CYBERSECURITY CALL

DEFINING THREATS
APPLYING SOLUTIONS

IZABELA ALBRYCHT, SIMONA AUTOLITANO, MICHAŁ KRAWCZYK,
PIOTR MARCZUK, ARWID MEDNIS, ROBERT SIUDAK,
JOANNA ŚWIĄTKOWSKA

THE KOSCIUSZKO INSTITUTE

CYBERSECURITY CALL

DEFINING THREATS
APPLYING SOLUTIONS

AUTHORS: IZABELA ALBRYCHT, SIMONA AUTOLITANO,
MICHAŁ KRAWCZYK, PIOTR MARCZUK, ARWID MEDNIS,
ROBERT SIUDAK, JOANNA ŚWIĄTKOWSKA

THE KOSCIUSZKO INSTITUTE

AUTHORS:

THE KOSCIUSZKO INSTITUTE

Izabela Albrycht
The rise of AI is the rise of cyberthreats

Michał Krawczyk
Cyberattacks – statistics at a glance

Robert Siudak
Security through innovation - case studies

Joanna Świątkowska, PhD
New front lines of cybersecurity

PWC

Arwid Mednis, PhD
Cybersecurity: key regulatory aspects

MICROSOFT

Simona Autolitano, Piotr Marczuk
Cybersecurity: key regulatory aspects

TRANSLATION: Błażej Bauer, Justyna Kruk PROOFREADING: Adam Ladziński TYPESETTING: Joanna Świerad-Solińska

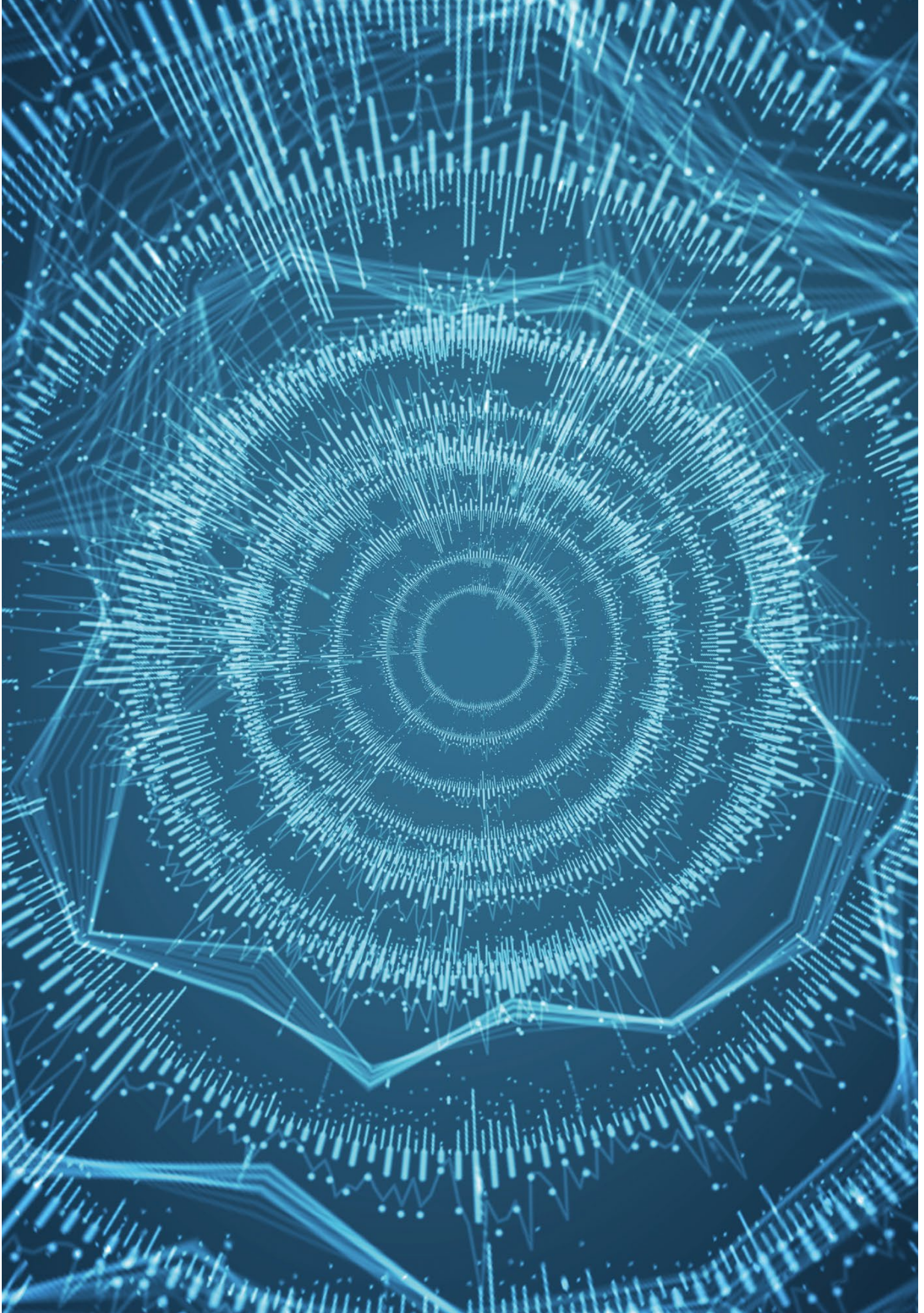
PARTNERS OF THE REPORT:

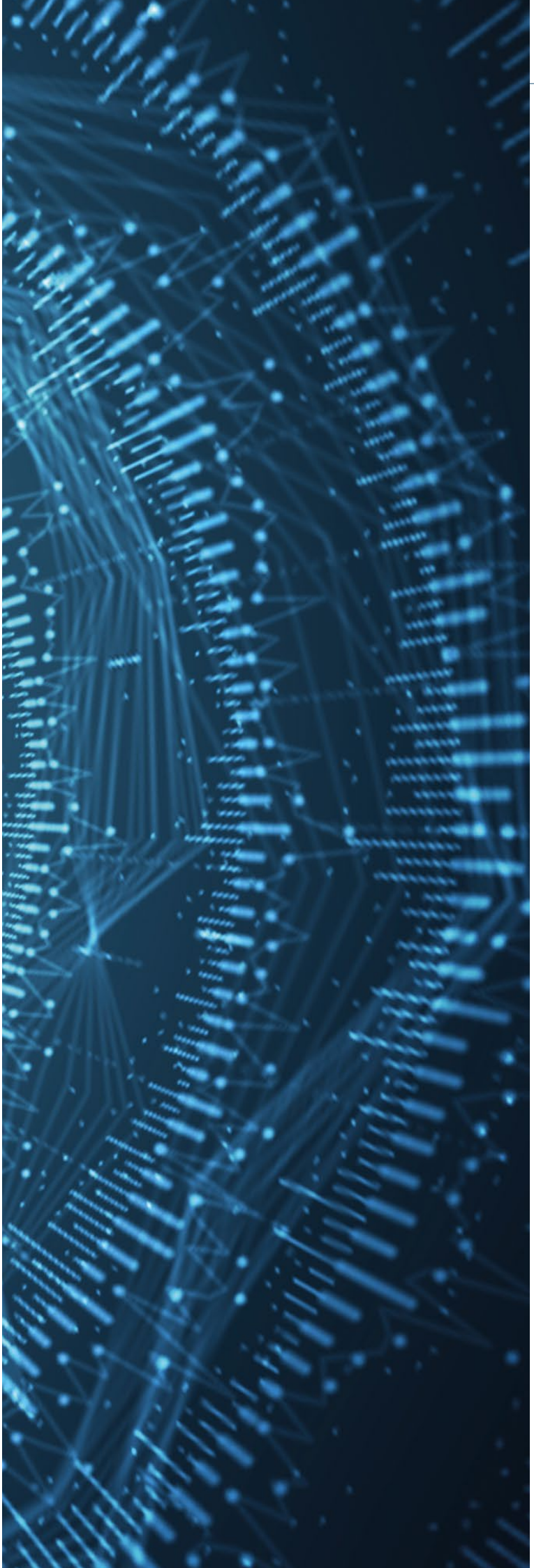
Acknowledgements: Malina Jankowska (PwC), Artur Kozłowski (Integrity Partners), Błażej Marciniak (Fudo Security), Joanna Miazga (STM Solutions), Dagmara Nikowska (Vector Synergy), Marek Ostafil (Cyberus Labs), Asen Petrov (Predica), Robert Posłajko (Axence), Miłosz Smolarczyk (Cryptomage), Ewa Wysłocka (Vector Synergy), Marek Zaleski (Microsoft).

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10,
31-130 Krakow, Poland
Phone: 00 48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

Krakow, 2019

CONTENTS





EXECUTIVE SUMMARY

The implementation of new digital technologies can bring enormous added value for economies the world over. The estimates say artificial intelligence is going to raise global GDP by 13 trillion dollars by 2030, which involves a yearly growth of around 1.2% (McKinsey and Company), whereas the 5G network is going to be able to generate 3 trillion dollars between 2020 and 2035 (IHS Markit). Competition in the technological realm between global state powers turned out to be the most important game changer in the second decade of the 21st century. It directly influences gaining advantage in social, economic and military dimensions. Digitising the economy and building the ICT sector are the most significant driving forces of economic growth, whereas military effectiveness hinges on the level of technological development.

An entire panoply of cyberthreats is also spreading right in front of us, including those that can lead to a paralysis of the digital world. For many years, we have been watching cyberattacks become a weapon in the hands of not only non-state actors but also governments. As a result of cyberattacks, in 2017 the world economy lost over 600 billion dollars altogether (McAfee&CSIS). Zurich Insurance forecasts indicate that in 2030 such losses will grow to 1.2 trillion dollars, which equals 0.9% of world GDP. A cyberattack may paralyse the operation of whole economic sectors, which the NotPetya attack strikingly illustrated as it generated 10-billion-dollar losses in 2017.

Faced with all of that, the dynamics of digital world must result in collective and responsible actions. The call for cybersecurity is a must.

SECURITY THROUGH INNOVATION

If we want modern technologies to drive our social and economic development in a sustainable manner, security must become the backbone of their progress. But that is not the end. "Security by design" principle shall be accompanied by innovations provided by dedicated cybersecurity solutions and implemented into the economy in a more agile manner. Currently, the global market of cybersecurity products and services is shaped to a great extent by American and Israeli ecosystems with their unique mesh-ups of startups, SMEs, corporates and academia. With eight case studies we include in this report, we want to show that Central and Eastern Europe, and especially Poland, might also become a vital part of the innovation-driven quest for cybersecurity. Polish developers and hackers won almost every well-known cyber contest from the Capture the Flag cycle (2014, 2018) through Locked Shields (2014) to the unofficial developers' world cup – Hello World Open (2014). Slowly, this abundance of cyber talents is also transforming the market with a growing number of innovative products being developed by start-ups and scale-ups from Poland.

ALL FOR ONE. ONE FOR ALL

The range, scale, sophistication and nature of cyberthreats are evolving dramatically, including digital threats that can jeopardise democratic processes. It requires a constant analysis of the changing environment and agile adaptability by each and every player, consequently their roles and tasks must be modified. Cyberspace has become a scene for many serious confrontations involving nations and their resources. But new types of cyberspace-enabled conflicts are involving not only state-owned entities, therefore the private sector is starting to play an ever-important part in building cybersecurity.

The private sector, especially technology companies as the suppliers of products and services and the end customers, has largely determined the shape and development of the new technology market. The companies' potential impact on the security of nations and societies is growing and they are playing multidimensional roles. The challenges facing the private sector reflect well the general trends in the field of cybersecurity. Its members are often at the front line of the battle against network security threats. They are also used for pursuing digital attacks both against machines and against our minds. IT system and network providers, internet platforms and social media were harnessed to wage digital and information warfare numerous times. It increases their responsibility, and on the other hand it gives them a completely new role to play – as a vital link in the security chain. Private entities must settle into this new role. There is no doubt that running business in the ICT sector brings huge benefits and opportunities. But they go hand in hand with equally large responsibility. Technology companies should:

- introduce security by design that embeds strong cybersecurity foundations into products and services in the entire value chain, throughout their entire life cycle;
- impose appropriate mechanisms e.g. to maintain customers privacy;
- launch initiatives that tackle strategic cybersecurity problems (an example: Global Internet Forum to Counter Terrorism);
- take actions at a strategic level by building platforms of cooperation within the digital sector and influencing the surrounding environment in order to make it more secure and to proactively raise a greater level of cybersecurity and increase trust in new technologies (for instance The Paris Call, Cybersecurity Tech Accord, the Charter of Trust).

State actors must understand that in addition to laying down requirements, commercial enterprises must receive broad support for their efforts, which at the end of the day are critical for entire societies.

TWO FACES OF THE ARTIFICIAL INTELLIGENCE

AI has just triggered runaway technological growth and might be considered a game changer in economy, politics and defence. In the hands of cybercriminals and hostile states, AI will make cybersecurity landscape even more complex. That is why the way we deploy AI will serve as a litmus test of the maturity and effectiveness of multi-stakeholder cybersecurity environment.

