. It is also planned to set up real use cases for various applications (e.g. in the health or energy sectors). Moreover, the intention is to demonstrate that quantum cryptography can be seamlessly integrated into existing systems. In the medium term, this is expected to prime the development of a market for this technology in Europe—including a whole ecosystem of European manufacturers, suppliers, vendors, etc. “Right now, it’s difficult for producers to get a footing in this segment because there’s no market yet,” Hübel remarks, adding: “It still is a nonstarter because of price, available transmission rates, and a lack of confidence that the system actually works and has great benefits.” ×

Wenn das System nicht »normal« läuft

Eine moderne Methode, um auch unbekannte Cyberangriffe erkennen zu können, ist die sogenannte Anomalieerkennung: Die Software lernt, wie sich ein IT-System normalerweise verhält, und schlägt Alarm, wenn es zu unerwarteten Systemzuständen kommt.

Absolute IT-Sicherheit gibt es nicht mehr. So lautete der Sukkus einer Veranstaltung im Rahmen der »Berlin Science Week«, die vom AIT, dem Austrian Institute of Technology, dem Complexity Science Hub (CSH) Vienna und der ETH Zürich im Herbst 2018 organisiert wurde. Drastisch drückte dies Martin Stierle (AIT) aus, der den »Krieg um die IT-Sicherheit« für verloren erklärte. »Wir versagen dabei, sichere Systeme zu produzieren. Es ist unmöglich.« Sichere IT-Systeme zu schaffen, um etwa kritische Infrastruktur zu schützen, mag daher ein hehres Ziel sein, ist aber nur mehr ein unzureichender Ansatz, so der Konsens der Vortragenden und Diskutanten.

Im Vordergrund steht also die Absicherung von IT-Systemen gegen Angriffe von außen. Seit vielen Jahren werden dafür Virenscanprogramme, Firewalls, Junkmailfilter usw. eingesetzt, die alle nach fest definierten Regeln funktionieren und eingreifen, wenn sie eine Bedrohung feststellen. Das Prinzip dahinter nennt man Blacklisting-Ansatz: Alles, was als »böse« bekannt ist, wird auf eine Liste gesetzt – und nach diesen Elementen wird gezielt gesucht. Das reicht nun allerdings nicht mehr aus, denn ständig tauchen bisher unbekannte Bedrohungen auf. Überdies werden mehrere Formen von Cyberattacken zunehmend zu sogenannten »advanced persistent threats« (APTs) gebündelt: Diese Angriffe sind wesentlich zielgerichteter und dauern typischerweise lange an. Dabei werden häufig unbekannte Sicherheitslücken ausgenutzt und neue Arten von Schadsoftware eingesetzt. Das wirft folgendes Problem auf: Was man nicht kennt, kann man auch nicht finden. Daher wirken herkömmliche Mittel nicht mehr; mit dieser Art von Bedrohung muss folglich ganz anders umgegangen werden.

Es brauche einen Paradigmenwechsel von der reinen Prävention zur schnellen Reaktion auf Cyberattacken, betonte Thomas Stubbings von der »Cyber Security Platform« (CSP) Österreich bei der Veranstaltung in Berlin. »Der Ansatz, Systeme einfach nur zu sichern, ist fehlgeschlagen.« Es gehe um eine neue Strategie: »Wir müssen das Spiel unserer Angreifer spielen«, erklärte Stubbings. Das bedeute, in Systeme zu investieren, die Attacken sofort identifizieren können und nicht erst, wenn es zu spät ist. Der strategische Vorteil liege naturgemäß immer außerhalb, fügte er hinzu: »Der Angreifer muss nur einmal richtigliegen, der Verteidiger die ganze Zeit.«

When the System Won't Function "Normally"

A modern method by which even unknown cyberattacks can be identified is called anomaly detection: software learns how an IT system behaves normally and sounds the alarm on unexpected system conditions.

Absolute IT security no longer exists. This was the gist of an event held during the "Berlin Science Week," which was organized by the Austrian Institute of Technology (AIT), the Complexity Science Hub (CSH) Vienna, and the ETH Zurich in fall 2018. Martin Stierle of the AIT put it drastically by declaring the "war over IT security" lost: "We fail to produce secure systems. It is impossible." Creating secure IT systems so as to protect, among other things, critical infrastructures might well be a noble goal, but has turned out an inadequate method, the speakers and panelists agreed.

The focus was thus on how to safeguard IT systems against attacks from outside. For many years, we have used virus scanners, firewalls, junk mail filters, etc., all of which function according to firmly defined rules and step in when detecting a threat. The principle behind this type of software is referred to as blacklisting: everything known as "bad" is added to the list—and searches then systematically watch out for these elements. Yet this no longer suffices, for previously unknown threats are constantly coming out. Moreover, multiple forms of cyberattacks are increasingly bundled to create so-called "advanced persistent threats" (APTs): these attacks are much more target-oriented and typically last for a long period of time. Frequently, they take advantage of unidentified security gaps and use new types of malware. This poses the following problem: what is not known cannot be found. Conventional means have therefore ceased to be effective; consequently, this type of threat has to be coped with completely differently.

A paradigm shift was needed, from pure prevention to a rapid response to cyberattacks, Thomas Stubbings of the "Cyber Security Platform" (CSP) Austria emphasized at the event in Berlin. "The approach according to which systems are simply secured has failed." A new strategy was called for: "We must play the game of our attackers," Stubbings declared. This meant investing in systems capable of identifying attacks immediately, not only when it was too late. Naturally, the strategic advantage always lies outside, he added: "The attacker has to hit the mark only once, the defender the whole time."

Die Methode, mit solchen Gefahren umzugehen, nennt man Anomalieerkennung. Die Basis dafür ist der sogenannte Whitelisting-Ansatz – der das genaue Gegenteil des oben genannten Blacklisting-Ansatzes ist. »Wir setzen alles, was wir für gut halten, auf eine Liste und gehen davon aus, dass alles, was nicht auf dieser Liste steht, böse ist«, erläutert Florian Skopik, Sicherheitsforscher am AIT. Die Kunst besteht nun darin, eine entsprechende White List zu erstellen. Oder anders formuliert: Wie kann man feststellen, was in einem IT-System »normal« ist, was also als gutes, erwartetes oder geduldetes Verhalten anzusehen ist – und wo man die Grenze zu einem Zustand zieht, der problematisch ist.

Dazu werden Methoden der künstlichen Intelligenz eingesetzt. »Wir haben Algorithmen, die durch Beobachtung lernen, wie ein System normalerweise verwendet wird«, so Skopik. Das geschieht auf einer sehr tiefen technischen Ebene, etwa bei den Logdateien, die widerspiegeln, welche Ereignisse in einem System auftreten – ob und wann eine Verbindung aufgebaut wird, ein Dokument abgerufen wird oder sich ein bestimmter Benutzer authentifiziert. Diese Ereignisse seien üblicherweise verkettet, erläutert Skopik und nennt ein Beispiel: Der Benutzer X greift normalerweise nie auf mehr als drei bis fünf Dokumente zu, und das immer zur normalen Geschäftszeit. »Das kann man beobachten: Durch maschinelles Lernen kann man herausfinden, was das normale Verhalten ist. Abnormal wäre es hingegen, wenn der Benutzer X um drei Uhr in der Früh auf einmal 100 Dokumente abruft.« Das muss alles extrem schnell ablaufen: »Bei einem mittelgroßen Unternehmen gibt es 7000 bis 10.000 Events pro Sekunde.«

Der Pferdefuß: viele Fehlalarme

Bei der Anomalieerkennung sagt man also der Software: Berichte mir alles, was abnormal ist. Und das System antwortet: Hier ist ein Ereignis aufgetreten, das ich so nicht erwartet hätte. Klingt nach einem perfekten System. Doch: »Die Sache hat einen Pferdefuß: Man bekommt so auch viele Fehlalarme. Denn sobald etwas nur geringfügig anders ist – wenn z. B. ein Update ausgeführt oder ein neuer Prozess ausgerollt wurde –, hat man schon eine Abweichung. Und man weiß nicht, ob diese Abweichung gewollt ist oder einen Angriff darstellt«, so Skopik. An diesem Punkt geht dann die Arbeit erst so richtig los – denn hier kommt der Mensch ins Spiel: Experten müssen jeden einzelnen Alarm evaluieren, herausfinden, was die Ursache war, und dann entscheiden, ob es sich um ein wirkliches Problem handelt. Zudem kommt es oft vor, dass zwei Ereignisse zwar statistisch miteinander korrelieren, es aber trotzdem keinen kausalen Zusammenhang gibt. Auch das muss im Zweifelsfall von Menschen entschieden werden – und zwar rasch.

Das größte Forschungsthema im Zusammenhang der Anomalieerkennung ist daher die Entwicklung von Algorithmen, die möglichst akkurate Alarme liefern. »Das funktioniert sehr gut bei Systemen, die

The method of dealing with such dangers is referred to as anomaly detection. It is based on the so-called whitelisting approach—the exact opposite of the blacklisting approach described earlier. "We put everything we deem good on a list and start out from the assumption that everything that is not on this list is bad," AIT security researcher Florian Skopik explains. The trick is to compile an adequate whitelist. Or, to put it differently: how can one define what is "normal" in an IT system, i.e., what can be considered good, expected, or tolerated behavior—and where do we have to draw a line to states that are problematic.

For this, researchers resort to methods of artificial intelligence. "We have algorithms learning through observation how a system is normally used," Skopik says. This happens very deep down on a technical level, such as in log files, which mirror what events occur in a system—if and when a connection is set up, a document is retrieved, or a particular user authenticates him- or herself. These events are usually linked, Skopik points out, giving an example: Normally, user X never accesses more than three to five documents and always does so during regular office hours. "This is what can be observed: normal behavior can be defined through machine learning. It would be abnormal, if user X suddenly retrieved 100 documents at three o' clock in the morning." All this has to proceed extremely fast: "In a medium-sized enterprise there are 7,000 to 10,000 events per second."

The drawback: many false alarms

In anomaly detection, the software is thus instructed to report everything that is abnormal. And the system responds: an event has occurred here that I did not expect to happen the way it did. Sounds like a perfect system. But: "The drawback is that you also get many false alarms. For as soon as something is only a little bit different—for example, an update is being carried out or a new process has been started—a deviation is diagnosed. And you have no idea if this deviation is something that has been intended or represents an attack," Skopik explains. At this point, the work proper starts—and humans come into play: experts have to evaluate every single alarm, find out how it has been caused, and decide then if a serious problem is involved. It also frequently happens that two events correlate statistically, but there is nevertheless no causal connection between them. In cases of doubt, this is another thing that has to be decided by humans—and quickly at that.

The most important field of research in the context of anomaly detection is therefore the development of algorithms supplying alarms that are as accurate as possible. "This works extremely well in systems accessed only by a limited number of users. For example, the method is

von nur wenigen Akteuren genutzt werden. Gut einsetzbar ist die Methode zum Beispiel bei Smart Grids und anderen komplett automatisierten Steuernetzen, in denen es strikte Abläufe gibt.« Wo hingegen viele Menschen am Werk sind, gibt es auch viele unerwartete Aktionen und Systemzustände.

Wegen des hohen Aufwandes, der getrieben werden muss, ist die Anomalieerkennung eher für die Großindustrie interessant und weniger für kleinere Unternehmen, für die der Aufwand größer scheint als der Schaden, der entstehen könnte. Von entscheidender Bedeutung können diese Systeme in Hochsicherheitsbereichen und bei kritischen Infrastrukturen im staatsnahen Bereich sein, wo der Schaden immens hoch sein kann – etwa bei einem kompletten Stromausfall, der, wenn er länger andauert, auch Menschenleben gefährdet. ×

suitable for smart grids and other fully automated control networks in which processes are strictly regulated." However, where many people are at work there also occur many unexpected actions and system statuses.

Because of the huge input of resources required, anomaly detection is more or less only interesting for big industries rather than for smaller enterprises, for which the costs seem higher than the damage that might be caused. Such systems have turned out to be of vital significance in high-security areas and critical infrastructures in spheres close to the government, where the damage can be enormous— such as in the case of a complete power blackout lasting for an extensive period of time and also jeopardizing the lives of humans. ×

Forensik im Darknet

Im Rahmen des großen EU-Projekts TITANIUM werden Hightechmethoden entwickelt, mit denen man Cyberkriminellen im Bereich von Kryptowährungen wie etwa Bitcoin auf die Spur kommen kann.

Das Darknet – jener Teil des Internets, in dem Nutzer ihre Identität mittels spezieller Browser und Netzwerke wirksam verschleiern – gilt als Zone des Zwielichts: Einerseits kann es, wenn öffentliche Debatten unterdrückt werden, einen geschützten Raum für freie Meinungsäußerung bieten. Andererseits schafft es ideale Bedingungen für schwerwiegende kriminelle Aktivitäten, etwa für Waffen- und Drogenhandel, Kinderpornografie und Auftragsstraftaten. Die Aufdeckung solcher Aktivitäten ist für Polizei und Justiz eine enorme Herausforderung.

Hier setzt das von der Europäischen Kommission eingerichtete Forschungsprojekt TITANIUM (Tools for the Investigation of Transactions in Underground Markets) an. In dem vom AIT Austrian Institute of Technology koordinierten Projekt arbeiten 15 Forschungseinrichtungen, IT-Unternehmen und Polizeibehörden aus sieben europäischen Ländern daran, neue forensische Technologien zur Ermittlung und Erforschung von Cyberkriminalität im Darknet zu entwickeln – unter ihnen so renommierte Partner wie Interpol oder das Karlsruher Institut für Technologie (KIT).

Ziel des im Mai 2017 gestarteten dreijährigen Projekts ist die Entwicklung von Software zur Unterstützung polizeilicher Ermittlungen im Darknet. Im Zentrum steht die Abwicklung krimineller Geschäfte mithilfe blockchainbasierter Kryptowährungen wie etwa Bitcoin, Monero, Ethereum oder Zcash: Erpressungen mit Ransomware (Verschlüsselungstrojanern) oder die zunehmende Marktkonzentration bei »Mining Pools«, die ab 50 Prozent problematisch ist, weil dadurch das Risiko einer nicht mehr kontrollierbaren Übernahme ganzer Blockchainsysteme steigt. Die globale Verfügbarkeit und vermeintliche Anonymität virtueller Währungen ist ein treibender Faktor für verschiedenste Delikte im Bereich der Internetkriminalität.

Im TITANIUM-Konsortium werden neue Methoden und Software-Tools zur Unterstützung elementarer Ermittlungsschritte entwickelt, die es ermöglichen sollen, gerichtsfestes Beweismaterial zu generieren: Das ist der Kern jeglicher Forensik – sei es in der Gerichtsmedizin, der Ballistik, bei Fingerabdrücken oder eben in der Cyberwelt. Voraussetzung dafür ist, dass die Behörden ihre Vorgangsweise bei der Datenanalyse und -auswertung genauestens dokumentieren, um im Sinn des in Europa etablierten rechtsstaatlichen Prinzips eine gerichtssichere Beweisführung vorlegen

Dark Net Forensics

The major EU project TITANIUM is concerned with developing high tech methods with which cybercriminals in the area of cryptocurrencies such as Bitcoin can be tracked down.

The Dark Net, that part of the Internet in which users effectively conceal their identity by means of special browsers and networks, is considered a twilight zone: while it may offer a protected space for freedom of expression when public debates are suppressed, it also creates ideal conditions for serious criminal activities such as arms and drug trafficking, child pornography, and contract crimes. Detecting such activities presents an enormous challenge for both the police and the judiciary.

This is where the research project TITANIUM (Tools for the Investigation of Transactions in Underground Markets) set up by the European Commission comes in. Coordinated by the AIT Austrian Institute of Technology, this project combines the efforts of fifteen research institutions, IT companies, and police authorities from seven European countries aimed at coming up with new forensic technologies for investigating and researching cybercrime in the Dark Net. The participants include such renowned partners as Interpol or the Karlsruhe Institute of Technology (KIT).

The three-year project that started in May 2017 intends to develop new methods and software tools to support police investigations in the Dark Net. The focus is on criminal business processes using blockchain-based cryptocurrencies such as Bitcoin, Monero, Ethereum, or Zcash: blackmail with ransomware (encryption Trojans) or the increasing market concentration in “mining pools,” which is problematic from 50 percent upward because this increases the risk of an uncontrollable takeover of entire blockchain systems. The global availability and supposed anonymity of virtual currencies is a driving factor for a wide variety of cybercrimes.

The TITANIUM consortium is developing software to support elementary investigation steps, which should make it possible to generate evidence that will stand up in court. This is the core of all forensics—be it in medicine, ballistics, in the field of fingerprints, or in the cyberworld. The prerequisite for this is that the authorities document their approach to data analysis and processing with the utmost accuracy in order to be able to present evidence that is secure in court

zu können. Ein zweiter Schwerpunkt des Projekts liegt auf der Analyse von Darknet-Plattformen, die für illegale Aktivitäten genutzt werden.

Das Kernstück des Forschungsvorhabens ist ein System, das vor einigen Jahren am AIT entwickelt wurde. Es nennt sich »GraphSense« und ermöglicht die Analyse von Geldflüssen in Kryptowährungssystemen.

Im Rahmen von TITANIUM werden nicht nur Methoden und Tools entwickelt, sondern gleichzeitig erforscht, wie diese unter Berücksichtigung ethischer Grundsätze und datenschutzrechtlicher Bestimmungen für forensische Zwecke eingesetzt werden. Es wurden von Anfang an vielfältige Schutzmaßnahmen implementiert (»Privacy by Design«), um eine angemessene und rechtmäßige Datenverarbeitung zu garantieren. Außerdem gibt es eine klare Trennlinie zwischen involvierten Forschungsorganisationen und mitwirkenden Strafverfolgungsbehörden bzw. künftigen Bedarfsträgern.

Im Jänner 2019 startete mit den »Field Labs« die erste Praxisphase des Projekts. Mehrere Monate lang wurde die entwickelte Software von Polizeibehörden in Österreich, Deutschland, Finnland und Spanien getestet. Rund 60 Cybercrimeexperten wurden über die Entwicklungen im Rahmen des Projekts informiert und in den Umgang mit den neuen Programmen eingeführt. Von der polizeilichen Erprobung erhoffen sich die TITANIUM-Partner wertvolle Rückmeldungen zu Bedienbarkeit, Funktionalität und Effizienz der Software. Eine zweite »Field-Lab«-Phase zur Erprobung weiterer Software ist für Ende 2019 angesetzt. ×

https://titanium-project.eu

in accordance with the principle of the rule of law established in Europe. A second focus of the project is the analysis of Dark Net platforms used for illegal activities.

The core of the research project is a system that was developed at the AIT a few years ago. This system called “GraphSense” makes it possible to analyse flows of money in crypto currency systems.

TITANIUM not only develops methods and tools, but also explores how they are used for forensic purposes, taking account of ethical and privacy provisions. This is why various protective measures were implemented from the outset (“privacy by design”) in order to ensure appropriate and lawful data processing. There is a clear dividing line between involved research organizations and participating law enforcement authorities or future users.