Unfortunately, cyber-world will not be a safer place once we deploy full-bodied AI and chief on the list of future digital threats are possible vulnerabilities and risks of the AI-augmented economy and weapons. AI-enhanced cyberattacks will be more frequent, automated and devious, while their detection and attribution will become even more complicated and uncertain. As a result, while implementing AI in all sectors of our lives, we need to consider both the bright and the dark side of the process.

Forms of AI-enhanced cyberattacks and threats both on our machines and minds we expect to see in the near future: weaponisation and dual-use of AI, AI-boosted phishing attacks, smart and devious malware, automated multi vector cyberattacks, deepfakes, AI-enhanced surveillance, fake data injection attacks, exploitation of AI algorithms and training models.

A REGULATORY ANSWER FOR CYBERTHREATS

Cyberattacks may be able to affect individual Member States as well as the entire EU. Security of network and information systems therefore affects the efficiency of internal markets. In recent years, an increase in the number of incidents posing threats to the operation of network and information systems has been observed in the European Union and met with regulatory actions introduced by the European Commission. One of the most important among them has been the NIS Directive, which include requirments for all Member States to adapt their national strategies on the security of network and information systems and to create a computer security incident response teams network.

Poland's Act of 5 July 2018 concerning national cybersecurity strategy is an example of implementing the NIS Directive and is presented in this report.

Other cybersecurity regulations and laws on the EU level include:

- **Recommendations on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (2017)**
- **Cyber diplomacy toolbox (2017)**
- **ePrivacy Regulation (2002, forthcoming)**
- **Open Data Directive (forthcoming)**
- **Cybersecurity Act (forthcoming)**

Especially the so-called Cybersecurity Act underlines an important aspect of cybersecurity, which is **standardisation.** The regulation is now being proceeded by the EC and will broaden the role of the European Union Agency for Network and Information Security, especially as regards the certification of various devices, services and processes in terms of immunity to cyberattacks; certificates will be applicable in the entire EU.

SECURITY THROUGH INNOVATION – CASE STUDIES

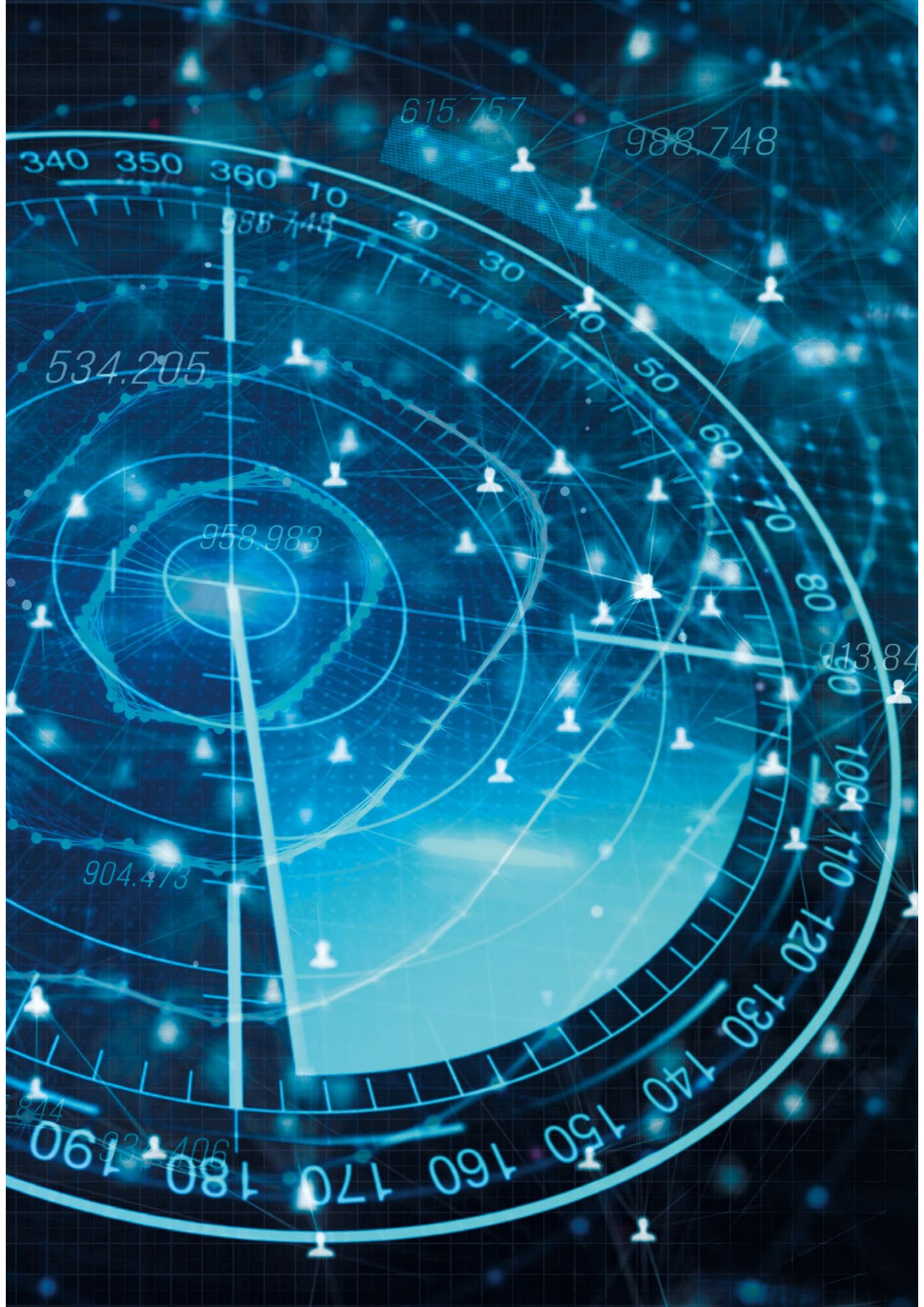
THE GLOBAL CYBERSECURITY MARKET OF PRODUCTS AND SERVICES HAS BEEN ESTIMATED TO BE WORTH BETWEEN 120 AND 150 BILLION DOLLARS IN 2018. THE UNITED STATES IS LEADING AS THE PRIME PROVIDER OF SOLUTIONS WORLDWIDE, FOLLOWED BY SEVERAL ASIAN COUNTRIES. IN THIS SECTION WE GATHERED EIGHT CASE STUDIES SHOWING THAT COMPANIES FROM CENTRAL AND EASTERN EUROPE, AND ESPECIALLY FROM POLAND, ALSO HAVE THE POTENTIAL TO SHAPE THE GLOBAL CYBERSECURITY MARKET IN THE COMING YEARS...

TESTING GROUND FOR CYBER SOLDIERS

2 million vacancies – this is the estimated global shortage of computer security experts today. CDeX (Cyber Defence eXercise Platform), created by Vector Synergy from Poznan, is rising to this very challenge – it supports training the required workforce and helps develop skills of staff responsible for IT security

Research institutions subordinate to the European Space Agency faced sophisticated attacks on their IT infrastructure. Over the past 3 months, there have been attacks on several institutions which are involved in development of hardware and software for the next generation of telecommunications satellites... is how one of CDeX training scenarios only just begins. In each of them, two teams compete with each other, customarily called Blue Team and Red Team. The task of Blue Team is to defend systems attacked by Red Team, whose actions may be based on automated scripts of their choice or on activity of experts who are behind CDeX. Training takes place in real time, within the customer's ICT infrastructure. It also features elements of gamification, such as achievable objectives and dedicated scoring, meant to enhance user experience and, by doing so, facilitate learning. The training not only brings participants notable benefits but also provides management boards with valuable information – following each session, a detailed report is generated which covers both actions of the players and weaknesses of the customer's IT infrastructure as well as possible consequences of them being taken advantage of outside the test environment.

Users of the platform include ministries of national defence, financial institutions and consultancy firms. Among them is the Polish Naval Academy in Gdynia, where CDeX is used for training future officers of the Polish Armed Forces. Two variants of CDeX are available at the moment: one is a direct implementation on the customer's server or in a cloud; the other consists in purchasing individual trainings for employees in the platform operated by Vector Synergy. A subscription-based model for individual customers is expected to be introduced in the late second quarter of 2019, with the purpose of making cybersecurity expertise available to anyone new to the field. In order to offer that, the platform is going to be extended to include e-learning; users will be able to purchase individual trainings and courses, have their results stored, and generate certificates upon completing their planned training paths.

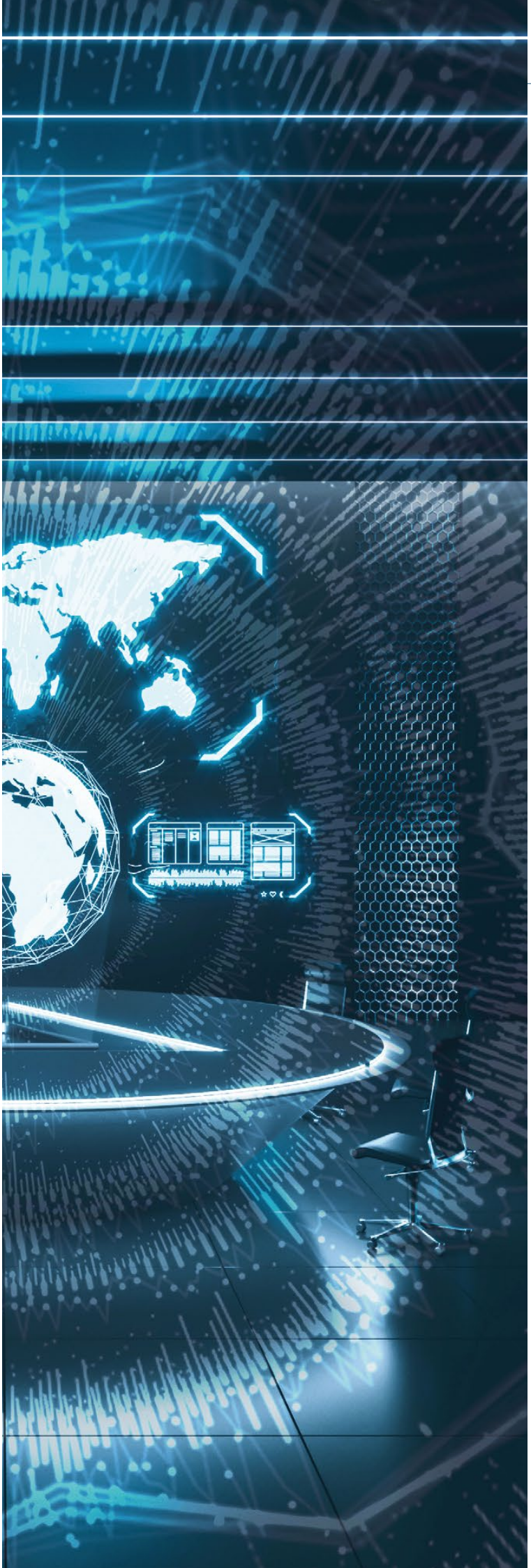

615.757
988.748
340 350 360 10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160 170 180 190
534.205
958.983
904.473

UNDERSTANDING COMPUTER CONVERSATIONS

cryptomage®

Communication between laptops, smartphones or servers takes place in their own language. What is enabling this are communications protocols operating in the backgrounds of our systems. There is more than just monitoring employees or administrators' activity to securing a network – one has to monitor and understand "conversations" between computers. Cryptomage Cyber Eye makes this possible – through deep analysis of network traffic it ensures security on all levels.

Steganography is focused on how to conceal communication – both contents of messages and the overall fact of exchanging them. Whoever happens to investigate doings of cybercriminals may dare to say that many of them could form the elite of this discipline. Masking communication with servers which are managing "zombie" computers (botnets), hiding stolen data by retransmitting them or by setting them into packet headers, or sewing them into VoIP (Voice over IP) delays... These are just few examples of tactics aimed at getting sensitive data out of a system without its owner knowing. Luckily, on the "right side of the force" there are experts from Cryptomage. In the late 2018 the company, which employs a team of cybersecurity specialists, among them professors, doctors, hardware engineers, programmers and analysts, demonstrated a Polish invention meant to deal with threats like those outlined above: the Cryptomage Cyber Eye.



Cryptomage Cyber Eye sonde provides real-time detection and prediction of anomalies. Its functionality covers analysis of concealed communication too, based on network steganography, which makes it a unique innovation. Inspecting every single network packet, original steganography detection algorithms, original algorithms for botnets' communication with C2 (Command and Control) servers, artificial intelligence algorithms and low-level network protocol analysis (for 0-day and DDoS attacks) – all of that enable this device to understand and interpret "computers conversations". The sonde itself also works together with SIEM (Security Incident and Event Management) solutions.

By design, the sonde is able to overcome challenges faced in such areas as critical infrastructure, armed and uniformed forces, public administration, financial services (banking, insurance), telecommunications (operators, service providers), pharmacy or health protection. Obviously, it can serve as a useful tool for entities which are going to be classified as Operators of Essential Services according to the European NIS Directive requirements.

SECURING THE INTERNET OF THINGS

CyberusLabs

What would happen if 60% of all passwords and logins in the world were published today, and everyone could access the services these were meant to protect? Hard to imagine? Yet, as shown by research, this is what (un)security of the Internet of Things (IoT) currently looks like. Many manufacturers are using universal hard-coded credentials stored in their devices. Such security gaps are to be filled by the ELIoT Pro system from Cyberus Labs, where password authentication and communication within IoT systems are going to be replaced by the company's original cryptographic invention – Cyberus Key.

The purpose of Cyberus Key is to get rid of the weakest link of cybersecurity: passwords and other credentials. In order to achieve that, one signs in to services – bank accounts, for instance – using tokens. These are forwarded as audio signals, which are transmitted as part of communication between the browser and the mobile application. User authentication methodology is based here on the only encryption system that has not been cracked, from Gilbert Vernam, and offers an innovative cryptographic solution; a patent application has been filed at the European Patent Office. That solution was the starting point for developing the ELIoT Pro system, which is meant to provide secure and encrypted authentication and communication within the Internet of Things.

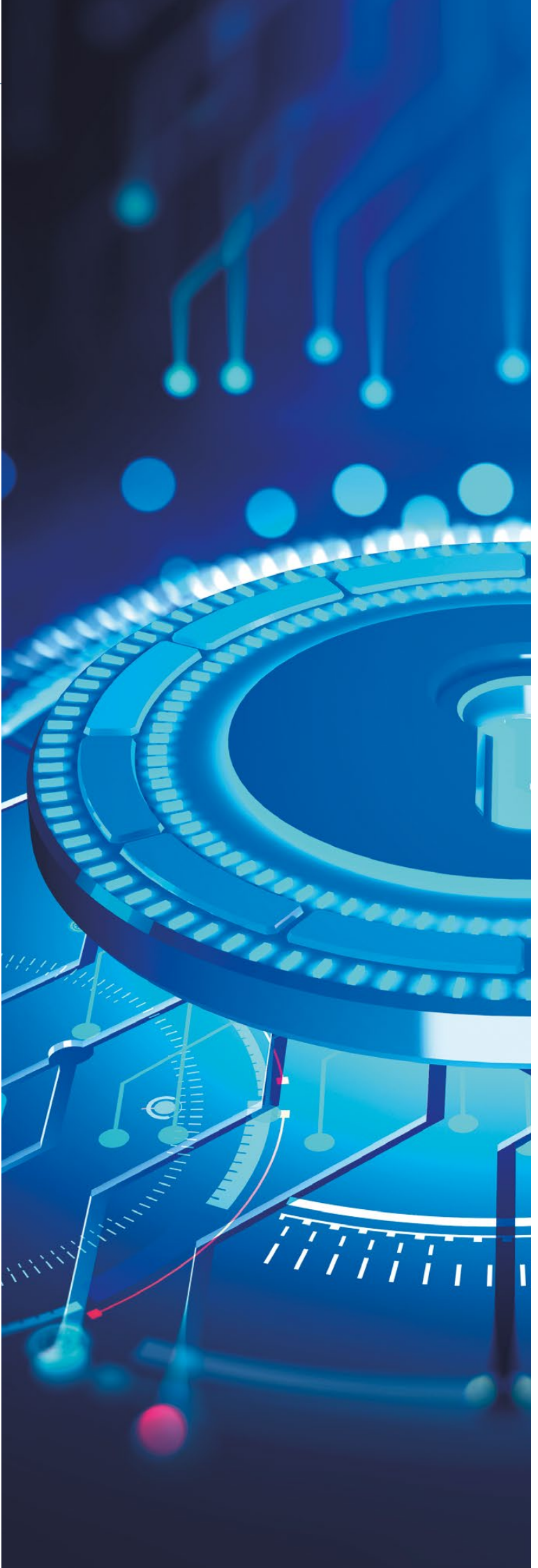
Protection of devices connected to the Internet of Things is not just a matter of security of data obtained from these individual endpoints – it is also a challenge for the Internet as we know it. In recent years, possible mass infection of poorly protected webcams, printers, garage doors or baby monitors has become a source of unprecedented distributed denial-of-service (DDoS) attacks. For example, hundreds of thousands of infected IoT devices gathered in a botnet were the means behind the 2016 attack on the web infrastructure supplier Dyn, which resulted in services like Airbnb, Spotify or Twitter being temporarily unavailable.

ELIoT Pro is a system which secures both the user's communication with his or her smart home or car (human-to-machine) and the information exchange between devices used for the purposes of Industry 4.0 or smart city systems (machine-to-machine). It ensures authentication of both users and devices as well as encryption of data exchanged between different locations. Also, it enables continuous monitoring of an entire IoT network, aimed at identifying anomalies. The goal of its developers is to introduce a comprehensive system for IoT security – one which could protect users, data and devices. The final product is going to be ready in mid-2019, and planned deployments will follow, in areas such as automotive industry, smart city, smart home, and industrial IoT.

ACCESS UNDER CONTROL

Suppose that every person working in your office block has keys and access to all areas within – from directors' offices, through archives, to conference and server rooms. Terrifying? This, in fact, is how a company's IT network looks without adequate privileged access solutions – that is, Privileged Access Management (PAM). Fudo Security is a Polish company successfully providing their Fudo PAM solution to Europe, Asia and North America's largest markets.

Fudo PAM makes it possible to assign appropriate rights to individual users and administrators of a network – but this is just the beginning. 55% of security breaches stem from abuse on the part of privileged accounts. Therefore, users and administrators' sessions in the system are monitored and recorded, and automatically terminated in the event of a threat (upon detecting the execution of a predefined code for instance). Fudo PAM also has an option to generate system passwords and store them securely; customisable in terms of complexity, these can be adapted to internal regulations. An additional security layer has been provided for highly sensitive resources. The so-called "four-eyes principle" (4EP) is a mechanism which requires independent authorisation of each attempt to access a specific resource – and this is just one example of how users can define their own access rules; other involve forbidding connections from certain devices, in certain hours or from specific locations.



In practice, Fudo PAM is a customised sieve installed between servers and users in a company. It enables control of access, and consequently of data flows. Each of the three versions of Fudo may take the form of either hardware set up physically in the company or a virtual device. Among entities using Fudo PAM are Poland's and EU's banking and financial institutions, but also US-based Yahoo, a German airport, or a hospital in Qatar. In line with one of their guiding principles – "Not just for the big guys" – Fudo Security keep stressing that every single company should be able to protect itself from attacks coming from privileged areas. That is why due to be released soon is a new version of the solution, intended for smaller enterprises.

SECURE CLOUD

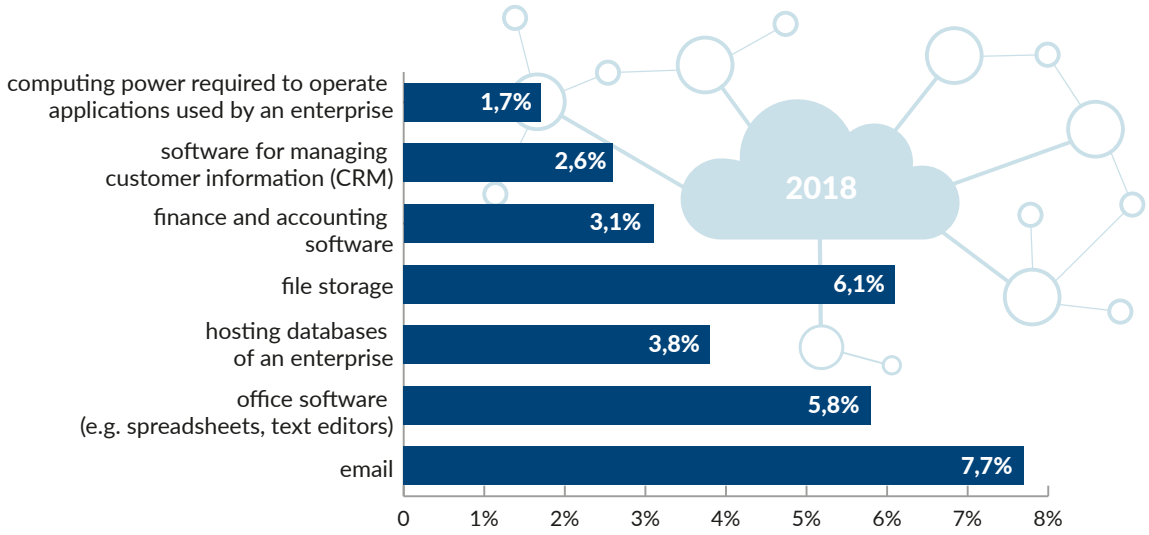
91% of companies using cloud are concerned about security of such services. This global data is confirmed in Poland too, where the greatest difficulties perceived in this respect are, on the one hand, limited awareness of what security features a supplier's infrastructure has, and on the other, establishing consistent security policies. The answer to these market concerns is the offering of Integrity Partners – experts who specialise in cloud and cybersecurity.

Today, the cloud means much more than just file storage – for many firms it is above all about several business services, from email, through database hosting and office software, all the way to computing power available on demand. Protecting so many processes in an environment so heterogeneous and complex can be a major challenge to even the most advanced IT units. Integrity Partners are building their cloud protection strategies on the following cornerstones:

1. Endpoint security
2. Information protection
3. Protection of cloud-based services
4. Cloud infrastructure security

That first area is mostly security of computers, laptops or mobile devices which enable the use of cloud-based services. Encryption that protects from unauthorised access, credential protection, preventing the execution of malicious code, and secure browser access are just a few services and products situated in the first line of defence against the possible threats.

Chart 1. Enterprises using paid cloud services in Poland, by type of services (% of all enterprises)

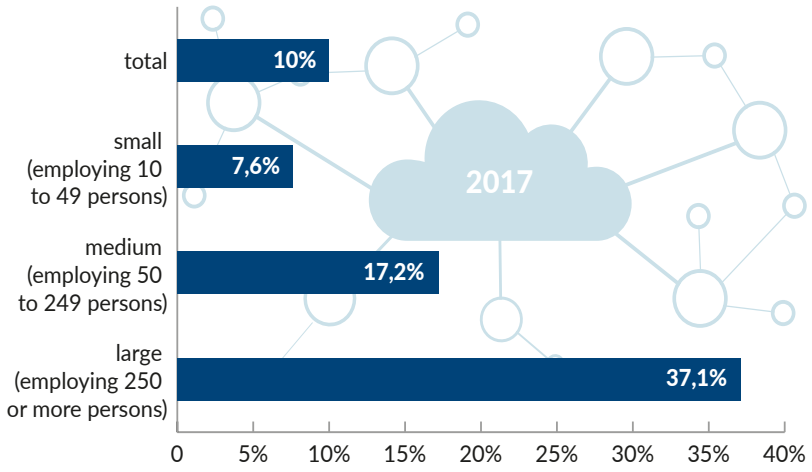


Source: GUS, *Information society in Poland 2018*

Should the attacker succeed in overcoming those, he or she is going to encounter another "wall" in the targeted laptop: mechanisms for the security of data stored therein. It is based on encryption, classification and restriction of access to individual files or databases.

Chart 2. Enterprises using cloud-based computing services in Poland, by size

In 2017, 10.0% of all enterprises – that is, 1.8 percentage points more than in the preceding year – have used cloud computing services. The index was highest among large enterprises – 37.1% of them declared having used at least one cloud-based processing service.



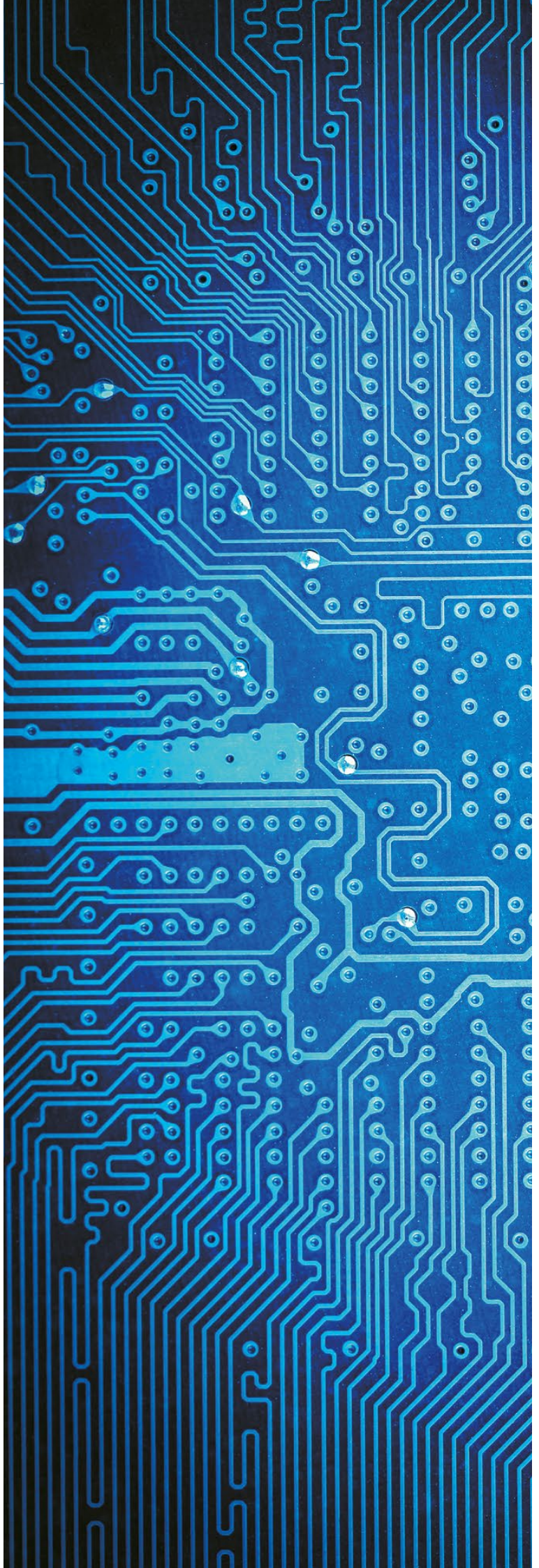
Source: GUS, *Information society in Poland 2017*

These may be supplemented with resource access monitoring and with automated reactions to suspicious behaviour.