The first practical phase of the project started in January 2019 with so-called Field Labs. The developed software was tested by police authorities in Austria, Germany, Finland, and Spain for several months. About sixty cybercrime experts were informed about the developments of the project and introduced to the implementation and application of the new programs. The TITANIUM partners hope that the police testing will provide valuable feedback on the usability, functionality, and efficiency of the software. A second field lab phase for testing further software is scheduled for the end of 2019. ×

https://titanium-project.eu

Üben in der Cyberrange

Simulationssysteme ermöglichen ein realitätsnahes Training von Maßnahmen gegen Cyberangriffe.

Organisationen und Unternehmen stehen heute vor vielen unterschiedlichen Herausforderungen. Durch die fortschreitende Digitalisierung und Vernetzung werden alle Systeme zusehends komplexer, ständig kommen neue Technologien (etwa Kryptowährungen) zur Anwendung, und laufend ergeben sich neue rechtliche Anforderungen (etwa durch die Datenschutzgrundverordnung, DSGVO). »Heute ist immer mehr Wissen notwendig, um die eingesetzten Systeme zu beherrschen, und es gibt zahlreiche neue Bedrohungen, die Organisationen herausfordern können. Da muss viel Wissen und Praxis angelernt werden«, sagt Maria Leitner, Forscherin am AIT Austrian Institute of Technology.

Viele Unternehmen und Organisationen bereiten sich auf ein breites Spektrum von Eventualitäten vor: Sie setzen sich mit Prozessen und Abläufen für Entscheidungen auseinander, die getroffen werden müssen, wenn kritische Situationen eintreten. Solche Konzepte auf dem Papier auszuarbeiten ist aber etwas ganz anderes, als diese dann im Ernstfall in die Praxis umzusetzen. »Wir wollen den Umgang mit neuen Bedrohungsszenarien in der Cyberrange trainieren und testen können«, so Leitner. Eine Cyberrange ist eine virtuelle Testumgebung, in der ein reales System (z. B. ein IT-System, eine Produktionsanlage oder ein Kraftwerk) simuliert wird und man Abläufe und Aktionen durchspielen kann. Mit einer Cyberrange können die eigenen Cyberskills – also die Fähigkeiten, mit Bedrohungen der IT-Sicherheit umzugehen – ausprobiert und trainiert werden. »Man kommt oft erst dahinter, welche Kenntnisse oder Fähigkeiten Mitarbeiter noch brauchen, wenn man eine reale Situation durchspielt«, so Leitner. Man geht Schritt für Schritt verschiedene Situationen durch und überlegt, wie man die sich stellenden Herausforderungen lösen kann. Dadurch kann man Strukturen und Prozesse analysieren und eruieren, welche Auswirkungen verschiedene Handlungen und Reaktionen haben. Und: Man kann auf diese Weise üben, wie die Zusammenarbeit zwischen verschiedenen Beteiligten funktioniert.

Erstmals im großen Stil durchgespielt wurde ein solcher Bedrohungsfall beim vierten Planspiel des Kuratoriums Sicheres Österreich (KSÖ) im Jahr 2017: Dabei ging es darum, simulierte Cyberangriffe auf kritische Infrastrukturen zu erkennen, abzuwehren und an die zuständigen Behörden zu melden, die wiederum für die einzelnen Organisationen relevante Handlungen setzten. Die Experten des AIT haben dafür eine Cyberrange entwickelt, die industrielle Steueranlagen simuliert und alle relevanten technischen und

Practicing at the Cyberrange

Simulation systems facilitate the training of measures against cyberattacks under conditions close to reality.

Nowadays, organizations and companies face many different challenges. Through progressing digitization and networking, no matter what systems have become increasingly complex; constantly, novel technologies (such as cryptocurrencies) are employed; and new legal requirements (such as the General Data Protection Regulation, GDPR) have to be met. “Today, more and more knowledge is needed to master the systems in use, and there are many new threats that can challenge organizations. Therefore a lot of knowledge and practice has to be learned,” says Maria Leitner, researcher at the AIT Austrian Institute of Technology AIT.

Many companies and organizations prepare themselves for a broad spectrum of eventualities: they deal with processes and procedures for decisions that have to be made in order to cope with critical situations. However, formulating such concepts on paper is entirely different from putting them into practice in an emergency. “We want to train and test how to tackle these new threat scenarios at the cyberrange,” Leitner adds. A cyberrange is a virtual test environment where a real system (e.g. an IT system, a production plant, or a power plant) can be simulated, and where procedures and actions can be played out. In a cyberrange you can try out and practice your cyberskills—abilities enabling you to cope with threats to IT security—at a cyberrange. “Frequently, you only realize what knowledge and expertise your employees need to develop when you simulate a real situation,” Leitner points out. You go through various situations step by step and think about possibilities how to solve the challenges you are confronted with. In this way you can analyze structures and processes and find out what impact various actions and reactions can have. In this way you can also put the cooperation amongst a number of stakeholders to the test.

The case of such a threat was played through for the first time on a larger scale during the fourth simulation game of the Kuratorium Sicheres Österreich (KSÖ) in 2017: the plan was to identify and repel simulated cyberattacks to critical infrastructures and report them to the competent authorities, which in turn took relevant action for the individual organizations concerned. For this, the AIT experts developed a cyberrange, which simulates industrial control systems while

rechtlichen Anforderungen beinhaltet. Für den Ablauf des Planspiels wurde ein exaktes Drehbuch mit verschiedensten Angriffsszenarien erstellt.

Zwei Tage lang haben rund 200 Teilnehmer in zehn Teams eine realistische Situation durchgespielt. Geübt wurden dabei auch Entwürfe der geplanten Vorschriften wie die NIS-Richtlinie der EU (Netzwerk- und Informationssicherheit) sowie die DSGVO (Datenschutzgrundverordnung). Bei der NIS-Richtlinie sind unter anderem Meldepflichten von Betreibern wesentlicher Dienste an die zuständigen Stellen vorgesehen, die dann ihrerseits koordinierend und helfend tätig werden. Ein wichtiger Aspekt im Planspiel war, dass die handelnden Personen aus den zahlreichen verschiedenen Unternehmen und Organisationen einander kennenlernten und sich mit organisationsübergreifenden Kooperationsformen vertraut machten. »Informationen auszutauschen ist der beste Weg, um mit solchen Vorfällen fertigzuwerden«, fasst Maria Leitner zusammen.

Die Einsatzgebiete solcher Cyberranges sind sehr vielfältig. Das AIT entwickelt z. B. gemeinsam mit der Internationalen Atomenergiebehörde IAEA im Rahmen des Projekts SIREN ein Simulationsmodell für die Steuerung eines kritischen Teils von Atomkraftwerken, an dem Sicherheitsübungen durchgeführt werden können. Ziel des Projekts ist die Förderung des internationalen Informationsaustausches sowie eine gezielte Erarbeitung von speziellen Weiterbildungsmaßnahmen und Trainingskonzepten rund um das Design und den Betrieb von Steuerungsanlagen in Atomkraftwerken, um künftigen Cyberbedrohungen effektiver entgegentreten zu können.

Ein anderes aktuelles Beispiel ist das Projekt ACCSA (Austrian Cyber Crises Support Activities), in dessen Rahmen ein System konzipiert wird, mit dem Training und Großübungen für den Fall einer Cyberkrise durchgeführt werden können – analog zu klassischen Großübungen im Krisen- und Katastrophenmanagement. Für alle relevanten Akteure werden umfangreiche Schulungs-, Übungs- und Auswertekonzepte erarbeitet, die darauf abzielen, Reaktionszeiten und Fehlerraten im Fall einer Cyberkrise zu verringern. Die Ergebnisse des Projekts sollen nach dessen Ende zielgruppenspezifisch weiterentwickelt werden und neben der Verwertung durch die beteiligten Bedarfsträger mittelfristig auch zu neuen Geschäftssegmenten bei den beteiligten Wirtschaftspartnern führen. ×

considering all the relevant technological and legal requirements. A precise script comprising diverse attack scenarios was drawn up for this simulation game.

For two days, some 200 participants acted out a realistic situation in ten teams. The provisions of the EU's NIS Directive (on network and information security) and new data protection rules were also taken into account. The directive obliges operators of critical infrastructures to report incidents to the competent agencies, which in turn will take coordinating and supporting action. An important aspect of the simulation game was for the various players from a number of different companies and organizations to meet and familiarize themselves with inter-organizational forms of cooperation. "Exchanging information is the best way to cope with such incidents," Maria Leitner sums up.

The application areas of such cyberranges are manifold. For example, together with the International Atomic Energy Agency (IAEA), the AIT, within the framework of the project SIREN, developed a simulation model suited for holding security exercises for the control of a critical part of nuclear power plants. Goals of the project are the facilitation of an international exchange of information and a systematic development of specific abilities and training concepts regarding the design and operation of control systems in nuclear power plants so as to be able to counteract future cyberthreats more effectively.

Another relevant example is the project ACCSA (Austrian Cyber Crises Support Activities), in the course of which a system has been conceived that lends itself to conducting large-scale exercises for the case of a cybercrisis—comparable to conventional exercises for the management of crises and catastrophes. Comprehensive training, practice, and evaluation concepts have been developed for all relevant stakeholders, aimed at minimizing response times and error rates in the case of a cybercrisis. At the conclusion of the project the findings are to be elaborated further with specific regard to the various target groups. In addition to being used by the participating stakeholders, in the medium term they should also lead up to new business segments among the economic partners involved. ×

Gefährdete Smart Grids

Zahlreiche Forschungsprojekte versuchen, kritische Infrastrukturen besser als bisher vor Angriffen zu schützen. Man setzt dabei an vielen Punkten gleichzeitig an – und vergisst auch auf Fragen des Datenschutzes und der Privatsphäre der Konsumenten nicht.

Herkömmlicherweise wurden Stromnetze im Wesentlichen nach bekannten Mustern gesteuert. Sowohl die Muster des Verbrauchs- als auch die Produktionskurve waren gut bekannt, bei erhöhtem Strombedarf wurden zusätzliche Kapazitäten hinzugeschaltet. Das hat sich drastisch verändert, seit immer mehr Strom aus erneuerbaren Energiequellen in die Netze eingespeist wird: Der Wind weht, wann er will, und der Ertrag von Photovoltaikanlagen fällt nur in den seltensten Fällen mit Stromverbrauchsspitzen zusammen. Um Stromnetze nicht zu überlasten, müssen sie wesentlich besser und feiner gesteuert werden als bisher – und das sollen sogenannte Smart Grids leisten: Elektrische Verteilsysteme werden digitalisiert, indem sie mit Informations- und Kommunikationssystemen gekoppelt werden. Netze werden mit einer Reihe von Sensoren ausgestattet (etwa in Trafostationen, bei Stromeinspeisern oder in Form von Smart Metern, d. h. intelligenten Zählern bei den Verbrauchern), die ständig Daten über den Zustand der Netze (Spannung, Frequenz usw.) liefern und in den Kontrollzentren für die Steuerung der Netze eingesetzt werden. Je nach Angebots- und Verbrauchslage werden Anlagen oder Speicher kurzfristig zu- oder abgeschaltet, ebenso – wenn möglich – Verbraucher (»demand management«).

Durch die Digitalisierung sollen Stromnetze zum einen größere Mengen von erneuerbaren Energien aufnehmen können und – trotz großer Schwankungen bei der Einspeisung – zuverlässig bleiben. Zudem lässt sich besser beobachten, wie Infrastrukturen arbeiten. Dieser Schritt schafft auch die technischen Voraussetzungen für neue Geschäftsmodelle in der Elektrizitätswirtschaft wie etwa für lokale Microgrids oder »virtuelle Kraftwerke«.

Technisch gesehen sind Smart Grids cyberphysische Systeme. Zusätzliche Schnittstellen zwischen physischer (Kraftwerke, Stromnetz) und virtueller Welt (digitale Systeme), die es bisher nicht gegeben hat, bringen allerdings auch neue Herausforderungen mit sich. Smart Grids können etwa zum Ziel von Cyberattacken werden. Cyberrisiken haben unmittelbare Auswirkungen in der physischen Welt. »Eine Cyberattacke hat das Potenzial, die Versorgung massiv zu stören, etwa Über-oder Unterspannung hervorzurufen oder sogar ein Blackout zu bewirken«, erläutert Paul Smith, Forscher

Smart Grids at Risk

Numerous research projects seek to improve the protection of critical infrastructures against attacks. The problem is approached from multiple perspectives—also taking into consideration issues of data protection and the privacy of consumers.

Conventionally, power supply systems used to be operated according to known patterns. Both the consumption and production curve patterns were well known and additional capacities were added in case of increased electricity demand. This has changed drastically since more and more electricity has been fed into the grids from sources of renewable energy: the wind blows at its own discretion, and only in the rarest of cases does the output of photovoltaic plants coincide with peak demands for electricity. In order to keep power grids from overloading, more fine-tuning and precision is required—a problem that is to be solved by so-called smart grids: electric distribution systems are digitized as they are interconnected with information and communication systems. The networks are furnished with a number of sensors (such as at transformer stations, in electric power feeders, or in the form of smart meters in consumers' households) that constantly supply data on network conditions (voltage, frequency, etc.) and which are used at the control centers for adjusting the grids. Depending on supply and demand, power plants or energy storage facilities are connected or switched off, as are, if possible, consumers (demand management).

Thanks to digitization, networks should be able to take in larger quantities of renewable energies on the one hand and remain reliable despite substantial fluctuations in terms of energy fed into the grid on the other. Moreover, the system facilitates observations as to how infrastructures work. This development also creates the technological prerequisites for new business models in the power industry, such as local microgrids or "virtual power plants."

From a technological point of view, smart grids are cyberphysical systems. But additional interfaces between physical (power plants, electricity network) and virtual worlds (digital systems) that did not exist before pose new challenges. Smart grids, for example, can become the target of cyberattacks. Cyberrisks directly impact on the physical world. "A cyberattack has the potential to interfere with the supply severely, such as through over- or undervoltage, or even to cause a blackout," Paul Smith, researcher at the AIT Austrian Institute

am AIT Austrian Institute of Technology. Das ist auch schon des Öfteren passiert; so gab es z. B. im Dezember 2015 in der Ukraine einen kompletten Stromausfall, der (höchstwahrscheinlich) auf einen Cyberangriff zurückzuführen war.

Sicheres Design

»Ein System muss sicher gebaut sein«, so Paul Smith. In einem ersten Schritt betrachtet man die möglichen Auswirkungen einer Attacke und verknüpft diese mit der Wahrscheinlichkeit ihres Eintretens. »Beim Design eines Systems geht es darum, Bedrohungen mit großem Risiko zu berücksichtigen«, so der Forscher. Die Schwierigkeit bestehe darin, dass oft nicht offensichtlich ist, welche Konsequenzen ein Angriff hat. Solche Situationen gilt es daher in Computermodellen zu simulieren. Hat man die Risiken verstanden, erfolgt darauf aufbauend das Design des Systems. Dafür gibt es etablierte Standards (etwa der US-Behörde NIST oder europäischer Organisationen). Die Bandbreite reicht von der Einrichtung verschiedener Sicherheitszonen – damit ein Angriff nicht in andere Teile des Systems überspringen kann – bis zur Absicherung der Kommunikation.

In der RASSA-Initiative (Reference Architecture for Smart Grids in Austria) wurde in den vergangenen Jahren eine Architektur für sichere Smart Grids entwickelt. Unter Leitung der Technologieplattform Smart Grids Austria kooperierten u. a. Forscher des AIT und von Hochschulen in Wien, Linz und Salzburg mit Netzbetreibern aus Oberösterreich, Tirol und Kärnten sowie Anlagenbauern wie Siemens oder Alcatel-Lucent. Bei dem Projekt ging es darum, die bisher von verschiedenen Netzbetreibern entwickelten Lösungen für einzelne Teilaspekte zu einem kompatiblen Gesamtbild zusammenzuführen. Eine abgestimmte Gesamtlösung bietet eine geringere Angriffsfläche, sodass gezielte Cyberattacken (beispielsweise auf kritische Kontrollelemente mit unentdeckten Sicherheitslücken) leichter verhindert werden können.

Angriffe erkennen – und richtig darauf reagieren

Mit sachgerechtem Design ist es allerdings noch nicht getan. Denn wenn ein System in Betrieb ist, verändert es sich ständig. Dadurch ergeben sich laufend neue Angriffsflächen. »Man muss einen Angriff erkennen und entsprechend reagieren können«, so Smith. Deshalb wird das gesamte System ständig durch geeignete Sensoren überwacht: der Datenverkehr im Netzwerk genauso wie das Systemverhalten und die physikalischen Prozesse. »Solche Intrusion-Detection-Systeme sollen erkennen, wenn etwas Ungewöhnliches passiert.« Eingesetzt werden dafür u. a. Methoden des maschinellen Lernens; Lerndaten dafür werden aus Testbeds gewonnen. Das Problem dabei ist, dass es zu vielen falschen Alarmen kommt, sollen doch keine relevanten Ereignisse übersehen werden. Um die Anomalieerkennung zu optimieren, werden die Beziehungen zwischen den verschie-

of Technology, points out. There have been several such incidents so far; for example, in December 2015 there was a complete blackout in Ukraine, which was (with high probability) brought about by a cyberattack.

Secure design

"A system has to be built safely," says Paul Smith. In a first step, the possible impact of an attack is looked into and then linked to the probability of its occurrence. "What matters in the design of such a system is to take into account high-risk threats," the researcher explains—the difficulty being that the consequences of an attack are frequently not that obvious. It is therefore important to simulate such situations in computer models. Once the risks have been understood, the system can be designed accordingly. There exist established standards for this (such as those of the US agency NIST or European organizations). The spectrum ranges from the implementation of a number of security zones—so that an attack is prevented from switching to other system layers—to safeguarding communication technologies.

An architecture for secure smart grids was developed over the past years within an initiative called RASSA (Reference Architecture for Smart Grids in Austria). Under the auspices of the technology platform Smart Grids Austria, researchers of the AIT and of universities in Vienna, Linz, and Salzburg cooperated with network operators from Upper Austria, Tyrol, and Carinthia and with equipment manufacturers like Siemens and Alcatel-Lucent. The goal of the project was to bring together solutions for individual aspects developed by diverse network operators and create a compatible whole. A concerted overall solution has fewer points of attack so that it is easier to prevent targeted cyberattacks (for example, on critical control elements with undiscovered security gaps).