The third area is protection of cloud-based services. So, what should be secured on that level? Well – the answer varies: products and services on offer are diverse, and Integrity Partners always customise the scope of service provided to the customer through a cloud. If you are, for instance, using Office 365 in your company, then this would cover email protection (advanced anti-spam and anti-malware systems in the form of sandboxes) as well as protection from information leaks, effected with rules that prevent transmission of certain data (e.g. credit card numbers or social security numbers).

The fourth area is security of the cloud infrastructure itself that you own physically or rent as a dedicated Azure or AWS service. That infrastructure is protected by, among other things, access control and encryption of data stored within, but also user behaviour analytics based on AI algorithms.

With such foundations, Integrity Partners help firms and institutions create work environments that ensure not just security, but productivity too, through the use of cloud-based solutions designed according to both private and public as well as hybrid models. In practice, this means more than 400,000 users working with the Microsoft Public Cloud services they provide, more than 200,000 mail accounts migrated to Exchange Online, and more than 30,000 privileged identities operated by the PASM systems they have implemented.

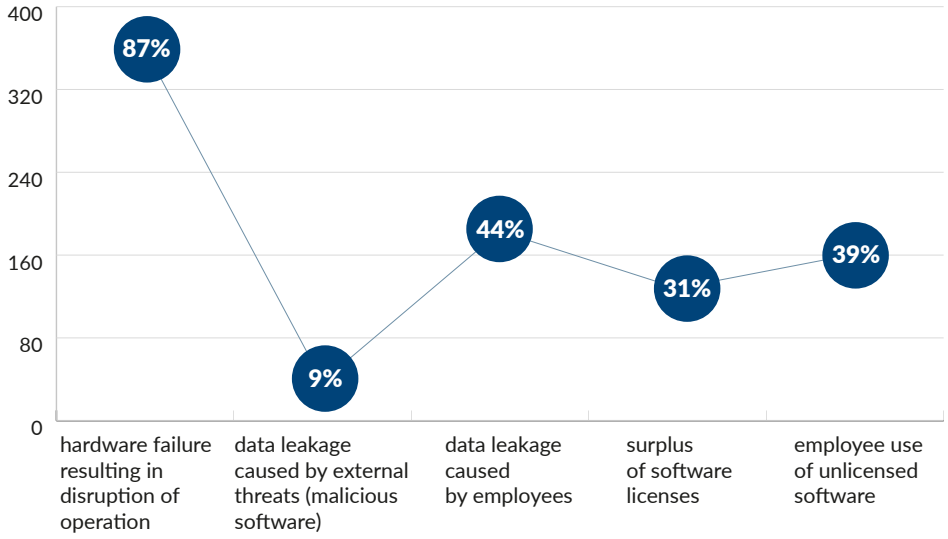


MANAGING CYBER RISK

85% of surveyed Polish IT administrators have witnessed a major hardware or software failure. Inadvertent errors on the part of employees, security gaps in IT systems or deliberate criminal doings may sooner or later expose any firm to leakage of sensitive data. Minimising losses and managing cyber risk make up an ongoing process which covers actions taken before, during and after the possible incident. In order to be able to apply this process effectively, IT administrators require appropriate tools – and that is why the Krakow-based company Axence introduced Axence nVision.

Digital security has to stem from holistic IT resource management policies and from improving user competence levels. The human factor is posing far greater challenges here than that of infrastructure. The most common cause of data leaking out of the workplace is employee use of non-authorised email service, or them plugging in unapproved storage devices. Whatever the employees' intentions, companies suffer real financial losses when sensitive commercial or industrial information leaks out.

Chart 3. Have your organisation ever experienced the following events?



Source: *Research conducted among polish IT Administrators*, Axence 2018

Therefore, data protection begins with implementing and exercising security rules among employees. Companies which are using the Axence nVision software for IT management purposes are able to minimise the risk by forbidding undesired behaviour such as website, application or device access. Managing rights and monitoring networks actively are just two of the many more aspects which improve security. Professional IT management helps avoid possible failures or react to unwanted incidents more promptly, thus preventing serious threats. In doing so, Axence nVision meets IT security officers and administrators' essential needs for the monitoring of networks and users, for the keeping of software and hardware inventories, for the provision of remote technical support, and for the protection of data from leaking out. At the same time it allows management boards to optimise operational costs of computer infrastructure, no matter its size.

Axence nVision is being used by more than 3,500 companies and institutions from all over the world. Counted among Axence's customers are international organisations such as Bombardier, ArcelorMittal or the American YMCA; also, large Polish companies like Wittchen and ZikoApteka; finally, public administrations and institutions, including courts of law, prosecutor's offices, municipalities and financial institutions.

DIGITAL PROTECTION FOR INDUSTRIAL FACILITIES

Stoppage of a nuclear program, or disabling an electric substation and leaving more than 200,000 consumers without power in the middle of winter – could that be caused by a computer virus? It could. Recent years have shown that cybersecurity is not just a challenge for ICT networks in office blocks, but also an issue for industrial control systems operating in facilities such as refineries, factories or power plants. STM Solutions specialise in combining those two areas – IT and OT. Their ADS (Attack Deception System) allows to protect the data stored on employees' computers as well as industrial automation processes run in the factory.

An ADS detects security anomalies in the infrastructure it is monitoring. Connectors to various sources of data allow the system to identify both IT and OT anomalies. The way it operates follows a proactive approach to digital security, derived from the well-known mechanism of setting up traps called "honeypots". The purpose of these is to lure the intruder into a specific location, one which is marked off, and so move the threat away from any elements critical to the organisation's operation. The honeypots used by an ADS are gathered in a native network called HoneyNet. They perform the task of implementing certain attack scenarios, meant to convince the attacker that the services they provide are authentic. Still, the HoneyNet itself is not the only element of an entire ADS – within the system there are also other security modules, whose function consists in obscuring the results of port scanning or in testing correctness of Wi-Fi configuration, among other things.

The dedicated element of an ADS which supports protection of industrial infrastructure is SFDS (SCADA Fault Detection System). It enables gathering information from OT systems, correlating the results with both IT and OT data, and warning about any irregularities. Furthermore, an ADS allows its user to deploy SCADA honeypots which imitate operations of industrial infrastructure.

One real-life example of using an ADS was having it deployed as a system for monitoring sensitive operations within an OT infrastructure related to liquid substances. The task of the system there was to monitor tankers being driven onto the customer's premises as well as further activity related to individual vehicles. Particular significance was attached to monitoring the process of filling the tankers – also in respect of possible disruptions (deliberate as well as unintentional). Deploying an ADS had allowed the near-real-time detection of anomalies connected to the industrial process, with automatic correlation of detected incidents with CCTV footage. For each incident detected, an alarm was being sent to the system operator's console right away, including a video surveillance recording as well as other information that expanded the context of the identified anomaly (e.g. about someone signing in to a customer's IT systems just before the disrupted filling).

FINDING YOUR BALANCE BETWEEN SECURITY AND USABILITY

predica.

In 2017, the average amount paid for each lost or stolen record containing sensitive or confidential information was USD 141. Most of those cases might have been mitigated only by proper identity managements in the IT systems – but this usually comes with usability costs. Predica, a company from Warsaw, helps customers to find balance between the security of their digital infrastructure and their business needs.

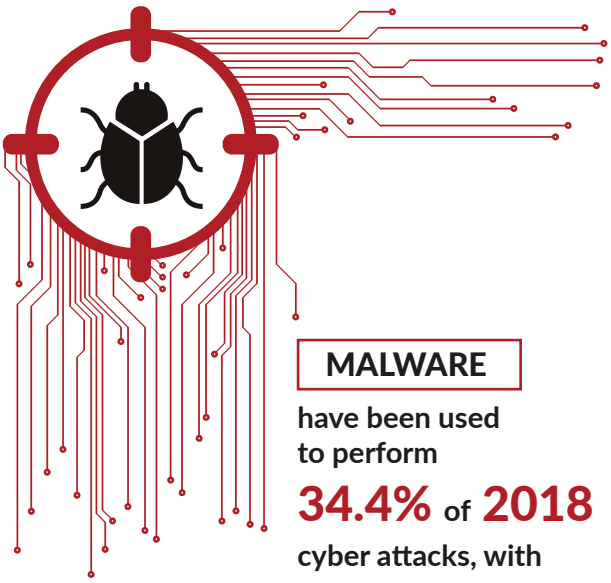
In critical infrastructure, the financial sector or governmental institutions, some systems have to be built with the highest IT security in mind. What does this look like in practice? The air gap, i.e. a lack of direct connections with external networks, including the Internet, is just the beginning. The architecture of the system might be based not on one, not even two, but on three administrative tiers with separate roles for each and totally detached competences. Tier 0 for domain administration, tier 1 for applications and servers, and tier 2 for a helpdesk. In that scenario, each layer should have dedicated workstations with multifactor authentication and latest security systems.

But not every company or institution needs digital Fort Knox. After implementing more than 900 projects in 22 countries, Predica is more than aware of this. Every business needs to find its balance within the triad of security – functionality – usability. Newest security products might help to shorten the distance between the three poles, but the final decision should always be taken with the focus on the operational needs. It may be that some companies do not need separate workstations for all three layers of administration; maybe they can only have two tiers? These kinds of decisions should always be backed by a comprehensive overview of the security landscape in the specific sector and geography.

Last but not least, the task of identity management might be accomplished in several innovative ways – even on a nation state level. Predica smart cards project for the Oman Information Technology Authority is one of such examples. The company built a complete IT infrastructure for registering cards in firms or public administration IT ecosystems to make them a universal secondary authorisation tool safeguarding access to data resources.

CYBERATTACKS – STATISTICS AT A GLANCE

As a result of cyberattacks, in 2017 the world economy lost over 600 billion dollars altogether (McAfee&CSIS). Zurich Insurance forecasts indicate that in 2030 such losses will grow to 1.2 trillion dollars, which equals 0.9% of world GDP. A cyberattack may paralyse the operation of whole economic sectors, which the NotPetya attack strikingly illustrated as it generated 10-billion-dollar losses in 2017 and for a few hours put out of operation such companies as Maersk, Merck, FedEx, Saint-Gobain, Mondelēz or Reckitt Benckiser.



MALWARE

have been used to perform

34.4% of 2018

cyber attacks, with

81.82%

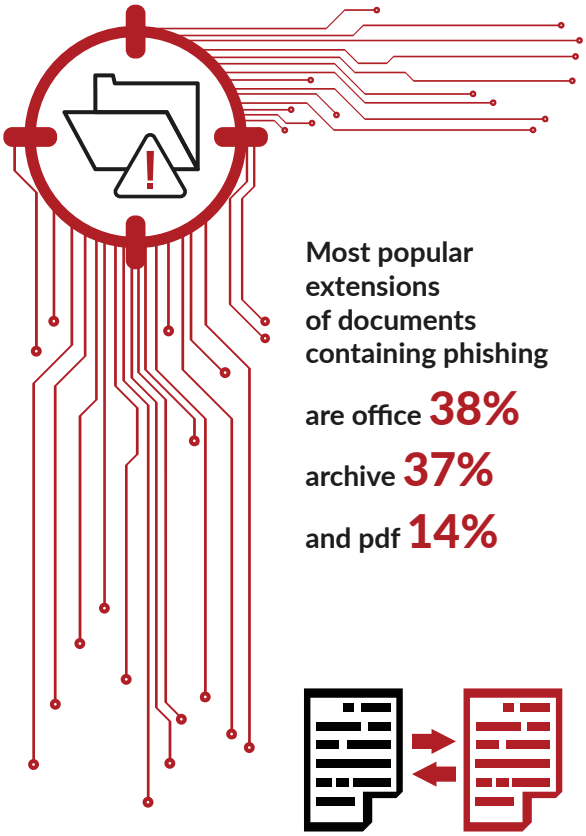
of them motivated by cyber crime

MALWARE

Malware have been used to perform **34.4%** of **2018** cyberattacks, with **81.82%** of them motivated by cybercrime [1]. The number of compromised records went up by **133%** in **2018**, which brought also shift of attack targets from individual consumers to organisations. Consumer malware detection decreased in last year by **25 million (3%)** [2]. The main carrier of malware is email (**92%**, **1** in every **13** mails contain a malware), followed by websites **(6.3%)**, with mainly JavaScript **(37.2%)** and Visual Basic Script **(20.8%)** as the file types used to hide malware [3]. Last year also brought a significant increase of new download variants, new malware on Macs, and mobile malware. Every day **230,000** new malware samples are produced, of which **51.5%** are Trojans [4]. The biggest new threat is connected with crypto mining, which was associated with **90%** of remote code execution attacks in early **2018**. Coin miner malware detections on endpoint computers in **2017** increased by **8,500%** [5]. A third of data breaches included use of malware, dangerous because of high costs and long time needed to identify it (average of **131** days) [6]. The average ransomware attack costs a company USD **5 million** [7].

PHISHING

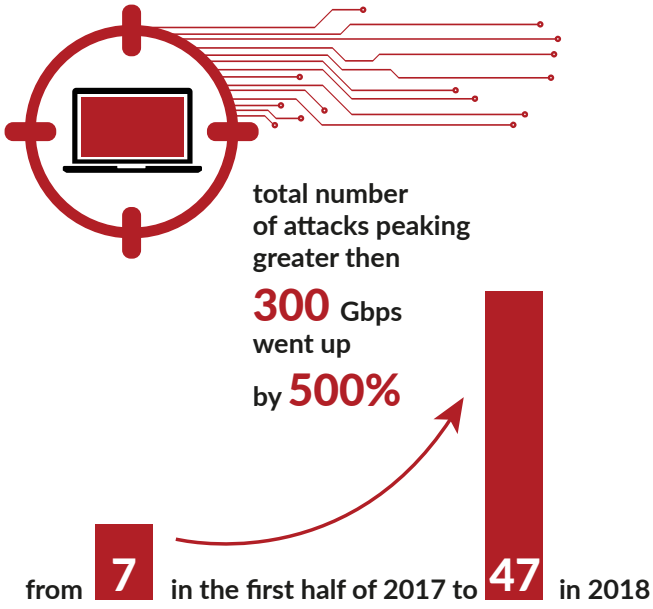
Phishing is one of the most common and popular ways to attack consumers and organisations; at the same time it is the most effective way to infect their computer systems. More than half **(56%)** of IT security decision-makers said that targeted phishing attacks are the top threat they face. Email is the most popular tool to send phishing to potential victims; more than half **(54%)** of all mail is spam. Most popular extensions of documents that contain phishing are office, archive, and pdf [8]. Authors of those emails are using a wide variety of motivators to convince future victim to open/use the sent file. The biggest average response is gained by using entertainment motivator **(19.5%)**, followed by social, reward/recognition, curiosity, job function, urgency, and fear. In the second quarter of 2018, phishing aimed at organisations most often targeted global Internet portals, financial & e-pay organisations and banks, IT-companies, online stores, government and tax organisations. Most affected were the following countries: Brazil **(15.51%)**, China **(14.77%)** and Georgia **(14.44%)** [9]. A dangerous form of phishing is Business Email Compromise **(BEC)** targeting



specific businesses that operate on the international market and regularly use electronic funds transfers. **BEC** scams affected **7,710** companies in 2017, with **4.9** attacks per organisation on average. Email users that were sent BEC phishing by industry: nonclassifiable establishments – **1 in 24**, mining – **1 in 30,** wholesale trade – **1 in 35** and public administration – **1 in 35** [10]. In the US, **15,690** BEC/EAC complaints were lodged with adjusted losses of more than **USD 675** million (2017) [11], and an average cost of **USD 130,000** per victim [12].

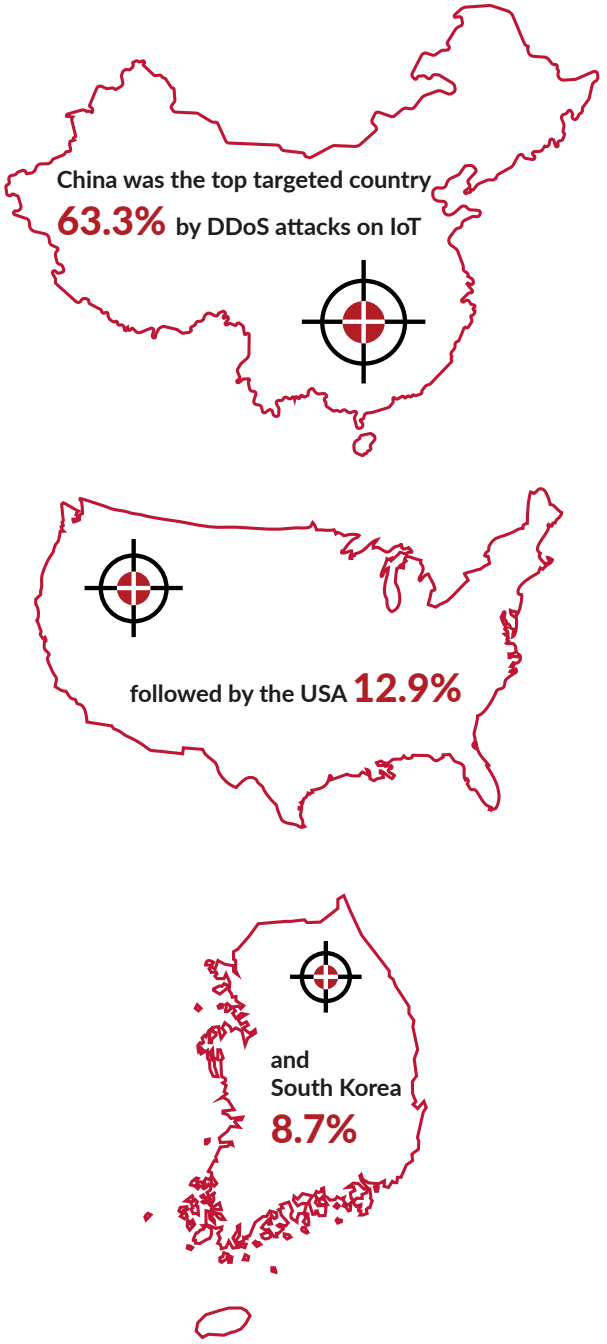
DDOS

Distributed denial-of-service **(DDoS)** attacks increased more than **2.5** times over the last **3** years [13]. The total number of DDoS attacks in **Q2 2018** has been **29.02%** bigger than in the same period of **2017**. At the same time, the size of attacks also significantly increased with the maximum of **1.35** Tbps [14] and the average of **26.37** Gbps **(+543.17)**; the total number of attacks peaking greater than **300** Gbps went up by **500%** from **7** in the first half of **2017** to **47** in **2018**. The average duration of attack was **318.1** minutes, the largest source of attacks was **USA (20%)**, and the most targeted sector in the first half of 2018 was that of telecommunications providers and cloud hosting [15] [16].DDoS attacks on IoT are becoming a growing threat with **38%** of IT companies that suffered from them in **2017**, and **35%** of them saying IoT devices were the primary source of a data breach. The average cost of downtime for **33%** of enterprises exceeds USD **1 million** an hour. China was the top targeted country by DDoS attacks on IoT, followed by the USA and South Korea.



APT

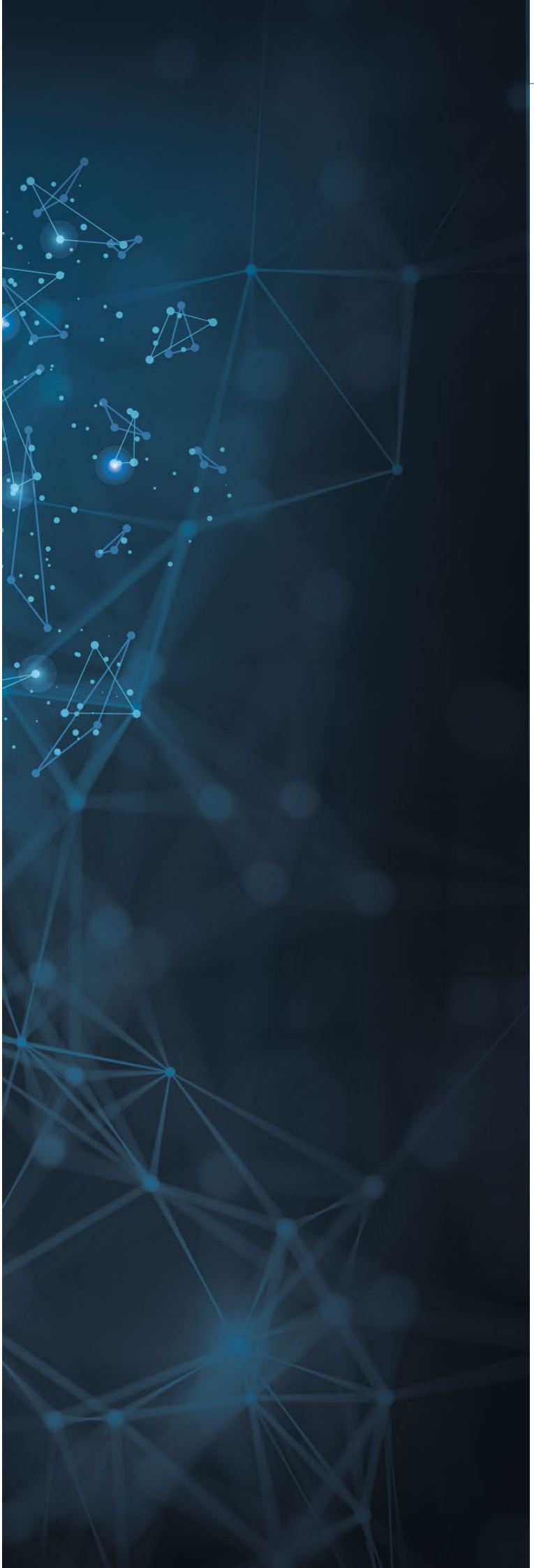
Advanced persistent threat **(APT)** is a well planned, often very sophisticated and targeted network attack on any organisation. APT attacks use a wide variety of techniques including: SQL injection, remote file inclusion (RFI), cross-site scripting (XSS), drive-by downloads, malware, phishing and spam. The most effective way of getting into a network system is through spear-phishing emails, which start **91%** of APT attacks [17]. APTs are long-term and large-scale attacks targeting most frequently governments, agencies and facilities, defence contractors, and biggest global companies [18].



According to the Symantec.cloud security, the most targeted industries in recent years are minerals and fuel (1 in 8), followed by transportation and utilities, telecommunications and engineering. According to Cyberthreat Defense Report, **21%** of IT professionals reported having been subject to an APT attack [19]. The lifecycle of APT is long compared to other cyberattacks, for example cyberspying operation called GhostNet, discovered in 2009, infiltrated network systems in **103 countries**, and the average time of host being actively infected was **145 days**, with the longest infection lasting **660 days** [20]. In the past few years **APT** attacks have been often used to carry out espionage campaigns, by collecting sensitive data from mobile devices or using one piece of malware infecting Windows, Linux and macOS [21]. Difficulty in discovering and stopping **APT** attacks is making them very expensive for a victim, for example in **2014** Home Depot and Target suffered breaches that cost them more than half a billion dollars [22].

REFERENCES

1. P. Passeri, 2018: *A Year of Cyber Attacks* [on-line]. Available at: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/.
2. Symantec, *Internet Security Threat Report* [on-line]. Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.
3. Verizon, *2018 Data Breach Investigations Report* [on-line]. Available at: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.
4. Pandalabs, *27% of all recorded malware appeared in 2015* [on-line]. Available at: https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/
5. Symantec, *Internet Security Threat Report* [on-line].
6. Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview* [on-line]. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=-SEL03130WWEN.
7. Barkly, *The True Cost of Ransomware* [on-line]. Available at: https://www.barkly.com/true-cost-of-ransomware.
8. Cisco, *Annual Cybersecurity Report* [on-line]. Available at: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2.
9. N. Demidova, T. Schcerbakova, M.Vergelis, *Spam and pishing in Q2 2018* [on-line]. Available at: https://securelist.com/spam-and-phishing-in-q2-2018/87368/.
10. Symantec, *Internet Security Threat Report* [on-line].
11. FBI, *2017 Internet Crime Report* [on-line]. Available at: https://pdf.ic3.gov/2017_IC3Report.pdf.
12. R. Mercado, *New online financial scam costs victims $130K per attack* [on-line]. Available at: https://www.cnbc.com/2018/02/02/new-online-financial-scam-costs-victims-130k-per-attack.html.
13. Cox Business, *12 DDoS Statistics That Should Concern Business Leaders* [on-line]. Available at: https://www.coxblue.com/12-ddos-statistics-that-should-concern-business-leaders/.
14. L. H. Newman, *Github Survived the Biggest DDoS attack ever recorded* [on-line]. Available at: https://www.wired.com/story/github-ddos-memcached/.
15. Calyptix Security, *DDoS Attacks 2018: New Records and Trends* [on-line]. Available at: https://www.calyptix.com/top-threats/ddos-attacks-2018-new-records-and-trends/.
16. Nexusguard, *DDoS Threat Report 2018 Q2* [on-line]. Available at: https://www.nexusguard.com/threat-report-q2-2018
17. NCX Group, *Phishing Is a Serious Threat To Your Business In 2018* [on-line]. Available at: https://www.ncxgroup.com/services/phishing/#.XFMqoFxKg2w.
18. Symantec, *Advanced Persistent Threats: A Symantec Perspective* [on-line]. Available at: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.
19. Cyberedge, *2015 Cyberthreat Defense Report* [on-line]. Available at: https://www.netiq.com/communities/cool-solutions/netiq-views/84-fascinating-it-security-statistics/.
20. Symantec, *Advanced Persistent Threats*: A Symantec Perspective [on-line].
21. Check Point Research, *Cyber Attack Trends*, 2018 Mid-Year Report [on-line]. Available at: https://research.checkpoint.com/wp-content/uploads/2018/07/Cyber-Attack-Trends-2018-Mid-Year-Report.pdf.
22. S. Watts, *What is an "Advanced Persistent Threat"? APTs Explained* [on-line]. Available at: https://www.bmc.com/blogs/advanced-persistent-threats/.