Identifying attacks—and responding appropriately

However, a proper design is not everything. For a system constantly responds to changes when operating, which results in ever-new points of attack. "An attack has to be identified so that one can respond appropriately," Smith says. This is why the entire system is continuously monitored with the proper sensors: this goes for the network's data traffic, system performance, and physical processes. "Such intrusion detection systems are expected to realize when something unusual happens." Among other methods, machine learning is used, with learning data gained from test beds. The problem is that it comes to many false alarms, as it is crucial not to overlook any relevant events. In order to optimize anomaly detection, relation-

denen Detektionssystemen modelliert und die Zusammenhänge zwischen Ereignissen in der physischen Domäne und Ereignissen in der Cyberdomäne genau analysiert. So versucht man, kausale Verbindungen zu finden und nicht rein mathematischen Korrelationen aufzusitzen. Die Herausforderung in der Praxis besteht darin, dass alles sehr schnell passieren muss: Sobald das System eine Anomalie meldet, muss man sich sofort auf die Suche nach der Ursache machen, um rasch die richtigen Entscheidungen treffen zu können.

»Hier gibt es immer einen Trade-off zwischen Safety und Security«, erläutert Smith. Manche Funktionalitäten, die für eine höhere Angriffssicherheit (Security) wichtig wären, sind der Betriebssicherheit (Safety) abträglich. Ein Beispiel: Unter Security-Gesichtspunkten sollte der Zugang zu einem Terminal für die Bedienung einer industriellen Steuerung beschränkt (etwa durch ein starkes Passwort geschützt) sein; aus Safety-Sicht braucht man hingegen einen guten Zugang. Verwendet man etwa in einem Dreischichtbetrieb regelmäßig wechselnde Passwörter, führt das meist dazu, dass diese auf ein Post-it notiert und auf den Monitor geklebt werden. »Beim Design muss man diese Spannung in den Griff bekommen«, so Smith. Erforderlich sei ein »Safety-Security-Co-Design«, das beide Aspekte bestmöglich berücksichtigt.

Die Reaktionsmöglichkeiten auf einen registrierten Cyberangriff sind bei industriellen Steuerungen keinesfalls trivial. »Das ist sehr herausfordernd: Man kann die Anlage nicht einfach abschalten, sondern muss alles im laufenden Betrieb machen«, erzählt Smith aus der Praxis. Daher ist die »digitale Forensik« – also die Suche nach der Ursache für eine Anomalie – im industriellen Bereich besonders wichtig. »Hier wird sehr viel geforscht«, so Smith. Das reicht hin bis zu Fragestellungen, ob und wie man ein Produktionssystem anpassen kann, um die schlimmsten Auswirkungen einer Cyberattacke zu vermeiden. Besonders heikel sind autonome Systeme, die sich selbst konfigurieren und regeln: Diese müssen bei Auftreten eines Problems in einem sicheren Modus betrieben werden, in dem sie allerdings nicht so effizient arbeiten.

Datenschutz und Privatheit

Neben solchen Herausforderungen stellt sich bei Smart Grids ein weiteres wichtiges Sicherheitsthema: Datenschutz. Die Betreiber von Smart Grids benötigen für den optimalen Betrieb ihrer Netze Verbrauchsdaten der Endverbraucher, die ihnen Smart Meters zugänglich machen. Aus diesen Verbrauchsdaten kann freilich viel herausgelesen werden: Man kann etwa ableiten, ob jemand zu Hause ist – eine für potenzielle Einbrecher sehr relevante Information. Weiß man, welche Elektrogeräte wann laufen, lässt das Schlüsse auf die Lebensgewohnheiten der Nutzer zu. Verbrauchsdaten verraten auch, wie effizient etwa ein Kühlschrank ist – ein Elektrohändler könnte aufgrund dieser Information den betreffenden Konsumenten gleich

ships between the various detection systems are modeled, and connections between events of the physical domain and events of the cyberdomain are thoroughly analyzed. In this way, one tries to find causal relationships instead of falling for purely mathematical correlations. In practice it is a challenge that everything must happen very fast: as soon as the system reports an anomaly one immediately has to go in search of the cause to be able to make the right decisions quickly.

"There is always a trade-off here between safety and security," Smith declares. Some of the functionalities, which would be important for more security, are detrimental to safety. An example: from a security point of view, access to an industrial control terminal should be restricted (for example, protected by a strong password); from a safety perspective, however, easy access would be decisive. Using regularly changing passwords in a three-shift system mostly leads to their being written down on Post-its attached to the monitor. "Design has to get a handle on this discrepancy," Smith says. According to him, a "safety & security co-design" taking into account both aspects is necessary.

When it comes to industrial control systems, the possibilities to respond to a registered cyberattack are by no means trivial. "This is extremely challenging: you cannot simply turn the plant off but are forced to do everything during full operation," Smith knows from practical experience. This is why a "digital forensic approach"—the search for the cause of an anomaly—is particularly crucial in the industrial sphere. "A lot of research is done here," Smith says. This goes as far as deciding whether or how production systems can be adjusted in order to prevent the worst consequences of a cyberattack. Autonomous systems configuring or controlling themselves are particularly sensitive: when a problem occurs, they must be operated in a secure mode in which they work less efficiently, however.

Data protection and privacy

In addition to such challenges, another important security issue manifests itself in the case of smart grids: data protection. For optimally running their networks, operators of smart grids need the data of end users, to which they gain access via smart meters. These user data in fact convey a great deal of information: one can deduce whether someone is at home—an extremely relevant piece of intelligence for potential thieves. Knowing which electric appliances are on at a particular hour permits conclusions regarding users' daily habits. As was shown by an experiment that became famous, one can even deduce the television program that is watched in a specific household at the moment. User data also tell how efficiently a fridge works—

ein Angebot für ein neues Gerät unterbreiten. »Alle diese Aspekte müssen berücksichtigt werden«, so Smith. Es gilt genau zu überlegen, wie oft Messdaten abgerufen werden, wie diese verschlüsselt und übertragen und wie lange sie gespeichert werden, usw. Je weiter die Entwicklung in Richtung Smart Homes (automatisierte Haushalte) geht, desto wichtiger wird es, im Hinblick auf das Verhältnis von Sicherheit und Privatsphäre die richtigen Entscheidungen zu treffen. ×

based on this piece of information, a dealer of electrical supplies could offer the respective consumers new appliances. “All of these aspects have to be considered,” says Smith.
It is necessary to find out how often performance data need to be retrieved, in what ways they should be encrypted, for how long they should be stored, etc. The further we proceed in the direction of smart homes, the more important it becomes to make the right decisions with regard to the relationship between security and private sphere. ×

Die Arbeit *This Much I'm Worth (The self evaluating artwork)* von Rachel Ara ermittelt den Wert der künstlerischen Arbeit auf der Metaebene: Algorithmen berechnen laufend ihren Verkaufswert anhand von Social Media, Kunstmarkt-Websites und Finanzmarktanalysen.

The work *This Much I'm Worth (The self evaluating artwork)* by Rachel Ara determines the value of artistic work at the meta-level: algorithms continuously calculate its sales value using social media, art market websites, and financial market analyses.

→ uncannyvalues.org

VIENNA BIENNALE FOR CHANGE 2019
Teil der Ausstellung
UNCANNY VALUES. Künstliche Intelligenz & du

Part of the exhibition
UNCANNY VALUES: Artificial Intelligence & You

CREDITS:
Exhibition view
UNCANNY VALUES. Artificial Intelligence & You
Rachel Ara, *This Much I'm Worth (The self-evaluating artwork)*, 2017

MAK Exhibition Hall
© Aslan Kudrnofsky, MAK

TEIL 3 / PART 3

Schlaglichter auf spezielle Themen

Special Themes in Focus

Sarah Spiekermann im Gespräch

»Am sichersten ist man, wenn man frei ist«

Die Wirtschaftsinformatikerin Sarah Spiekermann, die in ihrem kürzlich erschienenen Buch *Digitale Ethik* ein Wertesystem für das 21. Jahrhundert entwickelt, fordert, dass man den Risiken der Digitalisierung ins Gesicht sehen müsse – andernfalls richte man Unternehmen ebenso zugrunde wie persönliche Beziehungen.

In Ihrem Buch *Digitale Ethik* argumentieren Sie, dass die digitale Welt auf bestimmte Werte gegründet werden sollte. Warum müssen diese Werte Ihrer Meinung nach wieder wichtig werden?

Sarah Spiekermann: In jüngerer Vergangenheit hat man vor allem den Geldwert – sofern wir in diesem Fall überhaupt von einem Wert sprechen können – in den Vordergrund gestellt, Effizienz, Geschwindigkeit und Größe ins Zentrum gerückt. Das ist aber nur ein sehr reduzierter Ausschnitt dessen, worum es uns gehen sollte – gerade in Europa, wo traditionellerweise Werte der Freiheit, der Gleichheit (Respekt und Würde) und Brüderlichkeit (Gerechtigkeit, Fairness und Respekt) Vorrang hatten. Europäische Städte sind von Schönheit, von Gemütlichkeit, von Wohnlichkeit, von sozialer Gerechtigkeit geprägt. Das macht Europa ganz wesentlich aus und unterscheidet es von anderen Kulturen.

Aktuell steht der Wert der Sicherheit hoch im Kurs.

ss: Wenn Menschen feststellen, dass die Werte, an die sie sich gewöhnt und die sie schätzen gelernt haben, zugunsten von Profit, Effizienz und Geschwindigkeit wegbrechen, dann wird die Diskrepanz zwischen dem, was erwartet, und dem, was geschaffen wird, so groß, dass es zu einer Verunsicherung kommt. Jeder kann feststellen, dass das, was man sich wünscht, nicht mehr gegeben ist. Dadurch kommt es zu Unruhen in der Bevölkerung – man sieht das in Frankreich an der Gelbwesten-Bewegung, das äußert sich im Brexit, das macht sich in sozialen Netzwerken Luft.

Geboren 1973 in Düsseldorf, begann Sarah Spiekermann ihre berufliche Karriere in Unternehmen des Silicon Valley, wandte sich dann aber der Wissenschaft zu. Sie forschte und lehrte an der Carnegie Mellon University und an der Humboldt-Universität zu Berlin. Seit 2009 ist sie Professorin für Wirtschaftsinformatik an der Wirtschaftsuniversität Wien. Ihre Hauptforschungsgebiete sind ethische Fragen der Digitalisierung. Zuletzt veröffentlichte sie das Buch *Digitale Ethik. Ein Wertesystem für das 21. Jahrhundert* (Droemer). Sie berät zahlreiche Unternehmen und Organisationen, unter ihnen die EU und die OECD, und ist maßgeblich an der Ausarbeitung von Ethikstandards für Technikentwicklung durch das IEEE, den weltweiten Berufsverband von Ingenieuren, beteiligt.

An interview with Sarah Spiekermann

“You’re safest when you’re free”

Born in Düsseldorf in 1973, Sarah Spiekermann began her professional career in Silicon Valley companies before she turned to science. She researched and taught at Carnegie Mellon University and Berlin’s Humboldt University. Since 2009, she has been Professor at the Institute for Information Systems and Society, Vienna University of Economics and Business. Her main research areas are ethical questions of digitization. Most recently she published the book *Digitale Ethik. Ein Wertesystem für das 21. Jahrhundert* (Digital Ethics. A Value System for the Twenty-First Century, Droemer). She advises numerous companies and organizations such as the EU and the OECD and is significantly involved in the development of ethical standards for technology development by the IEEE, the worldwide professional association of engineers.

Business informatics professor Sarah Spiekermann, who develops a value system for the twenty-first century in her recently published book on digital ethics *(Digitale Ethik),* calls for facing up to the risks of digitization—otherwise, she says, businesses will be brought to ruin, as will personal relationships.

In your book on digital ethics you argue that the digital world ought to be based on certain values. Why must, in your opinion, these values be given importance again?

Sarah Spiekermann: In the recent past, it was mostly monetary value—if we can call it a value at all—that was in the foreground, with everything centered on efficiency, speed, and sheer size. But this only is a very reduced section of what should be important to us—particularly so in Europe where values of liberty, equality (respect and dignity), and fraternity (justice, fairness, and respect) were traditionally given predominance. European cities are characterized by beauty, homey comfort, livability, and social justice. This is what essentially defines Europe and distinguishes it from other cultures.

Right now, security is a particularly highly rated value.

ss: If people see that values they are accustomed to and appreciate are eroded and replaced by profit, efficiency, and speed, the discrepancy between what is expected and what is created becomes so big that it leads to insecurity and discomfort. Everybody can see that what you wish for is no longer available. This foments unrest—as can be seen in the Yellow Vests Movement in France, it finds expression in the Brexit, it is ventilated on social networks. Basically, these are insecurities ushered in by an extreme loss of values.

Im Prinzip handelt es sich um Unsicherheiten, die durch einen extremen Werteverlust mit eingeleitet wurden.

Verfolgt man das aktuelle politische Geschehen, stellt man fest, dass das Thema Sicherheit ungemein dominierend ist. Nehmen Sie das auch so wahr?

ss: Werte können auch missbraucht werden. Wir leben heute Statistiken zufolge in einer der sichersten Zeiten, die wir je hatten. Wenn man nun jemandem erzählt, er sei nicht sicher, legitimiert man damit einerseits Überwachungstechnologien und den weiteren Ausbau des Staates in Bereichen, die sich um die fiktive Unsicherheit kümmern müssten. Das ist Machtrhetorik. Andererseits sind wir durch die globale Überbevölkerung und die damit verbundenen Umweltprobleme tatsächlich in eine globale Schieflage geraten, die in eine Situation der Unsicherheit hineinführt. Diese Unsicherheit geht nicht auf das Konto einer machtpolitischen Institution, die gern Krieg spielt, sondern auf das von Waffenindustrien, die Geld damit verdienen, dass sie überall auf der Welt Kriege anzetteln. Der Finanzmarkt verdient zunächst einmal Geld damit, dass Waffen auf Kredit gefertigt und eingesetzt werden, und dann noch einmal beim Wiederaufbau. Der neoliberalistische Kapitalismus profitiert also vom Krieg, und es kommen kriegsspielende Fraktionen zum Zug, welche die globale Unsicherheit ganz massiv erhöhen. Diesen Fraktionen müsste man die Luft rauslassen. Das Urübel ist das heutige Finanzsystem. Wenn Staaten nicht alles durch Kredit finanzieren könnten, würden sie überlegen, in welche Bereiche sie investieren und in welche nicht. Dieses Agieren des Finanzsystems ist damit neben der Überbevölkerung und der Ressourcenknappheit der wesentliche Grund für die steigenden globalen Unsicherheiten.

Diese drei Faktoren – Überbevölkerung, Ressourcenknappheit und Finanzsystem – werden wir wohl kurzfristig nicht ändern können. Sie schlagen in Ihrem Buch einen anderen Weg vor.

ss: Es gibt einen vierten Faktor: die Digitalisierung. Das Digitale bringt Unsicherheiten mit sich, die es vorher nicht gegeben hat. Meiner Meinung nach sollte es hier – wie bei Medikamenten – eine Packungsbeilage geben, in der über Risiken und Nebenwirkungen aufgeklärt wird. Dazu gehört vor allem: Alles was digital abgebildet wird, ist

Following current political events, one realizes that the issue of security is incredibly dominant. Is this how you see it, too?

ss: Value can also be abused. According to statistics, we are living today in one of the safest times we've ever had. Now, if you keep telling people that they are not safe, you legitimate, for one thing, surveillance technologies and the further expansion of the state into areas that supposedly address those fictitious insecurities. This is the rhetoric of power. On the other hand, global overpopulation and the environmental problems it entails have brought us to a global imbalance that leads into a situation of insecurity. That insecurity is not the doing of some powerful political institution that likes war, but of arms industries that make money from inciting wars all over the world. The financial market makes money from the fact that weapons are manufactured, and deployed, on credit, and then from postwar rebuilding. Neoliberal capitalism thus profiteers from war, and there are war-mongering factions coming to the helm that massively increase global insecurity. These factions should be deflated. The arch-evil is today's financial system. If nation-states were not able to finance each and everything on credit, they would put more thought into which areas to invest in, and which not. The fact that the financial system acts this way is, apart from overpopulation and the shortage of resources, the central reason for the rising global insecurities.

These three factors—overpopulation, resource shortage, and the financial system—are something that we will probably not be able to do much about in the short term. In your book, you suggest a different path.

ss: There is a fourth factor: digitization. The digital brings along insecurities that did not exist before. In my opinion, it should come with a package insert—like drugs—that gives information on risks and side effects. This implies above all: anything that is digitally represented is error-prone—and highly so. If economic or social processes are completely digitally transformed, errors that we are not prepared for are introduced in those processes. We are relatively well-prepared to deal with human errors; those we

fehleranfällig – und zwar hoch fehleranfällig. Wenn man ökonomische oder soziale Prozesse vollständig digital transformiert, führt man in diese Prozesse Fehler ein, auf die wir nicht vorbereitet sind. Auf menschliche Fehler sind wir relativ gut vorbereitet, die kennen wir, wir wissen, was wir zu tun haben. Auf Maschinenfehler sind wir weit weniger gut vorbereitet. Das Digitale bringt noch eine zweite Unsicherheit in die Welt: Digitale Kommunikation ist immer asynchron. Man schreibt beispielsweise eine Nachricht, und irgendwann antwortet jemand darauf. Oft ist auch nicht ganz klar, was mit einer Nachricht genau gemeint ist, man kennt den Kontext nicht. Das führt auf individueller Ebene zu Unsicherheiten. Wenn man im Durchschnitt 130 Messages am Tag sendet und empfängt und das alle tun, dann ergibt das in der Masse eine massive Verunsicherung. Diese Unsicherheit liegt auf einer anderen Ebene als die zuvor genannten globalen Unsicherheiten. In historischen Zeiten hatten Menschen einen Rückhalt im Privaten: in der Familie, bei Freunden, in Vereinsstrukturen usw. Heute leben wir in einer seltsamen Zeit, in der wir auf der einen Seite globalen Unsicherheiten ausgesetzt sind und auf der anderen Seite der Rückzug ins Private hoch konfliktbeladen ist, weil er digital gestört ist.

Was kann man dagegen tun?

ss: In meinem Buch versuche ich, den Akteuren der Digitalisierung klarzumachen, dass sie ein Bewusstsein für bestimmte Werte aufbauen und in ihrem Leben und in ihren Unternehmen für die Entfaltung dieser Werte wieder Raum schaffen sollten. Eine bewusste Auseinandersetzung mit dem Wahren, Schönen und Guten erlaubt es, die Aufmerksamkeit von den Problemen weg und zu Lösungen hin zu lenken. Dazu gehört ganz maßgeblich der Wert der Gemeinschaft. Heute muss man immer erreichbar sein, das untergräbt Freundschaften. Wenn man sich wieder Zeit für Freunde nimmt und nicht mehr nur digital kommuniziert, kann man die Verunsicherung reduzieren und Rückhalt in der Wärme der Gemeinschaft finden, um diese politisch schwierigen Zeiten besser zu verkraften. Für Unternehmen bedeutet positives Wertdenken, sich ganz nüchtern der Digitalisierung zu stellen und zu fragen, welche Werte damit jenseits von Geld geschaffen werden können. Unternehmen sollten nicht so tun, als gebe es keine Risiken und Nebenwirkungen. Im Moment befinden

know, and we know what to do about them. But we are far less well-prepared for machine errors. The digital also bring another insecurity to the world: digital communication is always asynchronous. For example, you write a message, and sometime later, somebody replies to it. Often, it is not quite clear what a message actually means, you lack context. At the individual level, this leads to insecurities. Now, if you send and receive, on an average, 130 messages per day, and everybody does the same, this adds up to massive mass insecurity. This type of insecurity occurs at a different level than the global insecurities mentioned before. In previous times, people found backing and support in their private lives: family, friends, social clubs, etc. Today, we are living in a peculiar time in which we are, on the one hand, exposed to global insecurities and, on the other, retreat into the private sphere that is highly conflict-ridden due to digital disturbance.

So what can be done to help that?

ss: In my book, I try to make it clear to the actors of digitization that they should build awareness for certain values and make room again in their private lives and businesses for these values to unfold. Consciously engaging with the True, the Good, and the Beautiful makes it possible to direct attention away from problems and toward solutions. This crucially involves the value of community. Today, you have to be reachable all the time, which undermines friendships. If you start taking time out for friends again instead of only communicating digitally, you can reduce insecurity and find some comfort in the warmth of community so as to be better able to cope with these politically difficult times. It takes facing up to the risks; otherwise, businesses will go to ruin, as will personal relationships.

One major issue addressed at this year's Forum Alpbach will, aside from security, also be liberty as a social value. In your view, are liberty and security opposites—or are they mutually contingent?

ss: Benjamin Franklin once said that "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

wir uns in einer riesigen Digitalisierungsblase, in der jeder von Digitalisierung spricht, ohne die Risiken und Nebenwirkungen zu hinterfragen. Die IT-Industrie verdient sehr viel Geld damit, dass wir Dinge so tun, wie wir das tun. Den Risiken muss man ins Gesicht sehen, sonst bleiben Firmen ebenso auf der Strecke wie persönliche Beziehungen.

Beim heurigen Forum Alpbach wird neben Sicherheit auch der Wert der Freiheit stark thematisiert. Sind Freiheit und Sicherheit Ihrer Meinung nach ein Gegensatzpaar – oder bedingen die beiden Werte einander?

ss: Benjamin Franklin hat einmal gesagt: Wer für ein kleines bisschen Sicherheit seine Freiheit opfert, hat weder die Freiheit noch die Sicherheit verdient. Meiner Erfahrung zufolge führt persönliche Unsicherheit dazu, dass man sich in den eigenen Freiheiten unnötig beschränkt. Wer unsicher ist, versucht alles, um es allen anderen immer recht zu machen. Was unsere Gesellschaft braucht, ist Mut: Die Gesellschaft muss verstehen lernen, dass es im menschlichen Leben niemals vollkommene Sicherheit gibt. Man kann das Leben nie ganz kontrollieren. Das Streben nach maximaler Sicherheit schränkt einen in seiner Freiheit ganz unnötig ein – und am Ende stellt man fest, dass das alles nichts gebracht hat. Ich bin überzeugt: Am sichersten ist man, wenn man frei ist. Weil man aus der Freiheit heraus Unsicherheiten am flexibelsten begegnen kann: Wenn man unfrei ist, kann man auf Unsicherheiten nicht spontan improvisierend reagieren.

Wie wichtig ist den Menschen heute der Wert Freiheit?

ss: Am Papier und historisch gesehen wird der Wert Freiheit sehr hochgehalten. Auch bei der Digitalisierung ist der amerikanische Wert freier Meinungsäußerung im Netz ein sehr hoher Wert. Auch die EU hat stark zu den Freiheiten ihrer Bürger beigetragen. Wir haben eine Freiheit, zu leben und zu denken, wie es sie in der Menschheitsgeschichte niemals zuvor gab. Gleichzeitig stehen wir an einem Punkt, an dem wir lernen müssen, mit der Freiheit richtig umzugehen. Vergessen wurde etwas, das im antiken Verständnis von Freiheit eine große Rolle spielte: das Richtige wollen können. Die eigene Freiheit hört dort auf, wo die Freiheit des anderen beginnt. Die Fähigkeit zur Freiheit ist etwas, woran man ein Leben lang arbeiten muss. Man muss sich stets dessen bewusst sein, dass man nicht das Recht hat, alles zu sagen und zu tun. Weil es

In my experience, personal insecurity leads to unnecessary self-imposed restriction of one's personal freedoms. Anybody who is insecure will do whatever it takes to suit everybody else. What our society needs is courage: society will have to learn to understand that in human life there is no such thing as complete security. You can never have full control over life. Striving for maximum security quite unnecessarily constricts one's freedom—and in the end you realize it didn't get you anywhere. I am convinced: you're safest when you're free. Because freedom allows for most flexibility to counter insecurities: If you're unfree you cannot respond to insecurities spontaneously and by improvisation.

How important is freedom as a value to people today?

ss: On paper, and in historical perspective, the value of freedom is highly appreciated. In the digital sphere, too, the American value of free speech on the net is a highly cherished value. The European Union also has done much to amplify its citizens' civil liberties. We are enjoying a freedom of thought and living like never before in human history. At the same time, we have gotten to a point where we have to learn how to make the right use of freedom. One point was forgotten that played a major role in the classical understanding of freedom: being able to want what is right. One's own freedom ends where the freedom of others begins. The capability for freedom is something you have to keep working on your whole life. You always have to be aware that you do not have the right to say and do just anything. Because there is something that is called community. This community is not regulated by the state but between human beings. And this interpersonal element is fundamentally dependent on how well or how badly people handle their freedom.

How can we get there as a society?

ss: Our present-day educational systems and family relations must be more about setting boundaries. The point is creating a more lasting awareness of where individual freedom ends. The attitude of the 1968 movement, which propagated unconditional liberty in all fields of life, poses a major problem to society

etwas gibt, was man Gemeinschaft nennt. Diese Gemeinschaft wird nicht vom Staat, sondern zwischenmenschlich geregelt. Und das Zwischenmenschliche ist fundamental davon abhängig, wie gut oder wie schlecht Menschen mit ihrer Freiheit umgehen.

Wie kommen wir als Gesellschaft dorthin?

ss: In den gegenwärtigen Bildungssystemen und familiären Verhältnissen muss vermehrt auf Grenzen abgestellt werden. Es gilt nachhaltiger bewusst zu machen, wo die eigene Freiheit aufhört. Die Haltung der 1968er-Bewegung, die eine unbedingte Freiheit in allen Bereichen des Lebens propagierte, ist für die Gesellschaft heute ein großes Problem – vom Zwischenmenschlichen in der Familie bis hin zu internationalen Konflikten. Für eine Weltbevölkerung von zehn Milliarden Menschen, die über Kulturen und Religionen hinweg stärker denn je vernetzt leben, ist es ganz wichtig zu wissen, wo die Freiheiten enden und wo die Grenzen verlaufen. Tugenden müssen wieder eine viel größere Rolle spielen. Das Bildungssystem muss Tugenden und Grenzen vermitteln.

Sie sprechen im Untertitel Ihres Buches von einem »Wertesystem für das 21. Jahrhundert«. Da stellt sich die Frage: Brauchen wir neue Werte, oder müssen die altbekannten Werte neu gewichtet werden?

ss: Ich baue hier auf einem fast vergessen Bereich der Philosophie auf, nämlich auf der sogenannten »materialen Wertethik«, wie sie 1913 von dem Philosophen Max Scheler beschrieben wurde. Diese erlaubt uns, über Werte, über die Werthaltigkeit der Welt und über die Bedeutung von Werten für unsere Handlungen ganz neu nachzudenken. Das Wertesystem für das 21. Jahrhundert wurde also in der ersten Hälfte des 20. Jahrhunderts ausgearbeitet – wir müssen es wiederentdecken und für unsere Welt fruchtbar machen. Das ist es, was ich in meinem Buch bezogen auf die Digitalisierung versuche. Dieses Wertdenken muss vor allem in die Geschäftsmodelle der Unternehmen Einzug halten.

Wie kann man dabei konkret vorgehen?

ss: Sowohl Unternehmen als auch Einzelpersonen müssen drei Schritte setzen, um zu einem wert*volleren* Leben zu gelangen. Im ersten Schritt geht es um eine bewusste Auseinandersetzung mit den Werten, die einem wichtig

today—from human relations within the family to international conflicts. For a global population of ten billion, living together in a way that is more connected than ever before, across cultures and religions, it is extremely important to know where liberties end and where there are boundaries. Virtues will have to play a much bigger role again. The educational system must teach virtues and boundaries.

In the subtitle of your book, you speak of a "value system for the twenty-first century." This raises the question: do we need new values, or do the well-known old values need reappraisal?

ss: I am building on a nearly forgotten field of philosophy here, on what is called "material value-ethics," which was first described by philosopher Max Scheler in 1913. It allows us to think in an entirely new way about ourselves, about values, about the valuability of the world, and about the significance of values for our actions. The value system for the twenty-first century was thus expounded in the first half of the twentieth century—we need to rediscover it and bring it to fruition for our world. This is what I am trying to do in my book with respect to digitization. Above all, this type of value thinking must gain traction in corporate business models.

How can this be done, in concrete terms?

ss: Businesses as well as individuals need to take three steps to get to a more *valuable* life. The first step is conscious engagement with the values that are important to you. It is, however, not enough just to say that community or quality or whatever are important to you. You have to understand, in a second step, what these values mean, conceptually. We all are using value notions, but even the first probing questions show that we have forgotten how to think about what defines values. Aristotle has made it very clear what it means to be courageous, faithful, generous. I ask myself where in today's world an exploration of values in their most profound meaning is taking place. So, it is not just about setting goals but also about a comprehensive understanding of what to strive for, and why. The third step involves trying to realign one's own life and economic behavior. Such

sind. Es reicht aber nicht, nur zu sagen, Gemeinschaft oder Qualität oder was auch immer sind mir wichtig. Man muss im zweiten Schritt verstehen, was diese Werte konzeptionell bedeuten. Wir alle verwenden zwar Wertbegriffe, aber schon bei ersten Nachfragen zeigt sich, dass wir verlernt haben, darüber nachzudenken, was Werte auszeichnet. Aristoteles hat klar herausgearbeitet, was es bedeutet, mutig, treu, großzügig zu sein. Ich frage mich, wo in der Welt von heute eine Auseinandersetzung mit den Werten in ihrer tiefsten Bedeutung stattfindet. Man darf sich also nicht nur Ziele setzen, sondern muss auch umfassend verstehen, was man anstrebt und warum man das tut. Im dritten Schritt gilt es zu versuchen, sein eigenes Leben und Wirtschaften stärker daran auszurichten. Diese Ausrichtung ist nicht so einfach. Man kann sich viel vornehmen, aber es ist schwierig, seine Gewohnheiten zu ändern und sich in seinem Leben etwa an Menschen zu orientieren, die man schätzt. Vorbilder, Gewohnheiten und Maßhalten sind wesentliche Aspekte in diesem dritten Schritt.

In Ihrem Buch sprechen Sie in diesem Zusammenhang immer wieder von »ethics by design«. Was ist darunter genau zu verstehen?

ss: Wollen Unternehmen sicherzustellen, dass die Digitalisierung ihrer Strukturen so ausfällt, dass es tatsächlich zu Wert*schöpfung* kommt, müssen sie sich vorab mit Werten auseinandergesetzt haben und alle Prozesse und Anlagen daran ausrichten. Die drei genannten Stufen werden in entsprechenden Prozessen professionell durchlaufen. Das Institute of Electrical and Electronics Engineers (IEEE), der weltweit größte Berufsverband von Ingenieuren, arbeitet derzeit unter meiner Leitung an einem Prozessstandard, um systematisch über Wertschöpfung nachzudenken und diese in Technik und Rahmenprozesse einzubringen. Dadurch entsteht ein anderes Geschäftsmodell, eine andere »value proposition« – also ein anderes Nutzen- oder Wertversprechen an Kunden oder Wertschöpfungspartner.

Um noch einmal auf meine vorherige Frage zurückzukommen: Sie meinen also, dass wir keine neuen Werte für das 21. Jahrhundert benötigen?

ss: Nein, im Gegenteil. Die Welt von heute, gerade die europäische, ist von einer vielschichtigen Sensibilität für Wertigkeiten – für das Schöne, das Wahre und das Gute – beseelt. Das ist das, was das italienische Design ausmacht,

a realignment is not that easy. You can make many good resolutions, but it is difficult to change one's habits and to take one's orientation in life, for example, from people that you think highly of. Role models, habits, and moderation are essential aspects in taking this third step.

In your book, you repeatedly speak of "ethics by design" in this context. What exactly is to be understood by this?

ss: If companies want to make sure that the digitization of their structures leads to actual value *added* they will have to have engaged with values beforehand and align all processes and facilities accordingly. The three steps mentioned will be implemented professionally in suitable processes. The Institute of Electrical and Electronics Engineers (IEEE), the largest professional association of engineers worldwide, is currently working under my direction on developing a process standard to think systematically about value creation and to incorporate it in technology and framework processes. This leads to a new business model, a different "value proposition"—that is, a different promise of usefulness or benefit made to customers or partners in value creation.

To return once more to my earlier question: so you think we do not need new values for the twenty-first century?

ss: No, on the contrary. The world of today, particularly the European world, is inspired by an intricate sensibility for values—for the Beautiful, the True, and the Good. This is what is at the core of Italian design, of French cuisine, of German engineering. It is what distinguishes European cultures and makes them stand out by global comparison. That is why American and Asian tourists come to visit European cities. That is what makes life here far more interesting and beautiful than over there. And that is why I don't much like traveling to the USA today. Hardcore capitalism there has subjected each and every thing to profit and efficiency thinking. This is precisely what we do not want in Europe.

was die französische Küche ausmacht, was das deutsche Ingenieurwesen ausmacht. Das ist das, was die europäischen Kulturen unterscheidet und sie im globalen Vergleich auszeichnet. Deswegen besuchen amerikanische und asiatische Touristen europäische Städte. Das macht auch das Leben hier viel interessanter und schöner als dort. Daher fahre ich heute auch so ungern in die USA. Dort ist durch den Hardcore-Kapitalismus alles nur Profit und Effizienz unterworfen. Genau das wollen wir in Europa nicht.

Besteht da nicht die Gefahr eines neuen Eurozentrismus, wenn diese Werte dem Rest der Welt übergestülpt werden sollen?

ss: Das Schöne, Wahre und Gute gibt es auch in anderen Kulturen, die diese Werte jeweils auf ihre Weise ausgebildet haben. Wie ausgefeilt zum Beispiel die japanische oder die indische Kultur ist! Leider wurde und wird das alles von der kolonialen Homogenisierung der Erde und nun der Unterordnung aller Kulturen unter den neoliberalistischen Hardcore-Kapitalismus mit seinen zwei Werten Profit und Effizienz bedroht. Überall auf der Welt leiden Menschen unter dem gleichen Prozess: der Banalisierung und Homogenisierung früherer Vielfalt und dem massiven Verlust dessen, was für sie einmal von Wert war, von feinen Produkten und Speisen über Bücher bis hin zu Ritualen und kulturell ausgefeilten Lebensformen in funktionierenden Gemeinschaften.

Das heißt, das Schöne, Wahre und Gute ist uns Menschen immanent?

ss: Das Schöne, Wahre und Gute ist allen Menschen, ist allem, was lebt, immanent. Auch Tiere tragen viel Schönes, Wahres und Gutes in sich – auf sehr unterschiedliche Art und Weise. So sind etwa manche Tiere Vorbilder der Tugendhaftigkeit. Menschen haben darüber hinaus das, was wir Kultur nennen: Sie können sich Werte kognitiv bewusst machen, und sie können Werte bewusst in die Welt setzen. Das unterscheidet sie: Die Fähigkeit, etwas zur Schöpfung beizutragen, ist etwas zutiefst Menschliches. Auch die Digitalisierung ist ein schöpferisches Werkzeug. Auch sie gibt uns die Möglichkeit, Schönes, Wahres und Gutes zu schaffen. Mit der gleichen Technik können völlig unterschiedliche Werte etabliert werden. Es geht darum: Sollte die »digitale Transformation« weiter voranschreiten, dann würde ich den Begriff gern so

But doesn't imposing these values upon the rest of the world entail the danger of a new Eurocentrism?

ss: The Beautiful, the True and the Good also exist in other cultures, which have each articulated these values in their very own way. For example, think of how refined Japanese or Indian culture is! Unfortunately, all of that was, and still is, threatened by the colonial homogenization of the Earth and now by the submission of all cultures to neoliberal hardcore capitalism and the two values it knows: profit and efficiency. Everywhere in the world, people are suffering under the same process: the banalization and homogenization of previous variety and the massive loss of what once had value for them, from fine products and dishes to books, and to the rituals and culturally elaborated ways of living of functional social communities.

That means that the Beautiful, the True, and the Good are immanent in us as human beings?

ss: The Beautiful, the True, and the Good are immanent in all humans, and in everything that lives. Animals, too, have much in them that is beautiful, true, and good—in very different ways. Some animals, for example, are models of virtue. Beyond that, humans have what we call culture: they can make themselves cognitively aware of values, and they can consciously bring values to the world. This is what distinguishes them: the capability of contributing to creation is something profoundly human. Digitization is a creative tool, too. And it too provides us with a possibility of creating the Beautiful, the True and the Good. The same technology can be used to establish entirely different values. The point here is: should the "digital transformation" continue to progress, I would want to be able to understand the notion in such a way that we turn the stupid digitization pursued so far into a digitization that makes full use of its potentials—namely, to create the Beautiful, True, and Good and to move beyond the stupid logic of profit and efficiency, which eventually only one percent of one percent of the global population benefits from.

verstehen, dass wir aus dieser dummen Digitalisierung, wie sie bisher betrieben wurde, eine Digitalisierung machen, die ihre Potenziale ausschöpft – nämlich etwas Schönes, Wahres und Gutes zu schaffen und die Dummheit von Profit und Effizienz hinter sich zu lassen, von der letztlich nur ein Prozent von einem Prozent der Bevölkerung dieser Erde profitiert.

Das klingt nach einer schönen Vision …

ss: Ich werde häufig kritisiert, dass meine Gedanken zu positiv seien. Ich werde gefragt, ob es nicht naiv sei, daran zu glauben, dass man mit dem Digitalen das Schöne, Wahre und Gute schaffen kann – weil es an der harten Realität des bestehenden Systems komplett vorbeigeht. Es stimmt, dass die Realität nicht so orientiert ist. Ich glaube aber, dass man die Welt nicht zum Guten verändern kann, wenn man immer nur aufzeigt, was schlecht ist. Der einzige Weg, in dieser Welt etwas zum Positiven zu wenden, ist, das Positive und einen Weg dorthin aufzuzeigen. Dieser Weg mag naiv, träumerisch und märchenhaft anmuten, aber letztlich ist es der einzige Weg in eine bessere Zukunft. ×

Sounds like a beautiful vision . . .

ss: I am frequently criticized for being too positive in my thinking. People ask me if it's not naïve to believe that the digital can be used to create the Beautiful, the True, and the Good—because it completely misses the harsh reality of the existing system. It is true, reality is not oriented that way. But I believe that you cannot change the world for the better by always only pointing to what is bad in it. The only way to turn things for the better in this world is by pointing out the positive and how to get there. This path may seem naïve, like a dream, a fairy tale, but in the end, it is the only way into a better future. ×

Wirtschaftlicher Nutzen durch den Kampf gegen Cybercrime

Den Kosten, die Cyberattacken verursachen, stehen auch wirtschaftliche Chancen gegenüber – etwa durch die Entwicklung von sichereren Produkten, die einen Wettbewerbsvorteil begründen können. Die EU versucht in ihrer Digitalpolitik, Europa auf dem Weltmarkt neu zu positionieren.