NEW FRONT LINES OF CYBERSECURITY

The unique nature of cyberspace creates unprecedented conditions for the functioning of societies, economies and the security system. The growing multidimensional role and importance of the private sector, especially business, but also the civil society, academia etc., is one of the many consequences of activities that take place in the digital space.

While it is clear that private companies, both as the suppliers of products and services and the end customers, largely determine the shape and development of the new technology market, their potential impact on the security of nations and societies has not yet been fully discovered or defined. The challenges facing the private sector reflect well the general trends in the field of cybersecurity.

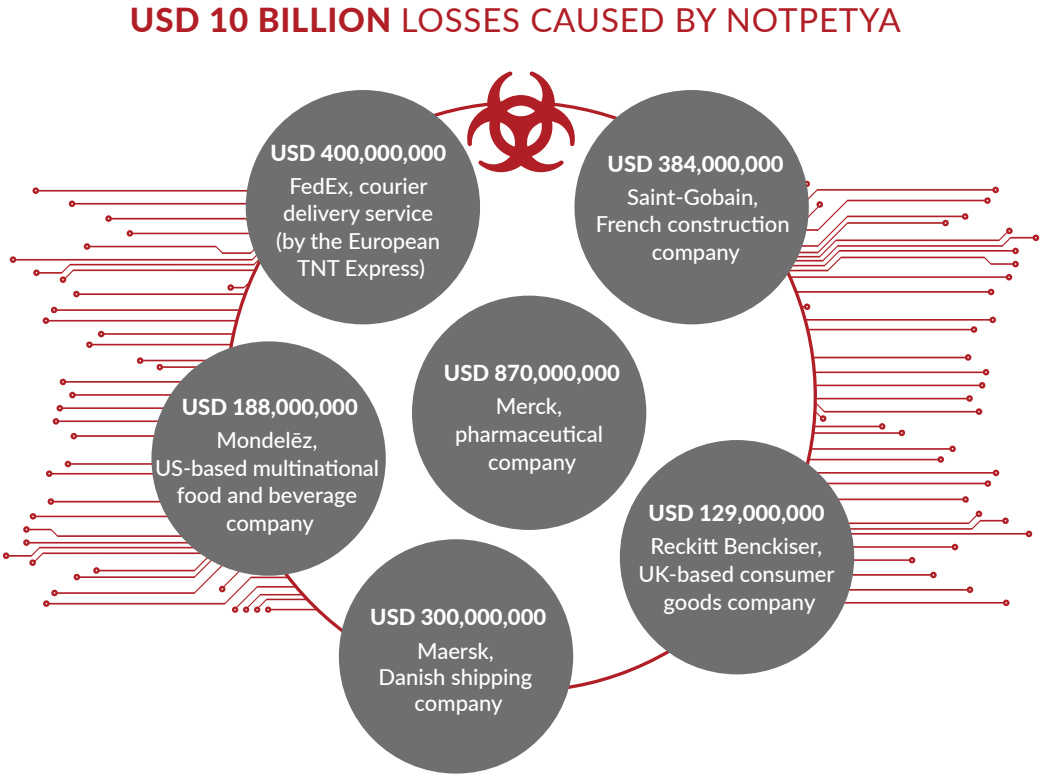
Cyberspace consists of technologies, solutions, platforms and systems that are provided mostly by commercial enterprises. Inevitably, therefore, it is them who often are at the front line of the battle against cyberthreats. Their new position also gives them a unique part to play. On the one hand, it increases their responsibility, and on the other hand, it positions them as a vital link in the security ecosystem. Every day, by using modern technology, billions of users entrust their safety to manufacturers and suppliers. Our everyday lives, business, operation of critical infrastructure such as banks, transportation, hospitals, etc. often hinge upon a smooth operation of the solutions provided. A key to success is, therefore, security by design that embeds strong cybersecurity foundations into products and services in the entire value chain, throughout their entire life cycle. Realising the magnitude of the problem, responsible private entities should make it a priority to take action in this area. The range, scale, sophistication and nature of threats are evolving dramatically. Building effective cybersecurity requires a constant analysis of the changing environment and adaptability.

WHERE DOES THE PROBLEM LIE?

Cyberthreats do not only stand for "standard" incidents that are associated with the daily use of the Internet. We live in a world where cyberspace has become a scene for many more serious conflicts involving nations and their resources. The consequences of these activities are grave; the losses may affect ordinary citizens or unrelated entities; they may even weaken entire economies.

Effective security measures often go beyond the capabilities of individual entities; therefore, decisions are needed at the strategic level, and these are also increasingly involving private stakeholders. The 2017 NotPetya cyberattack is a good illustration of this problem. Initially identified as a ransomware attack, NotPetya was, however, something far more serious.

Figure 1. Losses resulting from the NotPetya attack



Source: *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, https://www.wired.com/story/notpetya-cyberattack--ukraine-russia-code-crashed-the-world/.

It was even hailed "the most devastating cyberattack since the inception of the Internet".[1] The aim of the cyberattack was not just to extort money in exchange for decrypting infected computers. It meant to completely incapacitate them. NotPetya's prime target was Ukraine, but the cyberattack very quickly reaped a global harvest. It is widely believed that the cyberattack was politically motivated, and directly related to the conflict between that country and Russia. Regardless of the context, it was mainly private companies and ordinary users of cyberspace who fell victim to the cyberattack. The cyberattack used, among others, a tool known as EternalBlue. Developed by NSA, a US security agency, the exploit had been leaked in an incident earlier the same year. Using EternalBlue, the perpetrators were able to take advantage of Windows vulnerability, triggering a global cascade effect that caused many entities to suffer gigantic business and image losses. Some figures below perfectly illustrate the ramifications of the cyberattack.

1 A. Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History* [on-line]. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Regardless of the attack's geopolitical motivations, it was primarily private companies and their customers who found themselves in the eye of the storm. This showed very clearly that the new types of cyberspace-enabled conflicts go beyond the existing, classic framework, wherein the main actors used to be state-owned entities. In this context, it becomes evident that the private sector must play an ever-important part in building cybersecurity.

Another example, which clearly reflects the diverse nature of problems the entities responsible for cybersecurity have to tackle, are the events we witnessed in 2016 during the US presidential election campaign. At that time, cyberspace, Internet platforms and social media were harnessed to wage information warfare – a hostile interference in the sphere of information by conducting disinformation and manipulation campaigns as well as spreading hostile propaganda. During the US presidential campaign, Twitter, Facebook and other social media platforms became an arena of malicious activity that was meant to manipulate the decisions of users, and, consequently, the outcomes of the whole democratic process. When these revelations saw the light of day, the owners of these platforms came under widespread criticism. Many loudly demanded that they take more decisive preventive action. Again, similarly to NotPetya, commercial enterprises took centre stage in events directly related to security issues. In this case, however, the threat did not so much undermine ICT systems as the mechanisms to manage content posted on websites. It is a completely different challenge. Although the events of 2016 were the pinnacle of cyber manipulation, the question of liability of platform owners for content hosted on them had been raised before. Many groups indicated that Internet platforms were not doing enough to counteract the activities of terrorist groups that use the Internet to spread propaganda, radicalisation, etc.

INCREASING THE CYBERSECURITY LEVEL

Piling up challenges and threats, illustrated here by only two examples, are eliciting an increasingly active response from technology companies that have started to make self-regulation efforts in order to strengthen cybersecurity. Although the trend is visible, the question that arises is this: how effective are they?

An example of projects aimed at curbing the online activity of terrorist groups and their supporters is the Global Internet Forum to Counter Terrorism (GIFCT). The main aim of the project is to prevent the spread of propaganda produced by terrorists via the Internet. The GIFCT takes action at three levels:

1. The leverage of new technologies to counteract online terrorist activity;
2. The exchange of best practices and knowledge;
3. Conducting research and development activity.

One of the tangible outcomes that have been achieved by the members of the initiative was creating a shared industry database of hashes – unique "digital fingerprints" for pictures and videos related to pro-terrorist propaganda. Once identified, they are removed from the platform. At the moment, the database contains about 50,000 hashes.[2]

2 Global Internet Forum to Counter Terrorism [on-line]. Available at: https://gifct.org/about/.

Table 1. The results of activities undertaken by selected entities using machine learning algorithms

YOUTUBE	98% of videos placed on YouTube and removed due to extremist content are flagged by machine learning algorithms.
TWITTER	From July 2017 to December 2017, a total of 274,460 Twitter accounts were permanently suspended for violations related to promotion of terrorism. 74% of these accounts were suspended before their first tweet.
FACEBOOK	99% of the content associated with ISIS and Al-Qaeda that is removed from Facebook is the content which is detected before anyone has flagged it in their community, and, in some cases, before it even goes live on the site. Once Facebook has identified terrorist content, it removes 83% of subsequently uploaded copies within an hour of their upload.

Source: https://gifct.org/about/

The initiative was launched and is run by key technology companies.[3] As its members emphasise, the key is to work closely with civil society, the academic community and governments. The GIFTC has established a close partnership with Tech Against Terrorism, a project initiated by the United Nations Counter-Terrorism Committee Executive Directorate. A core part of work at Tech Against Terrorism is supporting smaller platforms in their efforts to strengthen their security. They do not always have the resources and knowledge to take effective preventive action. This weakness is increasingly exploited by perpetrators who use such platforms to carry on their sinister activity.

It is worth noting that due to the extremely sensitive matter of managing the content hosted on online platforms, the key is to carry out all the activities with respect for human and civil rights, including the right to freedom of expression. Successful fine-tuning of efforts in order to strike the right balance between the functionality and security of platforms on the one hand and privacy on the other is absolutely critical. In this regard, close cooperation between business and the representatives of civil society is of invaluable benefit.

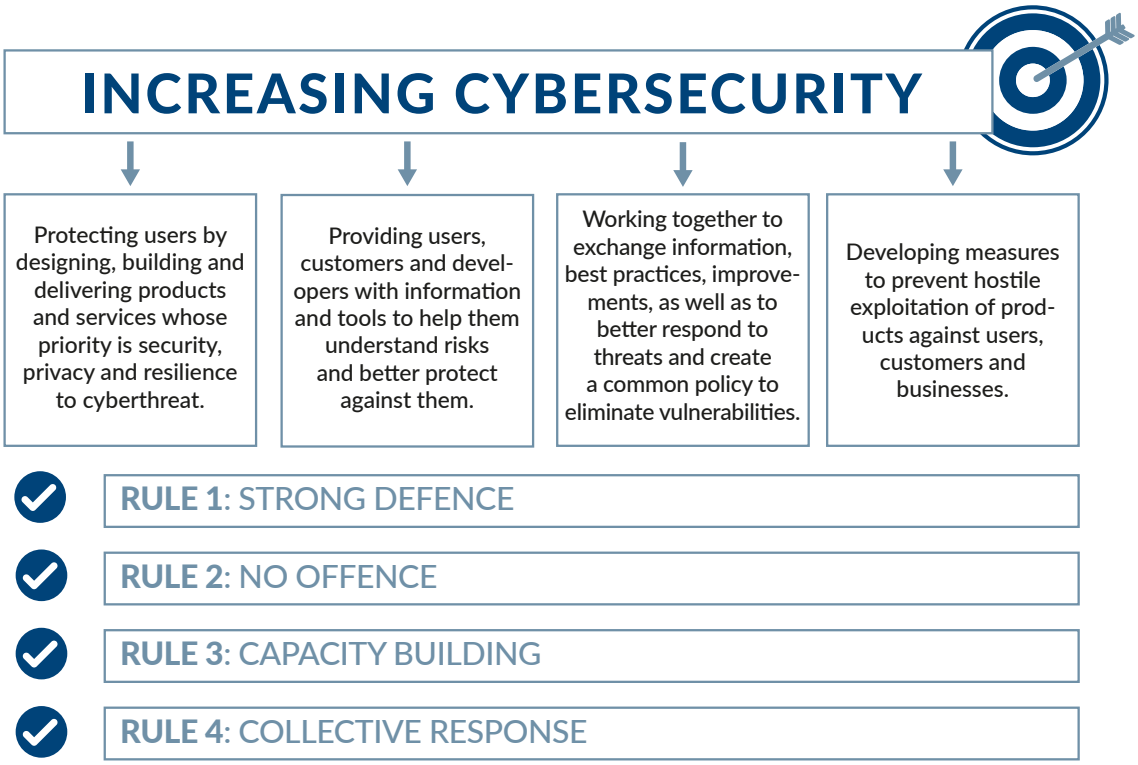
Having learned lessons from cyberattacks such as NotPetya, private companies have recognised the need to take action at a strategic level. Recently, we have seen initiatives starting to emerge which aim not to improve the security of products or services companies provide, but also to influence the surrounding environment in order to make it more secure. In this context, there are plenty of very bold proposals that have the ambition of creating systemic solutions in the domain of international relations.