Bis vor wenigen Jahren war Cybersecurity ein Thema, das vorrangig in technischen Fachkreisen debattiert wurde. Das hat sich spätestens mit den Ransomwareangriffen im Jahr 2017 völlig verändert: Seither ist einer breiten Öffentlichkeit klar, dass Cybersecurity auch ein großer Wirtschaftsfaktor ist. So ist etwa bekannt, dass mehr als die Hälfte der Unternehmen in Deutschland in den vergangenen Jahren Opfer von Cyberattacken geworden sind. Umfragen legen nahe, dass Ähnliches auch für Österreich zu erwarten ist – wobei hierzulande bis dato verlässliche Fakten fehlen, und das unter anderem deshalb, weil es keine Meldepflicht gab und die Dunkelziffer daher sehr hoch ist.

Weltweit werden Schäden durch Cyberangriffe auf bis zu 600 Milliarden Dollar geschätzt – ein Wert, der wegen der fortschreitenden Vernetzung und Ausbreitung des Internets der Dinge und damit der rapiden Vermehrung möglicher Einfallstore für Attacken weiter steigen wird. Die Schäden sind allerdings nur eine Seite der Medaille: Mittlerweile widmet sich ein gesamter Wirtschaftszweig dem Schutz vor Cybergefahren. Das beginnt bei spezialisierten Softwareentwicklern und reicht über Berater und Trainingsanbieter bis hin zu spezifischen Versicherungen.

Laut einer aktuellen Studie des Beratungsunternehmens PwC trägt Cybersecurity entscheidend zum Geschäftserfolg von Unternehmen bei: Bei der Befragung von mehr als 3000 Führungskräften und IT-Experten in 81 Ländern zeigte sich, dass die Pionierunternehmen in Sachen Cybersecurity auch eine höhere Wertschöpfung und bessere Geschäftsergebnisse lieferten. Dafür wesentlich ist die Abstimmung von Sicherheitsthemen und Geschäftsstrategien. »Unternehmen, die Cybersicherheit proaktiv in die Unternehmenskultur integrieren, sind am besten in der Lage, von den Vorteilen der digitalen Transformation zu profitieren, damit verbundene Risiken zu steuern und Vertrauen aufzubauen«, legt die Analyse der PwC-Experten nahe.

Die wirtschaftliche Relevanz des Themas Cybersecurity reicht aber noch viel weiter: Anstatt den Schutz vor Attacken aus dem Cyberraum als reinen Kostenfaktor anzusehen, könnte man diesen Bereich auch als Geschäftschance nutzen. Wenn Hersteller digitaler Geräte und Systeme

Fighting Cybercrime: The Economic Upside

The cost caused by cyberattacks is in part offset by economic opportunity—arising, for example, from the development of safer products that may give a competitive edge. In its digital policies, the EU is trying to reposition Europe in the global market.

Until a couple of years ago, cybersecurity was a topic for debate primarily in circles of technology experts. This has totally changed at least since the ransomware attacks of 2017: the general public has since become clearly aware that cybersecurity is also a major economic factor. More than half of all companies in Germany, for example, are known to have been victims of cyberattacks in recent years. Surveys suggest that similar numbers can also be expected for Austria—although, to date, reliable facts are still lacking for this country, partly because there was no disclosure requirement in place which is why the number of unreported cases can be assumed to be very high.

Globally, the damage caused by cyberattacks is estimated at up to 600 billion dollars—a figure that will continue to rise due to progressive interconnectedness and the spreading of the Internet of things and hence a rapidly growing number of potential entry points for attacks. However, the damage is only one side of the coin: an entire industry is now dedicated to offering protection against cyberthreats, starting with specialized software developers and extending from security consultants and training providers to specific insurance companies.

According to a recent study by consulting firm PwC, cybersecurity decisively contributes to the business success of companies: a survey of more than 3,000 executives and IT experts in 81 countries showed that companies pioneering in cybersecurity also delivered higher surplus value and better business results. This needs alignment of security issues and business strategies. “Companies that proactively integrate cybersecurity in their corporate culture are best able to profit from the benefits of digital transformation, manage the associated risks, and build trust,” the PwC experts’ analysis suggests.

But the economic relevance of the issue of cybersecurity goes much further than this: instead of merely considering protection against cyberspace attacks as a cost factor, the area could also be seen as offering a business opportunity. If manufacturers of digital devices and systems incorporate specific security features into their products,

gezielt Sicherheitsfeatures in ihre Produkte einbauen, heben sich diese von der Konkurrenz ab. Das verschafft ihren Produzenten einen Wettbewerbsvorteil. Die Logik dahinter: Macht man Cybersecurity zu einem Marktfeature und steigt das allgemeine Bewusstsein in diesem Bereich, wird es auch mehr Kunden geben, die für das bessere Produkt mehr zu zahlen bereit sind.

Darauf zielt auch die Politik der Europäischen Union ab: Wenn sich Europa als Kontinent des Datenschutzes und eines gemeinsamen Ansatzes zur Bekämpfung von Cyberkriminalität positioniert, erhöht das die Wettbewerbsfähigkeit europäischer Player auf dem globalen Markt. Der Cybersecurity Act der EU ermöglicht beispielsweise eine europaweite Zertifizierung von Geräten oder Onlinediensten nach einheitlichen Cybersecuritystandards. Das ist zwar noch nicht verpflichtend, doch es ist ein erster Schritt, um die Qualität europäischer Produkte in dieser Hinsicht zu steigern. Das Ziel ist, Sicherheitsmerkmale bereits in der Frühphase technischer Konzeption und Entwicklung zu berücksichtigen – und diese dann auch als Verkaufsargument und im Marketing zu nutzen (»eingebaute Sicherheit«).

Cybersecurity ist nur ein Baustein bei der von der EU anvisierten Etablierung eines digitalen Binnenmarkts: Dieser soll das Entstehen starker IT-Infrastrukturen in Europa (die sich derzeit auf die USA und China konzentrieren) sowie die Etablierung großer europäischer IT-Konzerne ermöglichen – und zudem als Vorbild für eine moderne Regulierung in die ganze Welt ausstrahlen. ×

these products stand out from the competition. This in turn gives manufacturers a competitive edge, the underlying logic being that by making cybersecurity a market feature, and with general problem awareness in this area on the rise, there will likely be more customers who are willing to pay more for a better product.

This is also what the policies of the European Union aim for: if Europe succeeds to position itself as a continent of data protection and a shared approach to combating cybercrime, it will increase the competitiveness of European players in the global market. The EU Cybersecurity Act, for example, institutes a European-wide certification of devices or online services according to uniform cybersecurity standards. Although not yet mandatory, this is a first step toward improving the quality of European products in this respect. The goal is to take security features into account already at an early stage of technical conception and development—and later use this as a selling and marketing point ("built-in security").

Cybersecurity is just one part of the foundation of the digital common market envisioned by the EU: it is supposed to facilitate the emergence of strong IT infrastructures in Europe (which are currently concentrated in the United States and in China) as well as the establishment of major European IT corporations—and to provide a model for modern regulation that sends a message to the world. ×

Fünf eigens für die Ausstellung *SPACE AND EXPERIENCE* konzipierte Pavillons, die mit verschiedenfarbig glasierten Wienerberger-Dachziegeln gedeckt sind, behandeln unterschiedliche räumliche, akustische und thematische Fragestellungen.

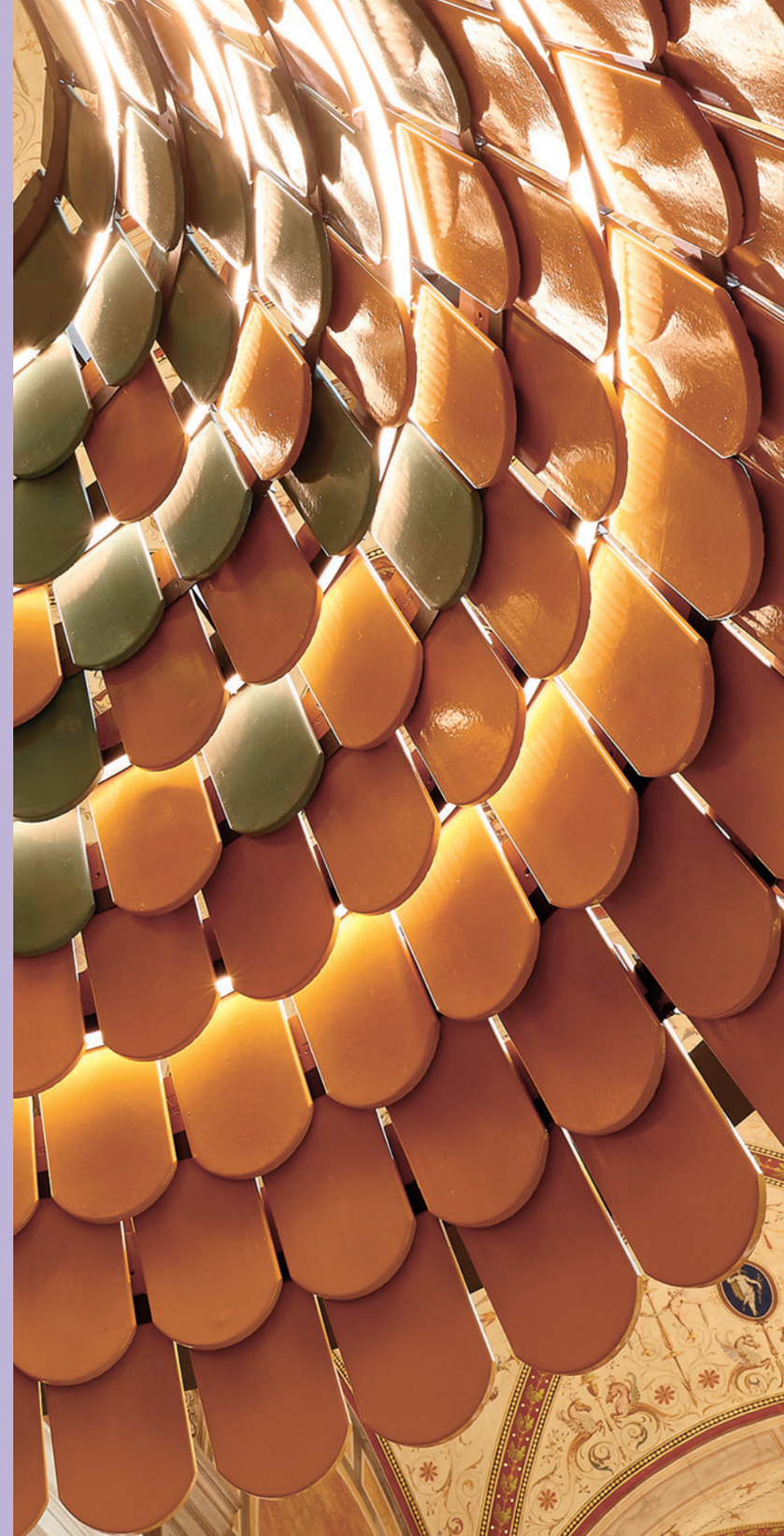
Specially designed for the *SPACE AND EXPERIENCE* exhibition, five pavilions covered with differently colored glazed Wienerberger roof tiles, deal with different spatial, acoustic and thematic issues.

→ mak.at/spaceand-experience

CREDITS:
Exhibition view *SPACE AND EXPERIENCE. Architecture for Better Living*

Tzou Lubroth Architekten, *Pavillon Materiality and the Design of Atmospheres*, 2019

MAK Columned Main Hall (1st floor)
© Peter Kainz, MAK



Christoph Thun-Hohenstein
Generaldirektor des MAK und Leiter der VIENNA BIENNALE FOR CHANGE 2019

Change!
Virtuelle und wirkliche Werte für eine bessere Zukunft

Wir leben in einem neuen Zeitalter, das unser Leben tiefgreifend verändert: Unterwerfen wir uns dieser digitalen Moderne ohne Wenn und Aber, oder nützen wir die großartigen Möglichkeiten digitaler Technologien, um uns als Menschen weiterzuentwickeln? Menschliche Superspezialisierung erscheint überholt, das können intelligente Maschinen zunehmend besser. Wir haben nunmehr die Chance, uns als Menschen wiederzuentdecken und unsere wertvollsten Qualitäten in die Gestaltung der Zukunft einzubringen. Das geschieht nicht von selbst. Wir müssen unser Leben ändern.

Wer sich mit Zukunft beschäftigt (und das sollten wir alle tun!), stößt in der Regel auf utopische oder dystopische Szenarien – oder auf Verharmlosungen. Utopien, vor allem solche aus dem Silicon Valley, wollen uns überzeugen, dass disruptive Innovationen in allen Lebensbereichen den Staat überflüssig und die Welt automatisch besser machen. Beispiele für Dystopien sind: Roboter und künstliche Intelligenz (KI) vernichten unsere Jobs. Oder: Eine uns überlegene Superintelligenz (SI) ergreift die Herrschaft der Welt und versklavt die Menschheit. Manche Szenarien sind so ambivalent, dass sie von den einen als dystopisch und von anderen als positiv eingestuft werden, wie etwa das in China ausgerollte »Sozialkreditsystem«, welches das Verhalten der Bürgerinnen und Bürger mit Plus- und Minuspunkten bewertet und deren Aussicht auf Schulplätze, hochwertige Jobs, Wohnkredite, Genehmigung von Auslandsreisen etc. vom Erreichen einer bestimmten Punkteanzahl abhängig macht. In China wird dieses System bisher kaum öffentlich diskutiert, in privaten Stellungnahmen jedoch eher positiv gesehen, u. a. deshalb, weil es durch seine »Objektivität« behördliche Willkür und Korruption verdrängt. Ein Beispiel für Verharmlosungen ist die häufig anzutreffende Aussage von KI-Forscherinnen und -Forschern, Ängste vor einer künftigen SI seien völlig unbegründet.

Das 21. Jahrhundert ist das Jahrhundert künstlicher Intelligenz. Ob es den Menschen am Ende dieses Jahrhunderts noch gibt, wird die Zukunft zeigen. Viel spannender ist die Frage, wie sich der Mensch bei exponentiellem technologischem Fortschritt in den kommenden 80 Jahren entwickeln wird. Mit anderen Worten: Wie werden die Menschen Mensch sein? Werden

Christoph Thun-Hohenstein (geb. 1960) ist seit 1. September 2011 Direktor des *MAK – Österreichisches Museum für angewandte Kunst / Gegenwartskunst*. Für das Bundesministerium für auswärtige Angelegenheiten der Republik Österreich hatte er Auslandsposten in Abidjan, Genf und Bonn inne. Von 1999 bis 2007 war er Direktor des Austrian Cultural Forum New York, danach fungierte er als Geschäftsführer von *departure – der Kreativagentur der Stadt Wien.*

Christoph Thun-Hohenstein publizierte insbesondere zur Europäischen Integration sowie zu Themen zeitgenössischer Kultur und Kunst und hielt zu Themen dieser Bereiche auch zahlreiche Vorträge. Er hat Ausstellungen zeitgenössischer Kunst kuratiert und übt regelmäßig Jurytätigkeiten aus.

Christoph Thun-Hohenstein
General Director, MAK, and Head of the VIENNA BIENNALE FOR CHANGE 2019

Change!
Virtual and Real Virtues for a Better Future

Christoph Thun-Hohenstein (born 1960) assumed direction of the *MAK – Austrian Museum of Applied Arts / Contemporary Art* on 1 September 2011. While working for the Austrian Foreign Ministry he held posts in Abidjan, Geneva, and Bonn. He was director of the Austrian Cultural Forum New York from 1999 to 2007, after which he served as managing director of *departure – the Creative Agency of the City of Vienna*, until August 2011.

Christoph Thun-Hohenstein has published on topics dealing above all with European integration and with contemporary culture and art, and has held numerous lectures on these topics. He has also curated exhibitions of contemporary art, and he regularly serves on selection juries.

We are living in a new era which is changing our lives fundamentally: will we surrender to this digital modernity with no ifs, ands, or buts, or will we make use of the magnificent possibilities of digital technologies to keep developing as human beings? Human superspecialization seems obsolete as intelligent machines are becoming increasingly better at it. We now have the chance to rediscover ourselves as human beings and to use our most valuable qualities to shape the future. This will not happen automatically, we will need to change our lives.

When engaging with the future (which all of us should do!), we will normally encounter utopian and dystopian scenarios—or downplaying. Utopias, especially those from Silicon Valley, want to convince us that disruptive innovations in all areas of life will make the state redundant and will automatically turn the world into a better place. Examples of dystopias are: robots and artificial intelligence (AI) will destroy our jobs. Or: a superintelligence (SI) superior to us will conquer the world and enslave humanity. Some scenarios are so ambivalent that some people consider them to be dystopian while others judge them to be positive, such as the "social credit system" unreeled in China, which rates the citizens' behavior with plus and minus points and makes their chance of admission to schools, high-quality jobs, mortgages, travel permits for abroad, etc. dependent on reaching a certain amount of points. In China, this system has barely been discussed in public so far; in private statements, however, it has been viewed rather positively, one reason being that its "objectivity" eliminates arbitrariness by the authorities and corruption. An example of downplaying is the commonly met assertion of AI researchers that the fear of a future SI is totally unfounded.

The twenty-first century is the century of artificial intelligence. Only the future will reveal whether humanity still exists at the end of this century. Much more fascinating is the question how human beings will develop over the next eighty years considering exponential technological progress. In other words: How will human beings be

sie mit heutigen Menschen überhaupt noch Gemeinsamkeiten haben? Was wird sie von letzteren grundlegend unterscheiden? Darauf kann gegenwärtig niemand eine Antwort geben, doch lässt sich trefflich spekulieren, mit welchen Herausforderungen wir uns vordringlich befassen müssen. Ich möchte dazu drei Thesen formulieren:

1. Das Schicksal der Menschheit entscheidet sich an künstlicher Intelligenz.
2. Wir Menschen sind maschinengesteuerte Cyborgs, die sich laufend optimieren.
3. Wir müssen die Zukunft neu erfinden, sonst wird sie uns neu erfinden.

Sind das gute oder schlechte Nachrichten aus der Zukunft? Je nachdem, könnte man antworten, wo wir die Menschheit in 80 Jahren idealerweise sehen. Eine persönliche Vision menschlicher Zukunft (und wenn man jung genug ist: der eigenen) für das Jahr 2100 zu entwickeln, ist der Anfang aktiver Zukunftsgestaltung und zugleich Voraussetzung für die gesellschaftspolitische Entwicklung einer gemeinsamen Vision für die Zukunft. Wir müssen alle Möglichkeiten nutzen, uns als kluge Digitalbürgerinnen und -bürger in die Gestaltung der Zukunft einzubringen. Das Ergebnis unseres gemeinsamen Bemühens wird vermutlich weder die reine Utopie noch der Realität gewordene Alptraum sein, sondern irgendwo dazwischen liegen. Entscheidend ist, dass die Richtung stimmt.

»Tief ist der Brunnen der Vergangenheit. Sollte man ihn nicht unergründlich nennen?«, hebt Thomas Manns weitläufiger Roman *Joseph und seine Brüder* an. Unendlich ist der Horizont der Zukunft, und ihre Ausgestaltung liegt in unseren Händen und ist unseren Köpfen anvertraut. Vergangenheit und Zukunft sind miteinander verwoben; wie effektiv wir diese Verknüpfungen nutzen, können derzeit noch wir Menschen bestimmen. Die Vergangenheit ist das gemeinsame Erbe der Menschheit, von den Höhen kultureller Leistungen bis zur ökologischen Katastrophe aufgrund des Raubbaus an unserem Planeten durch den Menschen. Erbkapital und Erblast tragen wir im Reisegepäck – ebenso wie die Verantwortung, künftigen Generationen, darunter unseren Kindern und Enkelkindern, eine möglichst gute Welt zu hinterlassen.

Das Schicksal der Menschheit entscheidet sich an künstlicher Intelligenz

KI begegnet uns schon heute in vielen Lebensbereichen als sogenannte »schwache«, »spezialisierte« KI (bei Kreditvergaben, Stellenbewerbungen, im Verkehr, im Versicherungswesen, im Gesundheitsbereich, um nur einige Beispiele zu nennen) und wirkt sich insofern bereits direkt auf unser Leben aus. Sie ist zugleich jene Technologie, in die weltweit am meisten Geld

human? Will they still share any similarities at all with today's human beings? And what will fundamentally distinguish them from the latter? Currently, nobody can answer these questions, but we can splendidly speculate about the challenges we will most urgently have to deal with. In this regard, I would like to put forward the following hypotheses:

1. Artificial intelligence will be the decisive factor for humanity's destiny.
2. We humans are machine-driven cyborgs continuously optimizing ourselves.
3. We have to reinvent the future or else it will reinvent us.

Is this good or bad news from the future? It depends, one could reply, on where we ideally want to see humanity in eighty years. Developing a personal vision of humanity's future (and if you are young enough: of your own) for 2100 is a first step toward actively shaping the future and at the same time a requirement for the socio-political development of a shared vision for the future. We need to make use of all possibilities to get involved in shaping the future as clever digital citizens. The result of our shared efforts will most likely neither be pure utopia nor a nightmare turned reality but rather be located somewhere in between. What is decisive is that the direction is right.

"Deep is the well of the past. Should we not call it bottomless?" begins Thomas Mann's extensive novel *Joseph and His Brothers* (trans. John E. Woods, 2005). The future's horizon is infinite, yet shaping the future lies in our hands and is entrusted to our minds. The past and the future are interwoven; right now, we humans can still decide how effectively we want to make use of these connections. The past is humanity's collective legacy, from the height of cultural achievements to the ecological catastrophe due to the exploitation of the Earth by humans. We carry inherited capital as well as inherited burden in our luggage—just as much as the responsibility of handing over as good a world as possible to future generations, including our children and grandchildren.

Artificial intelligence will be the decisive factor for humanity's destiny

Already today, we encounter AI in many areas of our life (granting of loans, job applications, traffic, insurances, health care, just to mention a few examples) as so-called "weak" or "narrow" AI, and it thus already has direct impact on our lives. On the other hand, it is the technology into which most money is being invested worldwide and a field where China is about to overtake the USA and by 2030 wants to be and

investiert wird, wobei China die USA in diesem Feld bereits überholt und bis 2030 die global klar dominierende KI-Macht sein will und wird. Die Forschung beschränkt sich natürlich nicht auf spezialisierte KI, sondern stellt sich zugleich der Herausforderung, eine sogenannte »starke« KI, die es an genereller Intelligenz mit dem Menschen aufnehmen kann, zu entwickeln. Eine solche »artificial general intelligence« (AGI) – eine allgemeine künstliche Intelligenz – hätte den Vorteil, dass sie nicht bloß für ein klar definiertes Spektrum von Aufgaben, sondern gleichsam universell einsetzbar wäre.

Wenn KI heutzutage oft mit Maschinenlernen gleichgesetzt wird, sind damit die neuen, dem menschlichen Hirn nachempfundenen Lernmethoden für KI angesprochen, die erst in den letzten Jahren aufgrund der enormen Rechnerkapazitäten und -geschwindigkeiten effektiv angewendet werden können. Mit diesen Methoden kann KI so trainiert werden, dass sie die mit hoher Wahrscheinlichkeit richtigen bzw. vergleichsweise besten Ergebnisse ermittelt. Selbstlernende Maschinen sind also darauf angelegt, nicht nur durch geringere Kosten möglichst viele Menschen zu ersetzen, sondern auch immer bessere Ergebnisse zu liefern – das heißt: Menschen zu übertreffen. Wie genau sie zu Ergebnissen kommen, ist aber selbst bei schwachen KIs häufig nicht mehr nachvollziehbar. Es geht also um die sogenannte »explicability« – die Erklärbarkeit – von KI-Entscheidungen, welche die Grundvoraussetzung für menschliches Vertrauen in KI ist (sogenannte »trustworthy AI«, siehe den Vorschlag der von der EU-Kommission eingesetzten »High-Level Expert Group on Artificial Intelligence« für ethische Richtlinien für vertrauenswürdige KI vom 18. Dezember 2018, https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai). Selbst diese wünschenswerte Nachvollziehbarkeit der KI-Entscheidungsfindung nutzt aber wenig, wenn – wie etwa im militärischen Bereich – eine augenblickliche intelligente Reaktion gefordert ist, die nur von superstarken und -smarten Maschinen geleistet werden kann: Was, wenn eine solche KI nach blitzschneller Entscheidungsfindung in Abwehr eines vermeintlichen Angriffs einen Vernichtungsschlag auslöst? Auch im Finanzbereich gibt es erhebliches Gefahrenpotenzial: An den Börsen hat »rogue AI trading« schon wiederholt für Tumulte gesorgt.

Wenn Big Data der Treibstoff selbstlernender Maschinen ist und China als ehrgeizigste KI-Nation der Welt bereits eine Milliarde Internetuserinnen und -user aufweist (davon 98 Prozent mobil), kann man sich ausrechnen, wie üppig KIs allein in China laufend gefüttert werden. Je vernetzter – jeder mit jedem, jeder mit allem, alles mit allem – unsere Welt wird, umso effektiver kann KI in allen Lebensbereichen zum Einsatz kommen. Diese Totalvernetzung wird auch in Japan mit dem Modell der »Gesellschaft 5.0« von Regierungsseite forciert. Wenn die mangelnde Nachvollziehbarkeit von Entscheidungen schon bei schwacher selbstlernender KI ein Problem ist, kann sie bei AGI zum Super-GAU werden.

will be the clearly dominating global AI power. Research, however, is of course not restricted to narrow AI but faces the challenges of developing so-called "strong" AI, which can compete with humans with regard to general intelligence. Such "artificial general intelligence" (AGI) would have the advantage of not only targeting a clearly defined spectrum of tasks but being more or less universally applicable.

When AI nowadays is often equated with machine learning, we refer to the new learning methods for AI based on the human brain as a model, which could only be applied effectively in the last years due to enormous computing capacity and processing speed. With these methods, AI can be trained to calculate the results that are most likely to be correct or comparatively the best. Consequently, self-learning machines are designed not only to replace as many humans as possible due to lower costs but also to produce ever better results, which means: to outperform human beings. How exactly they reach their results, however, can often no longer be comprehended, not even in the case of weak AIs. Consequently, we are talking about the so-called "explicability" of AI decisions which is the basic condition for humans to trust AI ("trustworthy AI"; see the draft of the AI Ethics Guidelines for Trustworthy AI presented by the European Commission's High-Level Expert Group on Artificial Intelligence from 18 December 2018, https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai). Even this desirable comprehensibility of AI decision making is of little use when—as, for example, in the military sector—immediate intelligent reactions are required which can only be provided by superstrong and supersmart machines: What if such an AI after making an instantaneous decision triggers an annihilating blow in order to fend off a suspected attack? There is also considerable risk in the finance sector: "Rogue AI trading" has already repeatedly caused turbulences in the stock markets.

If Big Data is the fuel of self-learning machines and China, as the world's most ambitious AI nation, already has one billion internet users (98 percent of which are mobile), you can work out how well AIs only in China are constantly being fed. The more interconnected—everybody with everybody, everybody with everything, everything with everything—our world is becoming, the more effectively AI can be applied to all areas of life. This total interconnection is also being propagated by the government in Japan with the model "Society 5.0." If the lack of comprehensibility is already a problem in the case of weak self-learning AI, it can cause an ultimate catastrophe when it comes to AGI.

Self-learning AGIs which reach a human level will not stop at this level when competing with each other but rather keep on developing to superintelligences. These, in turn, will develop self-learning super-

Selbstlernende AGIs, die menschliches Niveau erreichen, werden im Wettlauf miteinander nicht an diesem Punkt haltmachen, sondern sich zu Superintelligenzen weiterentwickeln. Jene werden ihrerseits selbstlernende superintelligente Maschinen hervorbringen, die von menschlicher Kontrolle noch weiter entfernt sind. Selbstlernende Maschinen sind vermutlich die letzte Megaerfindung der Menschheit, künftige Intelligenzexplosionen können wir getrost den supersmarten Maschinen überlassen. Worin die Intelligenz solcher Intelligenzexplosionen bestehen wird, ist aus menschlicher Sicht kaum vorstellbar.

Der Großteil der KI-Expertinnen und -experten schließt das Entstehen einer Superintelligenz für die nächsten drei bis vier Jahrzehnte dezidiert aus. Dabei wird immer davon ausgegangen, dass eine solche KI in allen Tätigkeitsbereichen das Intelligenzniveau bzw. die Fähigkeiten der Menschheit übertreffen müsste. Worauf es aber meines Erachtens ankommt, ist die Frage, für wie lange noch eine KI definitiv ausgeschlossen werden kann, die um einen kleinen Schritt besser im Manipulieren kritischer digitaler Systeme ist als Menschen (also gleichsam ein superintelligenter künstlicher Hacker). Niemand kann seriös vorhersagen, wie weit wir von diesem Punkt entfernt sind.

Das Schicksal der Menschheit wird sich auch in der Nutzung der positiven Potenziale von KI entscheiden, vor allem im Hinblick auf die beiden Hauptthemen Bekämpfung des Klimawandels und Verringerung sozialer Ungleichheit. Kongenialer Umgang mit KI setzt daher ein klares gemeinsames Werteverständnis voraus – global, regional, national und lokal. Dabei wird es entscheidend darauf ankommen, mit welchem Menschenbild KI zu tun haben wird.

Menschen als maschinengesteuerte Cyborgs, die sich laufend optimieren

Wir leben in einer Welt exponentiellen technologischen Fortschritts, vereinfacht gesprochen: das Tempo des Fortschritts verdoppelt sich alle zwei Jahre. Wie sollen wir Menschen als linear tickende biologische Wesen mit einer mittlerweile steil nach oben zeigenden Technologiekurve zurechtkommen? Grundsätzlich stehen uns zwei Wege offen: Entweder wir setzen alles daran, unsere biologischen Eigenschaften so rasch und umfassend wie möglich hinter uns zu lassen und durch die jeweils neuesten Technologien zu ersetzen, oder wir versuchen, die Zukunft nicht den Technologien anzupassen, sondern sie nach unseren menschlichen Bedürfnissen auszurichten.

Dieses Grunddilemma menschlicher Zivilisation stellt sich in der digitalen Moderne in besonderer Schärfe, leben wir doch im Zwiespalt zwischen biologischer Realität und technologischer Virtualität (und Virtuosität). Die 2020er-Jahre werden als Jahrzehnt extrem ausgeklügelter virtueller Realitäten in die Geschichte eingehen, sowohl im exklusiv virtuellen Raum (Virtual Reality) als auch im realen Raum (von »Augmented

intelligent machines which will be even more remote from human control. Self-learning machines will probably be humanity's last megainvention. We can safely leave future intelligence explosions to supersmart machines. What kind of intelligence will stem from such intelligence explosions can barely be imagined from a human perspective.

The majority of AI experts decidedly rules out the creation of a superintelligence for the next three to four decades. This conclusion is based on the presumption that such AI would have to outperform the level of intelligence or the abilities of humanity in all fields of action. In my opinion, however, it is more crucial to ask for how much longer we can definitely exclude AI that will be just a tiny step more advanced than humans at manipulating critical digital systems (similar to a superintelligent artificial hacker). Nobody can reliably predict how far away we are from this point.

Humanity's destiny will also be decided by making use of the positive potentials of AI, especially as regards the two key issues: fighting climate change and reducing social injustice. Congenial handling of AI, therefore, requires a clear common understanding of values—globally, regionally, nationally, and locally. Here it will vitally depend on which concept of human nature AI will be dealing with.

Humans as machine-driven cyborgs who continuously optimize themselves

We are living in a world of exponential technological progress. Simply speaking, progress is doubling its pace every two years. How can we humans, as linearly functioning biological beings, deal with a technological curve that continues to rise rapidly? In general, there are two paths we can take: Either we do everything in our power to overcome our biological characteristics as quickly and thoroughly as possible and replace them with the respective latest technologies, or we try not to adapt the future to technologies but rather to align it with our human needs.

This fundamental dilemma of human civilization is particularly acute in the age of digital modernity as we are living in a conflict between biological reality and technological virtuality (and virtuosity). The 2020s will go down in history as a decade of extremely sophisticated virtual realities both in the exclusively virtual reality and in the real world (from "augmented reality" to so-called "mixed reality"). It is not unlikely that we will be able to directly link our brain with AI in a non-invasive way within the course of the next ten to twenty years. Similar things will be happening to our biological bodies, which are already constantly being optimized by technology (e.g. by cochlear implants). This trend will increase radically, i.e., the mechanized percentage of our bodies will increase, our biological intelligence will

Reality« bis zur sogenannten »Mixed Reality«). Es ist nicht unwahrscheinlich, dass wir im Laufe der nächsten 10 bis 20 Jahre unser Gehirn auf nichtinvasive Weise mit KI direkt verlinken können. Ähnliches passiert mit unserem biologischen Körper, der durch Technologien bereits jetzt laufend optimiert wird (z. B. durch Hörimplantate). Dieser Trend wird sich radikal verstärken: Der Maschinenanteil in unserem Körper wird steigen, unsere biologische Intelligenz mit KI verschmelzen. Dies alles geschieht nicht mit einem Paukenschlag, sondern stückweise (»incremental change«), doch ist diese schleichende Veränderung umso wirkungsvoller.

Wie gehen wir damit um, wenn die in der Vergangenheit getrennten Sphären virtuelle Magie und reale Welt, Technologie und Biologie zunehmend verschwimmen? Wie stellen wir sicher, dass unser biologischer Körper und Geist damit nicht heillos überfordert werden? Lassen wir uns einfach im rasanten Strom technologischen Fortschritts treiben, oder wollen wir unser Menschsein aktiv verhandeln und die Zukunft, die wir wirklich wollen, mitgestalten? Wie können wir die Potenziale der supersmarten neuen Technologien nutzen, um das verheerende Erbe menschlicher Zivilisation – den Raubbau an der Erde und die dramatische soziale Ungleichheit – effektiv zu reparieren?

Es ist nicht schwer vorherzusagen, dass wir in der digitalen Moderne beides brauchen, um gegenüber unseren Mitmenschen wie auch gegenüber digitalen Maschinen einigermaßen konkurrenzfähig zu bleiben: erstens die laufende Verbesserung unserer geistigen Fähigkeiten und unseres Körpers durch digitale Technologien (die enormen Fortschritte im Bereich der Gentechnik wurden ja ebenfalls durch die exponentielle Steigerung von Rechnerleistungen ermöglicht) und zweitens die Entwicklung einer anderen Zukunft als jener, auf die wir in Riesenschritten zusteuern.

Wir müssen die Zukunft neu erfinden, sonst wird sie uns neu erfinden

Der sogenannte »Earth Overshoot Day« (Erdüberlastungstag) bezeichnet jenen Tag des Jahres, an dem die Menschheit so viel an Natur verbraucht hat, wie der Planet Erde im ganzen Jahr erneuern kann. 2018 fiel dieser Tag auf den 1. August; die Menschheit verbraucht also jährlich rund 1,7 Erden. Jedes Jahr vermindert sich die betreffende Zeit um rund fünf Tage (siehe dazu www.overshootday.org). Für Menschen im globalen Norden stellt sich die Lage noch viel dramatischer dar, denn der dort mehrfach überhöhte ökologische Fußabdruck bedeutet, dass jährlich mehrere Erden verbraucht werden. Trotz dieser erschreckenden Bilanz stehen die Zeichen überall unverändert auf Steigerung des Massenkonsums: mehr, besser, billiger bleibt das Dogma in fast allen Volkswirtschaften – und ausgeklügelte Algorithmen haben sich zu den besten Verkäufern der Welt entwickelt.

In den Regionen der Welt mit starkem Bevölkerungswachstum stehen die großen Wohlstandsschübe noch bevor – mit entsprechenden Auswirkungen auf den ökologischen Fußabdruck. Die Menschheit steuert angefuse with AI. All of this will not happen with a bang but step by step ("incremental change"). However, this gradual change will be even more effective.

How will we deal with the situation when the spheres of virtual magic and real world, technology and biology, which were separate in the past, become more and more blurred? How can we ensure that our biological bodies and minds are not utterly overwhelmed by this? Will we simply go with the incredibly fast flow of technological progress or do we want to actively negotiate our human existence and help shape the future we really want? How can we use the potentials of supersmart new technologies to effectively repair the devastating legacy of human civilization—the overexploitation of the planet Earth and dramatic social injustice?

It is not difficult to predict that we will need both in digital modernity in order to be able to compete with our fellow humans as well as with digital machines to some degree: firstly, the continuous improvement of our cognitive abilities and our bodies by means of digital technologies (after all, the enormous progress in genetic engineering also became possible due to the exponential increase in processing power), and, secondly, the development of a future different from the one we are heading for with giant steps.

We have to reinvent the future or else it will reinvent us

The so-called Earth Overshoot Day refers to the day of the year when humanity has consumed as much nature as the planet is able to regenerate in the entire year. In 2018, it fell on August 1. In other words, humanity consumes approximately 1.7 Earths every year, and every year this day advances by approximately five days (see www.overshootday.org). For people in the Global North the situation turns out to be even more dramatic as their more than excessive ecological footprint implies that they consume multiple Earths every year. Despite this alarming summary, all signs steadily point toward an increase in mass consumption: more, better, cheaper remains the dogma in almost all national economies—and sophisticated algorithms have become the world's best sellers.