One of the recent headline-hitting schemes is the Cybersecurity Tech Accord (Accord Tech) initiative, a public commitment that has been signed by over 60 companies so far. The signatories of the initiative declare their commitment to increase security and stability in cyberspace.[4] The foundation and the main instruments to help achieve this goal are close collaboration, responsible behaviour, joint use of resources and dialogue. The key components of Tech Accord are presented in the following diagram.

3 Facebook, Microsoft, Twitter, and YouTube are the founding companies.

4 The Cybersecurity Tech Accord [on-line]. Available at: https://cybertechaccord.org/about/.

Figure 2. Actions taken under the Tech Accord initiative



Source: Compiled on the basis of: https://cybertechaccord.org/about/

Rule number two (no offence) also entails that the signatories declare no support for public entities launching cyberattacks against innocent citizens or private entities. The aim is to reduce the arsenal of measures that could contribute to an even greater escalation of conflicts and adversely affect the stability of cyberspace.

Another initiative with similar objectives is the Charter of Trust. It seeks to proactively build a greater level of cybersecurity and increase trust in new technologies. The signatories of this project have committed to act according to 10 main principles that cover a wide spectrum of activities: anchoring the responsibility for cybersecurity at the highest business and governmental levels; ensuring security in the entire value chain, for example, through the use of encryption; adopting security measures in accordance with the principle of "security by default"; supporting certification, particularly for critical infrastructure and IoT critical systems; fostering cooperation in regulation and standardisation at a global level.[5]

All signatories of Tech Accord and the Charter of Trust also endorsed the French initiative known as the Paris Call. **On 12 November 2018, President Emmanuel Macron announced a declaration that lays down a set of rules to increase the security of cyberspace. The fundamental provisions of the document reaffirm the belief that international law also applies to online behaviour; they also support the creation and application of norms of responsible behaviour in cyberspace and the implementation of confidence-building measures. The Paris Call acknowledges the role of private entities in combating network security threats, stressing the need for their engagement and collaboration with governments.** The declaration draws attention to several high-priority areas that must be addressed in the first place. For example, the document calls for the non-state

5 Charter of Trust, *For a secure digital world* [on-line]. Available at: https://www.siemens.com/press/pool/de/feature/2018/corporate/2018-02-cybersecurity/charter-of-trust-e.pdf.

actors to refrain from taking offensive action on the Internet, including "hacking back".[6]

More than 50 countries and hundreds of entities, including leading technology giants, have joined the initiative launched by President Macron. Without a doubt, the Paris Call is an important action, but there are many questions about its effectiveness. The fact that many key players sat out the agreement is one of them. Besides the obvious abstainers such as Russia and China, the US did not sign the declaration either. In addition, there is a question mark over the practical implementation of the assumed objectives. An example that provides an argument for a cautious assessment of the initiative's success is the fact that even Australia, a signatory to the Paris Call, has recently adopted the Assistance and Access Bill, which forces software suppliers to build in backdoors to get around encryption. Certainly, it is not a decision that strengthens product security.

PUTTING A BRAKE ON OFFENCE

The challenge of restricting offensive operations in cyberspace evolves toward a foreground issue that is increasingly engaging a wider number of actors, including civil society organisations. Individual cyberspace users are being encouraged to establish a more prominent presence as well. The Digital Peace Now campaign is an example of such activity. It encourages various entities, primarily ordinary civilians, to actively build peace in cyberspace. The aim is to stimulate grass-roots social movements to exert pressure on the actors whose actions put the stability of the Internet in jeopardy. Under the banner of "no peace without digital peace", the Digital Peace Now initiative demands de-weaponisation of the shared online community. As part of the campaign, you can sign a petition that urges state actors not to use cyberspace for aggressive action. As of December 2018, the petition was signed by about 100,000 people from 140 countries.[7]

Both Paris Call and the Tech Accord initiative indicate the need to develop the so-called norms of responsible behaviour in cyberspace. They aim to establish the "rules of the game", the observance of which is essential for ensuring safe functioning in cyberspace. The norms are not a binding regulation enshrined in law. They are more of an agreement that there are certain activities that should be or, on the contrary, must not be undertaken. Certain norms are being proposed not only by the representatives of countries (e.g. as part of the UN Group of Governmental Experts), but, increasingly, also by non-state actors, such as experts or the representatives of civil society. One of the most important groups currently working on proposals for the norms is the recently formed Global Commission on the Stability of Cyberspace (GCSC). The GCSC members have developed many norms, among which is one that says to refrain from using digital tools by state actors to interfere in the electoral infrastructure of another country.[8] This particular proposal reflects well the general trends in international discussions about cybersecurity which are increasingly focused on the prevention of digital threats jeopardising democratic processes. Some recommendations in this regard were also in the package proposed in the Paris Call. The document explicitly mentions the need to "strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities".[9] Safeguarding elections is also an area in which technology companies are engaging more and more. For example, Microsoft has proposed the Defending

6 Ministère de l'Europe et des Affaires étrangères, *Paris Call for Trust and Security in Cyberspace* [on-line]. Available at: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

7 Microsoft, *Digital Peace Now* [on-line]. Available at: https://digitalpeace.microsoft.com.

8 Global Commission on the Stability of Cyberspace, *Call to protect the electoral infrastructure* [on-line]. Available at: https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

9 Ministère de l'Europe et des Affaires étrangères, *Paris Call for Trust and Security in Cyberspace* [on-line].

Democracy Program, which seeks to pursue four main objectives:

1. Protect election campaigns against hacking by increasing resilience, monitoring and an incident response system.
2. Increase the transparency of online political advertising through supporting relevant legislation.
3. Explore technological solutions to minimise risks.
4. Counter disinformation campaigns.

They are meant to be achieved by carrying out a number of activities that involve providing appropriate tools, workshops and training.

It is absolutely critical to take action to improve the cybersecurity of democratic processes. This is reflected not only in the above-mentioned commercial projects, but also in regulatory initiatives. One of the recent, most widely debated proposals is the Honest Ads Act, a US bill that would regulate the transparency of political campaign advertisements promoted online.[10] In the context of securing the electoral infrastructure itself, it is worth noting that an increasing number of countries are simply deciding to take a step back and limit the use of digital solutions. Ireland, Germany and the Netherlands are examples of countries that have decided to take precautionary measures in this regard.

LOOKING AHEAD TO THE FUTURE

There are plenty of lessons the above problems can teach us. Modern technologies drive social development and civilizational advancement. However, if we want to make them a permanent part of the social and economic DNA, security must become the backbone of their creation. Otherwise, the risk may be too high. The security and solution building paradigm in this area has changed dramatically. With the advent of cyberspace, governments and state-owned entities are no longer the only ones with reality creation capabilities. Today, the private sector – most notably technology companies – are the forerunners in fighting cyberthreats and preventive action. And although it is still the states who are the main actors, they must work with a broadly defined private sector as partners. This requires that the current modus operandi is adapted to the new rules of the game. Each party must do their part. On the one hand, state actors must understand that commercial enterprises have to receive broad support for their efforts, which at the end of the day are critical from the point of view of entire societies. On the other hand, however, private entities must settle into this new role. There is no doubt that running business in the ICT sector brings huge benefits and opportunities. But they go hand in hand with equally large responsibility. Just like the states must understand that in addition to laying down requirements they should also strive to be a helpful partner, so companies need to play by the rules imposed on them. And there are going to be more of them in the near future. Both sides must also work effectively together with other participants of the system, especially with the representatives of civil society. The digital world is changing every aspect of our lives. Modification of our lives, and evolving roles or tasks are no exception. One thing is certain – each party will benefit from the ability to successfully adapt to the new situation.

10 Ibid.

THE RISE OF AI IS THE RISE OF CYBERTHREATS

Today, it is largely emerging technologies that set the pace for the cybersecurity dynamics. One of the many disruptive technologies is Artificial Intelligence (AI). And AI has just triggered runaway technological growth and might be considered a game changer in economy, politics and defence. Cyber-world will not be a safer place once we deploy full-bodied AI. In the hands of cybercriminals and hostile state countries, it will make cybersecurity landscape even more complex – with AI-enhanced cyberattacks more frequent, automated and devious as their detection and attribution becomes even more complicated and uncertain. So when we think of how AI will transform our economies, societies and international politics, we need to consider both the bright and the dark side of the process. Especially that weaponisation and dual-use of AI have already been recognised as a threat at the point in history when we are witnessing the accelerating strategic competition between the US and the People's Republic of China. During World Economic Forum 2019 in Davos, the Chinese efforts to win the AI race were compared to the Manhattan Project, clearly illustrating both the scale and the possible application.[11]

CYBERTHREATS EMBEDDED IN THE AI'S DNA

In a nutshell, AI consists of an exorbitant amount of data, algorithms and high-performance computing. The latter is hackable and we know it; however, data manipulation and rigged algorithms are posing new types of challenges, especially in the face of the advancing global scale deployment of AI. Gartner predicted that by 2020, a black market for selling fake and corrupted sensor

11 H. Long, *In Davos, U.S. executives warn that China is winning the AI race* [on-line]. Available at: https://www.washingtonpost.com/business/2019/01/23/davos-us-executives-warn-that-china-is-winning-ai-race/?noredirect=on&utm_term=.87ad81752133.

and video data will exceed USD 5 billion.[12] It will give rise to criminal activity involving Fake Data Injection (FDI) attacks. As a result, feeding AI systems with mass volumes of manipulated data may cause disruption of autonomous cars, smart buildings and smart cities, automated factories, oil and gas industry infrastructure, agriculture and healthcare devices, or even GPS! This will not only adversely affect business but, in the worst case scenario, cause physical harm. Furthermore, politicians and insurers will increasingly rely on AI software to help them make decisions or assess risks. Conversely, successful cyberattacks on AI-based systems may exploit algorithms that make those predictions or decisions as well as the trained models used by the systems.[13] This in itself can lead to devastating results, making AI a single point of failure.

For all those reasons, AI as well as all cutting-edge technologies should be designed and deployed with security requirements and strategic concerns in mind.

CYBERTHREATS OF THE FUTURE START NOW

It is important for cybersecurity experts and decision-makers to understand what the future cybersecurity landscape will look like and how AI will enable hackers to increase their effectiveness. With the era of AI unfolding before our eyes and setting the cyber scene for years to come, **we can expect an unprecedented intensification of cyberattacks, both in quality and quantity, as well as their automation**. **AI-driven attacks will change the economics of cyberattacks**[14] and **the hacker's cost-benefit analysis** to the extent that they will be able to attack targets that were otherwise not worthwhile to reach.[15] AI systems with its "efficiency, scalability and ease of diffusion" will also **increase the number of actors who can carry out cyberattacks** against civilian, business and military targets.[16] Thanks to AI, we can already observe how **humans and machines are easily teaming up,** but there is a risk that in the future **AI might even overtake human hackers** in carrying out cyberattacks.

Deployment of AI will increase sophistication of some cyberattacks of today in a form of:

- **"AI-boosted phishing attacks"**[17]
  AI will be used not only to automate phishing attacks but also to personalise them to such an extent that the recipient will not be able to distinguish between real and artificial (sic) correspondence. "AI will be harnessed to produce communications that will be indiscernible from human or machine written"[18] and which will reference actual interactions with someone we know.[19] It will make a "good use" of our digital footprint that is dramatically expanding because of the data-collection from devices connected to the Internet of Things and

12 Gartner, *More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things* [on-line]. Available at: https://www.gartner.com/en/newsroom/press-releases/2016-01-14-gartner-says-by-2020-more-than-half-of-major-new-business-processes-and-systems-will-incorporate-some-element-of-the-internet-of-things.

13 *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* [on-line]. Available at: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

14 Advisor Magazine, *The Economics of Cyberattacks* [on-line]. Available at: https://www.lifehealth.com/the-economics-of-cyberattacks/.

15 *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* [on-line].