In those regions of the world with strong population growth, the big wealth thrusts are yet to happen—including the respective consequences for the ecological footprint. In light of climate change and other megaproblems, such as the loss of species diversity and the overfertilization of inland and coastal waters, humanity is approaching an ecological catastrophe, and we are clueless as to how to deal with it although there is no lack of suggestions. In the Global North, the ecological footprint will have to be reduced dramatically and a new vision of wealth based on circular economy will urgently have

sichts des Klimawandels und anderer Megaprobleme wie des Verlusts der Artenvielfalt und der Überdüngung von Binnen- und Küstengewässern auf eine ökologische Katastrophe zu, und wir sind ratlos, wie wir damit umgehen sollen. Dabei mangelt es nicht an Vorschlägen. Im globalen Norden muss der ökologische Fußabdruck einschneidend reduziert und dringend eine neue Vision kreislaufwirtschaftlichen Wohlstands entwickelt werden. In anderen Teilen der Welt muss von vornherein – ebenfalls auf Basis technischer und biologischer Kreislaufwirtschaft – ein Modell zukunftsfähigen Wohlstands angestrebt werden, das die Irrwege der westlichen Industrieländer vermeidet.

Zugleich erleben wir in vielen Teilen der Welt einen alarmierenden Anstieg sozialer Ungleichheit: Demokratien schwächeln, der Mittelstand droht zu zerbröseln, einigen wenigen Superreichen steht eine wachsende Mehrheit von armen und armutsgefährdeten Menschen gegenüber – Zündstoff für Migrationswellen, politische Erdbeben und Revolutionen, wie in vielen reichen und ärmeren Ländern bereits zu beobachten ist.

Die Zukunft, wie sie sich derzeit herauskristallisiert, kann nicht die Zukunft sein, die wir wollen. Wir müssen daher unsere Zukunft neu erfinden. Dazu brauchen wir auch eine kluge und vertrauenswürdige KI, die uns mit ganzheitlichem Blick darin unterstützt, unser viel zu ressourcenintensives Leben mit den langfristigen Interessen des Planeten in Einklang zu bringen.

Die Bewältigung dieser drei miteinander verbundenen Megaherausforderungen – umsichtiger Umgang mit KI, Zurechtkommen mit der neuen »conditio humana« als maschinengesteuerte, selbstoptimierende Cyborgs und radikale Neuerfindung der Zukunft – wird nur auf der Grundlage gemeinsamer Werte gelingen. Es geht um nichts Geringeres, als einen für die digitale Moderne passenden Kanon von Werten zu definieren, die sich zu einem ganzheitlichen Ansatz verdichten lassen und damit unteilbar sind. Das Hervorheben einzelner Werte muss immer unter grundsätzlicher Beachtung der übrigen erfolgen. Aber welche traditionellen Werte müssen wir erneuern, welche Werte neu erfinden?

Ausgangspunkt ist die Frage, welchen menschlichen Eigenschaften wir in Zeiten allumfassender Digitalisierung besondere Bedeutung für die Zukunft beimessen. Eine erste Liste besonders zukunftsrelevanter menschlicher Stärken könnte – ohne Anspruch auf Vollständigkeit – (in alphabetischer Reihenfolge) wie folgt aussehen: achtsam; authentisch, aufrichtig, echt; demütig; einfühlsam und liebevoll; fair; fantasievoll, ideenreich; fürsorglich; ganzheitlich; gemeinwohlorientiert; hochwertig; kooperativ; kreativ und kokreativ; kritisch denkend; kundig, vor allem digital; nachhaltig; offen und tolerant; resonant; sozial und inklusiv; teilend; traditionsbewusst, vor allem regional und lokal; verantwortungsvoll; vertrauensvoll; visionär; wertschätzend.

Viele dieser menschlichen Stärken können als Werte charakterisiert werden, andere sind Ausgangspunkt für die Bestimmung menschlicher Werte. Die

to be developed. In other parts of the world, a model of sustainable wealth—also based on technical and biological circular economy—will have to be pursued from the beginning thus avoiding the mistakes of Western industrial nations.

We are also experiencing an alarming increase in social injustice in many parts of the world: Democracies are ailing, the middle class is on the verge of crumbling, a few superrich are faced with a growing majority of people who are poor or at the risk of poverty—fuel for waves of migration, political earthquakes, and revolutions, as can already be observed in many rich and poor countries.

The future, in the way it is taking shape right now, cannot be the future we really want. Therefore, we will have to reinvent our future. In order to do so, we will also need smart and reliable AI to support us with a holistic view of aligning our resource-intensive lives with the long-term interests of the planet.

Overcoming these three intertwined megachallenges—sensible handling of AI; coming to terms with our new "conditio humana" as machine-driven, self-optimizing cyborgs; and radical reinvention of the future—will only be successful if based on common values. We are dealing with nothing less than defining a suitable canon of values for digital modernity that condense to a holistic approach and will thus be inseparable. Highlighting individual values must always take the other values into account. But which traditional values will have to be renewed, which ones reinvented?

Starting point is the question which human qualities we want to place particular emphasis on for the future in times of all-encompassing digitization: A first list of human strengths especially relevant for the future could—without claiming to be complete—be as follows (in alphabetic order): appreciative; attentive; caring; common-good-oriented; cooperative; creative and co-creative; critical in thinking; fair; genuine; high-quality; holistic; humble; imaginative; literate, especially digitally; open and tolerant; resonant; respectful; responsible; sensitive and loving; sharing; social and inclusive; sustainable; tradition-conscious, particularly regionally and locally; trusting; visionary.

Many of these human strengths can be characterized as values, others are starting points for determining human values. The values derived directly or indirectly from these strengths should, in any case, qualify as future-proof maxims of action, hence be effectively applicable. We are therefore talking of applied values, the synergy of which will provide a clear orientation for the continuous development of our society in digital modernity. Primarily, they are aimed at individuals and want to support their self-actualization. At the same time, they address the major socio-political forces such as politics, media, civil

direkt oder indirekt daraus abgeleiteten Werte sollten sich jedenfalls als zukunftsfähige Handlungsmaximen eignen, also effektiv anwendbar sein. Es geht somit um angewandte Werte, die in ihrem Zusammenwirken eine klare Orientierung für die Weiterentwicklung der Gesellschaft in der digitalen Moderne bieten. Sie richten sich zunächst an Einzelmenschen und wollen deren Selbstverwirklichung unterstützen. Sie sind zugleich an die großen gesellschaftspolitischen Kräfte Politik, Medien, Zivilgesellschaft und Kultur, Wirtschaft, Wissenschaft/Forschung und Technologie adressiert und sollen damit nicht nur den Einzelnen, sondern auch die Gesellschaft in die Pflicht nehmen. Nicht zuletzt richten sich diese Werte an KI und sollen entsprechende Relevanz sowohl für die Erstprogrammierung von Algorithmen allgemeiner und spezialisierter KI als auch für deren Maschinenlernen entfalten.

Digitale Technologien, insbesondere KI, können positiven Wandel bewirken, wenn sie nicht mehr den Massenkonsum ankurbeln, sondern die Gesellschaft zukunftsfähig machen. Eine Gesellschaft ist zukunftsfähig, wenn sie Gemeinwohlgrundsätzen wie Vertrauen, Verantwortung, Kokreativität (der gemeinsamen Entfaltung von Potenzialen), Fairness, Empathie, Solidarität und (Für-)Sorge, Teilen, Reparieren, Nachhaltigkeit und Qualität, Dezentralität (Stärkung des Lokalen) und Vielfalt verpflichtet ist und diese Grundsätze mit einem ganzheitlichen Ansatz zur Anwendung bringt.

Aus den vorstehenden Überlegungen lassen sich drei Regeln ableiten, die zwar aus der Perspektive des Einzelmenschen formuliert sind, sich aber in gleicher Weise an die großen gesellschaftspolitischen Kräfte richten:

Regel 1: Menschen sollen zum menschlichen Gemeinwohl (»human commons«) beitragen und danach streben, ein sinnstiftendes Leben zu führen, das in ökologischer, sozialer, kultureller und wirtschaftlicher Hinsicht nachhaltig und zukunftsfähig ist.

Regel 2: Menschen sollen menschliche Qualitäten hochhalten – es sei denn, dies steht in Widerspruch zu Regel 1.

Regel 3: Menschen sollen miteinander und mit KI und Robotern kooperieren – es sei denn, dies steht in Widerspruch zu Regel 1 oder Regel 2.

Wir werden diese Regeln dringend benötigen, um die Herausforderungen dieses Jahrhunderts zu meistern. Doch Regeln sind »Spaßbremsen«, wir aber brauchen Freude, Begeisterung und Leidenschaft für positiven Wandel. Wir können auch nicht wollen, dass KI die Einhaltung dieser Regeln akribisch überwacht und uns – in Anlehnung an das chinesische »Sozialkreditsystem« – als vorbildliche oder weniger gute Bürgerinnen und Bürger benotet und daran allfällige finanzielle Sanktionen (z. B. eine individuell höhere Steuerbelastung) knüpft. Wir wollen einen anderen Weg gehen – einen Weg, der uns zu leidenschaftlichen Menschen und souveränen und stolzen Bürgerinnen und Bürgern der digitalen Moderne macht. Gerade in einer Zeit, in der alles digital vermessen wird und wir uns laufend selbst vermessen, erscheint eine menschliche Stärke, die sich nicht vermessen lässt, besonders relevant: Resonanz.

society and culture, economy, science/research, and technology and therefore are also meant to not only make the individual but also society assume their responsibilities. Last but not least, these values target AI and are supposed to exert relevance for both the initial programming of algorithms of general and narrow AI and their machine learning.

Digital technologies, especially AI, can produce positive change if they no longer boost mass consumption but instead make us future-proof. A society is future-proof when it is committed to the principles of the common good such as trust, responsibility, co-creativity (collective unfolding of potential), fairness, empathy, solidarity and care, sharing, repairing, sustainability and quality, decentrality (strengthening local resources), and plurality and applies these principles with a holistic approach.

From the reflections above, three rules can be deduced which may be phrased from the perspective of the individual human being but equally address the major socio-political forces:

Rule 1: Humans should contribute to the human commons and strive to lead a meaningful life that is sustainable and future-proof in an ecological, social, cultural, and economic way.

Rule 2: Humans should foster human qualities—unless this conflicts with rule 1.

Rule 3: Humans should cooperate with each other as well as with AI and robots—unless this conflicts with rule 1 or rule 2.

We will desperately need these rules to master the challenges of this century. But rules are fun killers, and what we need is fun, enthusiasm, passion for positive change. We also cannot want AI to meticulously monitor compliance with the rules and to rank us—like the Chinese "social credit system"—as model citizens or less good citizens and to link possible financial sanctions (e.g. individual higher taxes) to this ranking. We want to take a different path—a path that turns us into passionate people and sovereign and proud citizens of digital modernity. Especially in a time when everything is measured digitally and we are constantly measuring ourselves ("quantified self" etc.), one human strength that cannot be measured seems particularly relevant to me: resonance.

The German sociologist Hartmut Rosa has received worldwide recognition for his studies on the acceleration of our lives. In his masterpiece *Resonance,* published in 2016, Rosa provides a comprehensive "Sociology of Our Relationship to the World" and with it, in my opinion, the most convincing fundamental theory on the development from a modernity obsessed with increase and focused on acceleration to a sustainable modernity focused on quality. In the description of his follow-up *Unverfügbarkeit* (Unavailability), published in 2018, Rosa's

Der deutsche Soziologe Hartmut Rosa hat mit seinen Untersuchungen über die Beschleunigung des Lebens weltweit Beachtung gefunden. Mit seinem 2016 erschienenen Meisterwerk *Resonanz* hat Rosa eine umfassende »Soziologie der Weltbeziehung« und damit die meines Erachtens überzeugendste Grundtheorie für die Weiterentwicklung der steigerungsbesessenen Beschleunigungsmoderne zu einer nachhaltigen Qualitätsmoderne vorgelegt. In der Beschreibung seines 2018 erschienenen Folgewerks *Unverfügbarkeit* werden Rosas Überlegungen wie folgt zusammengefasst: »Das zentrale Bestreben der Moderne gilt der Vergrößerung der eigenen Reichweite: Die Welt soll ökonomisch und technisch verfügbar, wissenschaftlich erkennbar und beherrschbar, rechtlich berechenbar, politisch steuerbar und zugleich alltagspraktisch kontrollierbar und erfahrbar gemacht werden. Diese verfügbare Welt ist jedoch, so Hartmut Rosas brisante These, eine verstummte, mit ihr gibt es keinen Dialog mehr. Gegen diese fortschreitende Entfremdung von Mensch und Welt setzt Rosa die ›Resonanz‹, als klingende, unberechenbare Beziehung mit einer nicht-verfügbaren Welt.«

Wenn Beschleunigung das Problem ist, dann ist Resonanz für Rosa vielleicht die Lösung. Resonanz kann den Maßstab für ein gelingendes Leben liefern, indem Lebensqualität nicht mehr nur indirekt an der Steigerung von materiellem Wohlstand, Optionen und Ressourcen gemessen wird, sondern direkt an der Qualität der Weltbeziehung, z. B. einem anregenden Gespräch mit anderen Menschen oder dem Gebrauch eines Alltagsgegenstandes, dessen Schönheit man schätzt. Ein gutes Leben wäre dann eines, das reich an Resonanzerfahrungen ist und über stabile Voraussetzungen für das Erleben von Resonanz verfügt.

Rosa versucht, Resonanz als ein Metakriterium gelingenden Lebens zu etablieren, und macht sich mit der Resonanz-Theorie auf die Suche nach dem »Anderen« im Sinn einer besseren Daseinsform. Resonanz ist nicht wertfrei konzipiert, sondern liefert angesichts wichtiger Ausprägungen von Resonanzsensibilität wie Empathie, Empfindsamkeit und Emotionalität eine klare Richtungsidee für den Umbau unserer Gesellschaft. In einer total vernetzten und berechneten Welt erscheint Resonanz – als das Unberechenbare und Unverfügbare – daher als Schlüsselkonzept, um eine erstrebenswerte andere Welt zu gestalten, in der nicht der Massenkonsum, sondern die Lebensqualität wächst und nicht digitale Algorithmen und Big Data, sondern souveräne Bürgerinnen und Bürger als resonanzsensible, umwelt- und gemeinwohlorientierte soziale Wesen das Maß gelingender Zivilisation sind. Wir wollen weniger »quantified self« und mehr »qualified we«.

Daher eignet sich Resonanz auch in besonderer Weise für ein neues ökologisches und soziales Bewusstsein: Wer Resonanz sucht, entwickelt vermutlich ein höheres Maß an Empfänglichkeit sowohl für Natur und Umwelt als auch für Mitmenschen. Eine Stärkung der Voraussetzungen für

thoughts are summarized as follows: “The main striving of modernity focuses on increasing its own reach: The world is to become economically and technically available, scientifically observable and controllable, legally predictable, politically manageable, and, at the same time, controllable and experienceable for everyday practice. This available world, so Hartmut Rosa’s controversial theory goes, is, however, a silent one with which a dialogue no longer exists. Rosa opposes this increasing alienation of humans and the world with ‘resonance,’ a sounding, unpredictable relationship to a non-available world.”

If acceleration is the problem, then—according to Rosa—resonance might be the solution. Resonance can deliver the normative yardstick for a successful life by no longer measuring the quality of life only indirectly by the increase of material wealth, options, and resources, but instead directly by the quality of one’s relationship to the world. This could, for example, be an inspiring conversation with another person or the use of an everyday object whose beauty one appreciates. A good life would then be one rich in experience of resonance and providing stable conditions for experiencing resonance.

Rosa tries to establish resonance as a metacriterion of a successful life and, based on his resonance theory, embarks on a quest for “the other” in the sense of a better form of existence. Resonance is not conceptualized as value-free but instead—considering important manifestations of the sensitivity toward resonance such as empathy, sensibility, and emotionality—provides a clear idea of a direction toward which our society could be reconstructed. In a totally interconnected and calculated world, resonance—as the unpredictable and unavailable—appears to be the key concept for designing a desirable different world in which not mass consumption but quality of life is increasing and the measure of a successful civilization is not digital algorithms and Big Data but sovereign citizens as resonance-sensitive social beings oriented toward the environment and the common good. We want less “quantified self” and more “qualified we.”

Hence, resonance also particularly lends itself to a new ecological and social awareness: If you are looking for resonance, you will probably be much more susceptible to both nature and the environment and to fellow humans. Strengthening the conditions for experiencing resonance is also a fundamental requirement for the much-needed further development of democracy.

I am aware of the fact that these ideas at first sight might appear to primarily address people who can financially afford to change their lives. These people have to become models for positive change—in the Western industrialized nations and elsewhere. This, however, cannot mean that change is a luxury, quite the contrary: The necessary change of direction will affect all people in all countries of the world.

das Erleben von Resonanz ist auch ein wesentliches Erfordernis für die dringend notwendige Weiterentwicklung unserer Demokratien.

Mir ist bewusst, dass diese Überlegungen auf den ersten Blick vorrangig an Menschen gerichtet erscheinen, die sich eine Änderung ihres Lebens finanziell leisten können. Solche Menschen müssen Modelle eines positiven Wandels werden, in den westlichen Industriestaaten und anderswo. Das kann aber nicht bedeuten, dass »Change« im Sinne positiven Wandels ein Luxus ist, ganz im Gegenteil: Die notwendige Richtungsänderung betrifft alle Menschen in allen Ländern der Welt. Die jeweiligen Möglichkeiten mögen unterschiedlich sein, Ansätze für Verhaltensänderung sind aber überall und in allen Teilen der Bevölkerung vorstellbar. Wo ein Wille ist, da lassen sich auch Wege finden.

Als zunehmend maschinengesteuerte Menschen müssen wir alles daransetzen, innovative KI in den Dienst unserer Werte zu stellen, und diese Werte müssen maßgeblich in innovative Geschäftsmodelle einfließen. Es geht also darum, das durch die Digitalisierung eröffnete Innovationspotenzial zu nutzen, um jene Werte nachhaltig zu verankern, auf die wir unsere Zukunft bauen wollen. Wir brauchen somit eine ganzheitlich ausgerichtete, wertebasierte Innovation, »values-based innovation« (VBI). Zu diesem Zweck gilt es, die neue unternehmerische Avantgarde (Start-ups, Spin-offs, »social entrepreneurs« und sonstige Unternehmen, speziell innovative Klein- und Mittelbetriebe, die zu positivem Wandel beitragen wollen) mit der neuen Kreativavantgarde in Design, Mode, Architektur und bildender Kunst strukturiert zu vernetzen. Die Erarbeitung angewandter Werte soll Ausgangspunkt für weiterführende Fragestellungen und daran anknüpfende innovative digitale Geschäftsmodelle (gewinnorientiert oder »not for profit«) sein, die den Übergang vom Massenkonsum zur Kreislaufwirtschaft vorantreiben und dazu beitragen, möglichst vielen Menschen ein sinnstiftendes Leben im digitalen Zeitalter zu ermöglichen.

Eine technologiebesessene Zukunft ohne Werte ist wertlos. Wir brauchen eine breite öffentliche Diskussion darüber, welche traditionellen und neuen Werte wir für die Gestaltung der Zukunft benötigen. »Tradition ist nicht die Anbetung der Asche, sondern die Weitergabe des Feuers.« Dieser Sinnspruch – meist Gustav Mahler zugeschrieben, tatsächlich stammt er etwas komplexer formuliert von dem französischen Philosophen und Politiker Jean Jaurès (1910) – bringt auf wunderbare Weise zum Ausdruck, wie Tradition Veränderung inspirieren kann und soll. Ich möchte diesen Gedanken auf unseren wünschenswerten Umgang mit neuen Technologien übertragen: Zukunftsgestaltung – und damit die Weiterentwicklung unserer Zivilisation – ist nicht die Anbetung der jüngsten Technologien, sondern die technologieunterstützte Erneuerung unserer menschlichen Werte. ×

VIENNA BIENNALE FOR CHANGE 2019: SCHÖNE NEUE WERTE. Unsere digitale Welt gestalten

Zum dritten Mal veranstalten das MAK, die Universität für angewandte Kunst Wien, die Kunsthalle Wien, das Architekturzentrum Wien und die Wirtschaftsagentur Wien sowie das Slovak Design Center als neuer Associate Partner und das Austrian Institute of Technology (AIT) als außeruniversitärer Forschungspartner die VIENNA BIENNALE, die Kunst, Design und Architektur zur Frage einer wertebasierten Zukunft ins Spiel bringt.

VIENNA BIENNALE FOR CHANGE 2019: BRAVE NEW VIRTUES. Shaping Our Digital World

For the third time, the MAK, the University of Applied Arts Vienna, Kunsthalle Wien, Architekturzentrum Wien, and the Vienna Business Agency, as well as the Slovak Design Center as new Associate Partner and the Austrian Institute of Technology (AIT) as non-university research partner, are organizing the VIENNA BIENNALE, which brings art, design, and architecture into play on the question of a value-based future.

→ viennabiennale.org

The respective possibilities may differ, but first steps toward behavioral change can be conceived everywhere and in all parts of society. Where there's a will, ways can be found.

As increasingly machine-driven humans, we should do everything in our power to make innovative AI serve our values; and these values must play a crucial role in innovative business models. The aim is to make use of the innovation potential opened up by digitization in order to firmly anchor sustainability for those values upon which we want to build our future. We therefore need "values-based innovation" (VBI) with a holistic focus. For this purpose, the new entrepreneurial avant-garde (start-ups, spin-offs, social entrepreneurs, and other enterprises, especially small and middle-sized businesses wanting to contribute to positive change) has to be connected in a structured way with the new creative avant-garde in design, fashion, architecture, and fine art. Developing applied values should be the starting point for further questions and resulting innovative digital business models (profit-orientated or not-for-profit) that promote the transition from mass consumption to circular economy and contribute to providing a meaningful life for as many people as possible in the digital era.

A future obsessed with technology but without values is worthless. We need a broad public discourse on which traditional and new values we will need to shape the future. "Tradition is not worshiping the ashes but passing the flame." This aphorism—often credited to Gustav Mahler, actually phrased by Jean Jaurès, a French philosopher and politician, in a slightly more complex fashion in 1910—expresses in a wonderful way how tradition can and should inspire change. I would like to transfer this idea to the way we should ideally treat new technologies: Shaping our future—and, therefore, developing our civilization further—is not worshiping the latest technologies but renewing our human values with the support of technology. ×

Trevor Paglen arbeitet seit langer Zeit zu den Themen Überwachung und der politischen Dimension von Technologien. In seiner fotografischen Serie *Adversarially Evolved Hallucinations* ließ er zwei KI-Systeme – ein bilderkennendes und ein bildgenerierendes – aufeinander reagieren.

Trevor Paglen has been working on surveillance and the political dimension of technologies for a long time. In his photo series *Adversarially Evolved Hallucinations,* he has two AI Systems—one that recognizes and one that generates images—react to each other.

→ uncannyvalues.org

VIENNA BIENNALE FOR CHANGE 2019
Teil der Ausstellung
UNCANNY VALUES. Künstliche Intelligenz & du

Part of the exhibition
UNCANNY VALUES. Artificial Intelligence & You

CREDITS:
Exhibition view *UNCANNY VALUES. Artificial Intelligence & You;* from left to right: Trevor Paglen, *Porn (Corpus: The Humans), Adversarially Evolved Hallucination,* 2017; *A Man (Corpus: The Humans), Adversarially Evolved Hallucination,* 2017; *Vampire (Corpus: Monsters of Capitalism), Adversarially Evolved Hallucination,* 2017
Courtesy of the artist and Metro Pictures, New York

MAK Exhibition Hall
© Aslan Kudrnofsky, MAK

Alpbacher Technologiegespräche »Freiheit und Sicherheit«

22. – 24.08.2019

Die Alpbacher Technologiegespräche werden vom AIT – Austrian Institute of Technology, Österreichs größter Research-and-Technology-Organisation, und ORF Radio Österreich 1 veranstaltet. Das Projekt wird von Mag. Michael H. Hlava (AIT) und Dr. Martin Bernhofer (ORF Ö1) geleitet, das Projektbüro von Claudia Klement (AIT). Dem Steering Committee der Alpbacher Technologiegespräche gehören Dr. Hannes Androsch (Vorsitzender des Aufsichtsrats des AIT, Vorsitzender des Rats für Forschung und Technologieentwicklung), Prof. Dr. Wolfgang Knoll (wissenschaftlicher Geschäftsführer des AIT) und Monika Eigensperger (Radiodirektorin ORF) an.

Wissenschaftliche Partner der Alpbacher Technologiegespräche 2019 sind die Helmholtz-Gemeinschaft Deutscher Forschungszentren sowie das European Research Council (ERC), Industrial Partner ist die Industriellenvereinigung (IV).

Die Veranstaltung wird maßgeblich vom österreichischen Bundesministerium für Verkehr, Innovation und Technologie (BMVIT), vom Bundesministerium für Digitalisierung und Wirtschaftsstandort (BMDW) sowie vom Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) unterstützt.

Den rasanten technologischen und gesellschaftlichen Entwicklungen nähern sich die Technologiegespräche 2019 aus dem Blickwinkel »Freiheit und Sicherheit«. Das alles vernetzende Internet hat ungeahnte Freiheiten geschaffen, Information und Bildung für alle versprochen, aber auch seine dunklen Seiten wie Cyberkriminalität, Mobbing und gezielte Manipulation gezeigt. Das Internet der Dinge erweitert nun auch noch unsere Sinne; kluge, mit künstlicher Intelligenz gepaarte Assistenten und Roboter nehmen uns unangenehme Arbeiten ab. Wie wollen wir also diese digitale Welt gestalten? Die Technologiegespräche versuchen, Antworten zu geben. ×

Alpbach Technology Symposium “Liberty and Security”

August 22—24, 2019

The Alpbach Technology Symposium is organized by AIT—Austrian Institute of Technology, Austria’s largest research and technology organization, and ORF Radio Österreich 1. The project is managed by Mag. Michael H. Hlava (AIT) and Dr. Martin Bernhofer (ORF Ö1); Claudia Klement (AIT) is head of the project office. The Alpbach Technology Symposium’s Steering Committee includes Dr. Hannes Androsch (head of the supervisory board of AIT, chairman of the Austrian Council for Research and Technology Development), Prof. Dr. Wolfgang Knoll (scientific managing director of AIT), and Monika Eigensperger (radio director ORF).

Scientific partners of the Alpbach Technology Symposium 2019 are the Helmholtz Association of German Research Centres and the European Research Council (ERC); its industrial partner is the Federation of Austrian Industries (IV).

The Symposium is substantially supported by the Austrian Federal Ministry for Transport, Innovation and Technology (BMVIT), the Austrian Federal Ministry of Digital and Economic Affairs (BMDW), and the Austrian Federal Ministry of Education, Science and Research (BMBWF).

The Alpbach Technology Symposium 2019 explores the rapid technological and social developments of recent years from the perspective of “Liberty and Security.” Linking anything and everything, the Internet has offered unexpected freedom, promised information and education for all, but also shown its dark sides like cybercrime, mobbing, and calculated manipulation. The Internet of things is now even extending our senses, and clever assistants and robots paired with artificial intelligence relieve us of nasty chores. How do we intend to design this digital world? The Technology Symposium tries to provide answers. ×

Jahrbuch anlässlich der Alpbacher Technologiegespräche 2019
Yearbook on the occasion of the Alpbach Technology Symposium 2019

TEC

Alpbach Technology Symposium
Alpbacher Technologiegespräche

Idee und Konzept Idea and concept
Hannes Androsch, Michael H. Hlava, Martin Kugler
Alpbacher Technologiegespräche

Sarah Hellwagner, Clemens Kopetzky
art:phalanx, Kultur & Urbanität

Medieninhaber Media owners
art:phalanx, Kultur und Urbanität

Herausgeber Publishers
Hannes Androsch, Wolfgang Knoll, Anton Plimon und art:phalanx Kommunikationsagentur GmbH, Wien

Projektmanagement Project management
Sarah Hellwagner, Selina Kainz
art:phalanx, Kultur & Urbanität

Redaktion Editor
Martin Kugler

Lektorat Copy-editing
Wolfgang Astelbauer
Michael Strand, Wien; Brigitte Willinger, Wien

Grafische Gestaltung Visual design
The Graphic Society, KettnerVogl

Druck Printed by
Medienfabrik Graz GmbH

Lithografie Lithography
Pixelstorm, Wien

Papier Paper
Munken Polar, Fedrigoni Tatami White

Schriften Fonts
Vista Sans, Vista Slab (Xavier Dupré)

Verlag Publishing house
Verlag Holzhausen GmbH

Bildnachweis Photo credits
S./p. 6: © AIC, Peter M. Mayr; S./p. 42: © Redtenbacher; S./p. 76: © IRKS; S./p. 100: © privat; S./p. 164: © David Payr; S./p. 186: © MAK, Sabine Hauswirth

1. Auflage 2019 1st Edition 2019
ISBN 978-3-903207-36-3

Printed in Austria, EU
Alle Rechte vorbehalten
All rights reserved

Bibliografische Informationen der Österreichischen Nationalbibliothek und der Deutschen Nationalbibliothek
Die ÖNB und die DNB verzeichnen diese Publikation in den Nationalbibliografien; detaillierte bibliografische Daten sind im Internet abrufbar. Für die Österreichische Bibliothek: http://onb.ac.at, für die Deutsche Bibliothek: http://dnb.ddb.de.

Bibliographic information published by the Österreichische Nationalbibliothek and the Deutsche Nationalbibliothek
The ÖNB and the DNB are listing these publications in the Nationalbibliografien; detailed bibliographic data are available on the Internet. For the Österreichische Nationalbibliothek: http://onb.ac.at; For the Deutsche Nationalbibliothek:http://dnb.ddb.de.

Aus Gründen der Lesbarkeit wurde verzichtet, durchgängig geschlechtsspezifische Formulierungen zu verwenden. Soweit personenbezogene Bezeichnungen nur in männlicher Form angeführt sind, beziehen sie sich auf Männer und Frauen in gleicher Weise.

Checkliste für mehr Cybersicherheit
Checklist for Improved Cybersecurity

1 Vorsicht bei der Weitergabe persönlicher Daten
Be careful with sharing data!

Das Internet hat ein langes Gedächtnis, und auch für nichtöffentliche Inhalte gibt es keine Garantie, dass sie nicht doch irgendwann einmal in falsche Hände geraten. Überlegen Sie daher genau, was Sie im Internet von sich preisgeben.
The Internet has a long memory, and even non-public content may fall into the wrong hands at some point. So be careful with personal information you decide to reveal on the Internet!

2 Schutz der Privatsphäre
Protect your private sphere!

Vor allem Kinder und Jugendliche gehen mit dem Schutz der eigenen Privatsphäre oft nicht sehr aufmerksam um. Aber auch bei vielen Erwachsenen herrscht ein mangelndes Bewusstsein, dass die Privatsphäre ein schützenswertes Gut ist.
It is frequently children and adolescents who are rather careless when it comes to protecting their own private spheres. But also many adults are not sufficiently aware of the fact that one's private sphere is a protectable asset.

3 Sicherheitsmaßnahmen von Anfang an integrieren
Integrate security features from the very beginning!

Unzureichende Standardeinstellungen und falsche Konfigurationen sind der Grund für viele Sicherheitsvorfälle. Es muss sichergestellt werden, dass alle Computer nach dem neuesten Stand der Technik konfiguriert sind.
Insufficient default settings and wrong configurations lead up to many security incidents. Make sure that all computers are configured based on state-of-the-art technology!

4 Verschlüsselung
Encrypt your data!

Verschlüsseln Sie sensible Daten sowohl bei der Übertragung als auch bei der Speicherung (auch auf Speichermedien wie tragbaren Festplatten oder USB-Sticks).
Encrypt sensitive data when transmitting or storing them (also on such storage media as portable hard disks and USB sticks).

5 Passwörter regelmäßig wechseln
Change your passwords regularly!

Passwörter sollten regelmäßig geändert werden. Wichtig ist, das vorherige Passwort nicht bloß um einzelne Zeichen zu ergänzen. Es gibt diverse Strategien für sichere Passwörter, die man sich auch merken kann: Man kann sich z. B. einen Passwortsatz merken und das Passwort aus den Anfangsbuchstaben der Wörter dieses Satzes zusammenstellen. Effektiv ist auch, Buchstaben nach einem persönlichen Plan durch Sonderzeichen und Zahlen zu ersetzen.
Passwords should be changed regularly. It is important to not merely add a few individual signs to a previous password. There are various strategies for secure passwords that are also easy to remember: for example, one can memorize a password sentence and compose the password of the first letters of the words of this phrase. It can also be useful to replace certain letters with special characters or numbers.

6 Unterschiedliche Passwörter für unterschiedliche Anwendungen
Use different passwords for different applications!

Für unterschiedliche Webseiten und Anwendungen sollte man unbedingt unterschiedliche Passwörter benutzen. Und: Man sollte Passwörter niemals an andere Personen weitergeben – so vertrauenswürdig diese auch sein mögen.
Different passwords should be used for different websites by all means. And you should never pass on your passwords to others, no matter how much you trust them.

7 Benutzungsrichtlinien
User guidelines

In Firmen ist die Erstellung einer Benutzungsrichtlinie hilfreich, um das von Mitarbeitern erwartete Verhalten zu beschreiben. Arbeitnehmer sollten eine Vereinbarung unterzeichnen, in der festgehalten wird, dass unerlaubter Datenzugriff ein schwerwiegendes Vergehen darstellt. Es sollte über die Wahl von sicheren Passwörtern, physische Schutzmaßnahmen und die Risiken externer Festplatten aufgeklärt werden.
In companies it is helpful to draw up user guidelines to define the behavior expected from employees. Employees should be asked to sign an agreement stating that unauthorized access to data constitutes a serious offense. And they should be informed about secure passwords, physical protection measures, and the risks of external hard disks.

8 Trennung von Rolle und Funktion
Separation of role and function

In Firmen sollte mit entsprechenden Richtlinien verhindert werden, dass ein einziger Arbeitsnehmer seine Befugnisse missbrauchen kann. So sollten etwa Accounts mit hoher Berechtigungsstufe vom normalen Account des Nutzers getrennt werden.
In companies pertinent guidelines should prevent individual employees from misusing their competencies. For example, accounts with high authorization levels should be separated from the user's regular account.

9 Funktionsbasierte Zugriffsrechte
Function-based access authorization

Ändert sich die Rolle eines Arbeitnehmers innerhalb der Organisation, sollte das Unternehmen die Zugriffsrechte formell neu überprüfen. Passwörter, die dem Arbeitnehmer in seiner früheren Rolle oder Funktion bekannt waren, sollten geändert werden.
When an employee's role within the organization has changed, the company should formally recheck his or her access authorization. Passwords an employee has been familiar with in his or her former role or function should be changed.

10 Vereinbarungen mit Dritten
Agreements with third parties

Viele Datenschutzverletzungen gehen auf das Konto von vertrauenswürdigen Dritten. Diese sollten daher Benutzungsrichtlinien unterschreiben und nur Programme nutzen dürfen, die den üblichen Sicherheitskriterien (Firewalls, Virenschutz etc.) entsprechen.
Violations of data protection are frequently caused by trustworthy third parties. They should therefore be asked to sign user guidelines and only be permitted to use programs in line with standard security criteria (firewalls, virus protection, etc.).

Quellen Sources

AIT, ÖIAT

Neue Spielregeln für die Cyberwelt

Wie seinerzeit der Übergang vom Agrar- ins Industriezeitalter bringt das digitale Zeitalter eine Veränderung aller Lebensbereiche mit sich, allerdings in noch größerem Ausmaß und atemberaubendem Tempo. Die Transformation wirft viele Fragen auf, die bisher ungelöst sind – ethische und juristische ebenso wie ökologische, ökonomische, soziale und politische. Dazu kommen neue Gefahren aus der Cyberwelt: Je mehr Arbeit uns digitale Technologien abnehmen, umso abhängiger werden wir von ihnen – und umso schlimmer wird es, wenn sie ausfallen, manipuliert oder angegriffen werden. Das macht uns extrem verwundbar. Die Umbrüche und neuen Risiken erzeugen Unsicherheit, Sorgen und Ängste. Das zunehmende Unsicherheitsgefühl ist eine Quelle, aus der politisches Kapital geschlagen werden kann.

Dieses Jahrbuch zu den Technologiegesprächen Alpbach 2019 widmet sich zahlreichen Aspekten des Themas Cybersecurity sowie des Verhältnisses zwischen Sicherheit und Freiheit. Neben aktuellen Gefahren und Trends wird vor allem das weite Gebiet der Sicherheitsforschung beleuchtet. Eine Reihe von Interviews und Positionen der zeitgenössischen Kunst runden den Band ab.

New Rules for the Cyberworld Game

Similar to the transition from the agricultural to the industrial age, the digital age brings about change in all spheres of life, but on an even larger scale and at breathtaking speed. The transformation raises many unresolved questions: ethical and legal as well as ecological, economic, social and political ones. Moreover, we find ourselves faced with new dangers from the cyberworld: the more work digital technologies do for us, the more dependent we become on them—and the worse it gets if they fail, are manipulated, or attacked. That makes us enormously vulnerable. These upheavals and new risks create insecurity, worries, and fears. The growing sense of insecurity is a source from which political capital can be made.

This yearbook accompanying the 2019 Alpbach Technology Symposium explores numerous aspects of cybersecurity and the relationship between security and freedom. It highlights not only current dangers and trends but also the wide field of security research. A series of interviews and positions in contemporary art round off the volume.

9 783903 207363