16 AI Supremacy, *Artificial Intelligence and Risk Management* [on-line]. Available at: https://ai-supremacy.com/news/2018/9/20/artificial-intelligence-and-risk-management.

17 S. Finnie, *Cyber threats fuelled by AI: Security's next big challenge* [on-line]. Available at: https://www.csoonline.com/article/3315740/security-awareness/cyber-threats-fueled-by-ai-securitys-next-big-challenge.html.

18 E. Benishti, *Artificial Intelligence is Revolutionizing Phishing – and It's Not All Good* [on-line]. Available at: https://ironscales.com/blog/Artificial-Intelligence-Revolutionizing-Phishing/.

19 S. Finnie, *Cyber threats fuelled by AI: Security's next big challenge* [on-line].

from different apps we use on a daily basis:[20] "the 'check in' from our local coffee shop, Instagram updates, tweets and retweets, and even our use of GPS powered apps".[21] As it was recently concluded by EU Commissioner Julian King, "AI opens up opportunity to use or abuse huge volumes of personal data."[22]

- **Smart and devious malware**
  AI will be used to enhance malware and make it learn about the digital environment it is running in so that it can mimic typical behaviour found in a given system. This way, AI-enriched malware will bypass security gateway solutions and evade detection in order to exfiltrate data.[23] By the same token, AI might be used to carry out more powerful forms of DDoS attacks – AI-based DDoS attacks.
- **Automated multi-vector cyberattacks**
  AI will replace humans in conducting cyberattacks, with automated AI hacking machines operating round the clock as a result. AI will be gathering information to unleash combined and full-spectrum cyberattacks, including software bugs and social media channels to exploit vulnerabilities. These cybercriminal fully automated AI systems will make "millions of intuitive decisions per second about the best way to breach all kinds of systems, whether cloud, IoT or industrial IoT/SCADA".[24]

AI will transform the threat landscape as we know it by helping to advance some of the existing cyberthreats. But we can also expect an emergence of new varieties of "attacks of tomorrow". That may include harnessing AI to turn some devices such as autonomous cars, drones, medical devices or even robots into potential weapons which could cause physical harm to humans.

AI CYBERSECURITY THREATS FOR DEMOCRACY AND PEACE

The use of AI for "dark" political purposes, surveillance, persuasion and deception may expand the threat surface associated with invasion of privacy and social manipulation[25] in order to undermine the principles of democracy, radicalise social behaviours, polarise societies, sow discord and division, provoke protests, impact public debate, affect voting results and destroy privacy and freedom. Those threats can have a profound negative effect on both domestic politics and international relations.

- **Deepfakes – a new dimension of disinformation wars and campaigns**
  Highly realistic fabricated or manipulated video or audio recordings will exacerbate the threats of the post-truth world in which societies will no longer be able to trust the information they receive, or worse – will start to trust fake information. Deepfakes can be deployed both by cybercriminals and hostile authoritarian regimes. They can also be used against individuals to blackmail, discredit, sabotage or intimidate them.
- **AI-enhanced social engineering**
  Individually targeted, automated and sophisticated propaganda (via social media platforms, emailing campaigns, etc.) can be disseminated, drawing on our digital footprint, i.e. data showing our activities, moods or even beliefs. It might be used against citizens both in authoritarian and democratic states.

20 Ibid.

21 E. Benishti, *Artificial Intelligence is Revolutionizing Phishing – and It's Not All Good* [on-line].

22 J. King, *The EU needs its own security strategy to confront the digital threat* [on-line]. Available at: https://www.ft.com/content/cd9f206e-2562-11e9-b20d-5376ca5216eb.

23 S. Finnie, *Cyber threats fuelled by AI: Security's next big challenge* [on-line].

24 Ibid.

25 *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* [on-line].

- **Misuse of AI-enhanced surveillance**
  The analysis of mass-collected data by AI-based systems can be performed not only by intelligence agencies but also hackers, thus potentially diminishing liberal freedoms and privacy around the world.

"Cyberattacks of tomorrow", both against machines and against our minds, should be addressed strategically by governments, for instance in national strategies and R&D programmes for cybersecurity and artificial intelligence, as well as by business, which already started to embed AI solutions into security systems.

AI WEAPONISATION AS A CYBERSECURITY THREAT TO THE GEOPOLITICAL ORDER

In 2017 Vladimir Putin said loud and clear that "whoever reaches a breakthrough in developing artificial intelligence will come to dominate the world" and that "it would be strongly undesirable if someone wins a monopolist position".[26] Also in 2017, China's government was vocal about its goal of becoming a global leader in artificial intelligence by 2030.[27] And here we are, in 2019, facing the fact that it is China who is closer to making that breakthrough in AI application for the business sector.[28] The country is also leading in AI investments from both public and private funds.[29] PwC report from 2017 also stated that the greatest economic gains from AI are expected in China (boost of up to 26% GDP in 2030) whereas North America may be lagging behind (potential 14% boost).[30]

But AI is a purely dual-use technology and it is said to significantly change the warfare battlefield. We can expect the use of AI weapons in cyberspace, geospace and space (CGS). When we combine it with what was said by Hank Thomas, namely that the biggest cybersecurity threat in the world is the People's Liberation Army – China's armed forces[31] – the conclusion should be that the AI-augmented cyberthreats are just taking off. Autonomous weapons systems and military robots will most likely become a critical arsenal in the new phase of the strategic competition between global powers. That is why the US Department of Defense has established a new Joint Artificial Intelligence Center that will spend USD 1.75 billion over six years to give US forces "an asymmetric advantage across the full spectrum of conflict",[32] but experts say it is only a fraction of the size that China's investments actually are.[33] This approach should be adopted by all NATO members who are lagging behind in terms of strategic consideration and investments in AI capability development, which poses a risk of technological dependency. Also the EU, which is even more technologically dependent than the US, needs to think strategically, especially about security, and collectively invest in AI.[34]

26 CNBC, *Putin: Leader in artificial intelligence will rule world* [on-line]. Available at: https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html.

27 CBS NEWS, *China announces goal of leadership in artificial intelligence by 2030* [on-line]. Available at: https://www.cbsnews.com/news/china-announces-goal-of-leadership-in-artificial-intelligence-by-2030/.

28 9% of AI initiatives are present on a wide scale in Asia-Pacific organisation and 4% of AI initiatives are fundamental to Asia-Pacific organisation's operations; in North America only 3% and 2% respectively, more: https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf.

29 In 2017, Chinese firms raised USD 5 billion in venture capital funding, more than US firms, more in *The wrong trade war*, "Newsweek International Edition", vol. 172,no. 03, p. 42.

30 PwC, *Sizing the prize. What's the real value of AI for your business and how can you capitalise?* [on-line]. Available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

31 G. Chavez-Dreyfuss, *Venture capital funding of cybersecurity firms hit record high in 2018: report* [on-line]. Available at: https://www.reuters.com/article/us-usa-cyber-investment/venture-capital-funding-of-cybersecurity-firms-hit-record-high-in-2018-report-idUSKCN1PB163.

32 B. Mitchell, *Artificial intelligence is the heart of CIO Dana Deasy's plan to modernize the DOD* [on-line]. Available at: https://www.fedscoop.com/artificial-intelligence-dod-strategy-cio-dana-deasy/.

33 The Straits Time, *In Davos, US executives warn that China is winning the AI race* [on-line]. Available at: https://www.straitstimes.com/world/europe/in-davos-us-executives-warn-that-china-is-winning-the-ai-race.

34 J. King, *The EU needs its own security strategy to confront the digital threat* [on-line].

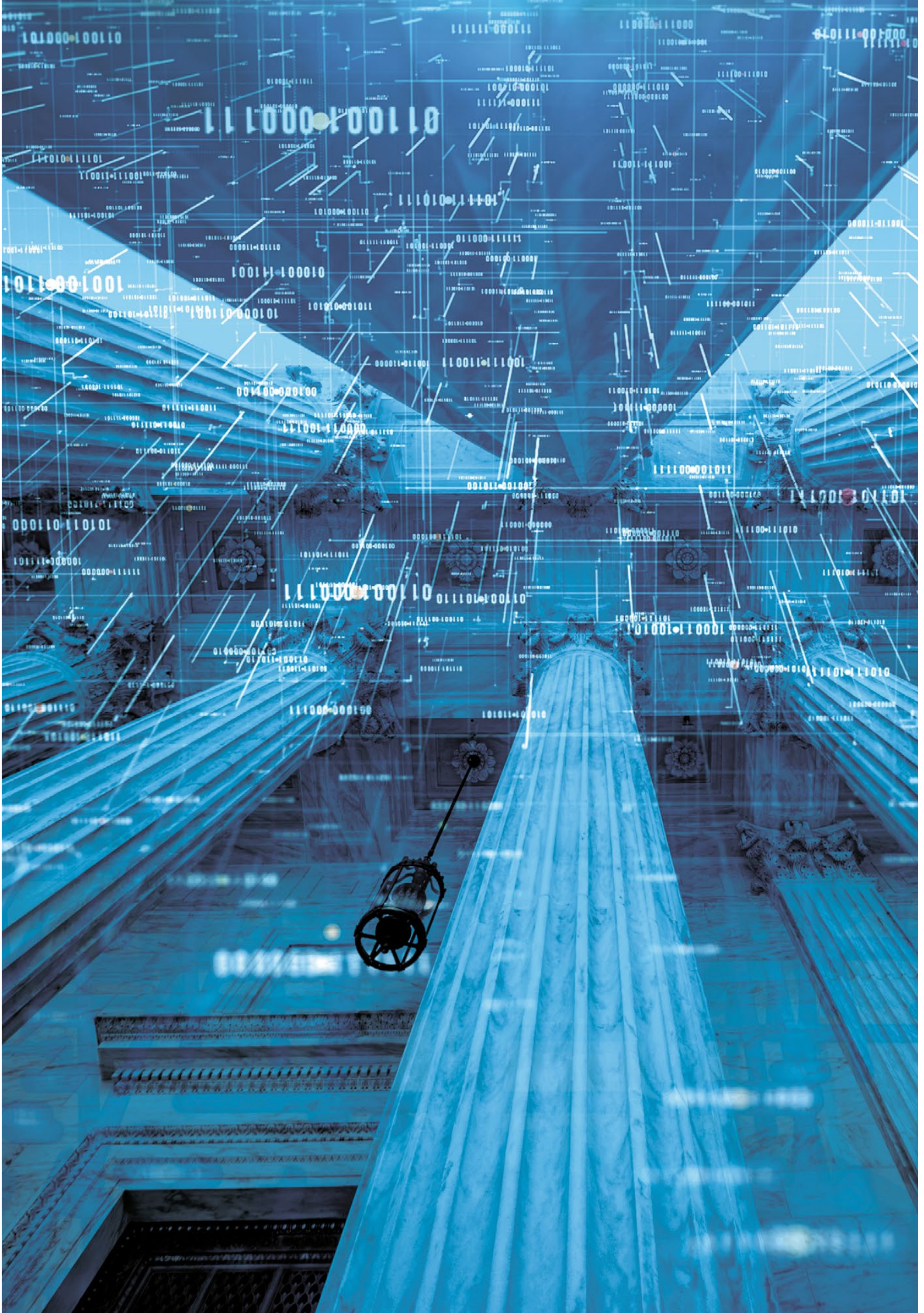
AI AS THE NO 1 CYBERTHREAT FOR THE HUMAN CIVILISATION?

Listing the AI-augmented cybersecurity risks should end with the ultimate threat – technological singularity that will allow AI systems to exceed human capabilities. It is in fact a cyber-world-derived threat for the human race that needs to be considered while we are speeding up AI deployment. The concept of technological singularity was presented to the world for the first time in 1958 by Stanislaw Ulam, a Polish mathematician, in his account of a discussion with John von Neumann. Ulam reported that "accelerating progress of technology and changes in the mode of human life [...] gives the appearance of approaching some essential singularity in the history of the race beyond which human affairs, as we know them, could not continue".[35] We were vocally reminded of this in 2014 by Stephen Hawking when he said that "the development of full artificial intelligence could spell the end of the human race".[36] One of the world's leading AI experts, Nick Bostrom, in his 2014 book *Superintelligence: Paths, Dangers, Strategies*, also expressed his concerns regarding the development of systems that will exceed and surpass humans, and potentially go beyond our control. The application of artificial superintelligence in public, private and military spheres should, therefore, be sustainable in order to minimise threats to ICT networks and systems and also humankind. There is particular responsibility vested in the public sector for how we are going to deploy AI. We need to build TRUSTED AI. As UN Secretary General António Guterres said in Paris in November 2018 at the Internet of Trust Forum "technology should empower, not overpower us".[37] This is cybersecurity in the AI era *per se*.

35 L. H. Anh, *Roadmap of technological singularity* [on-line]. Available at: https://medium.com/twogap/roadmap-of-technological-singularity-45fcfe3bc718.

36 R. Cellan-Jones, *Stephen Hawking warns artificial intelligence could end mankind* [on-line]. Available at: https://www.bbc.com/news/technology-30290540.

37 A. Guterres, *Address to the Internet Governance Forum* [online]. Available at: https://www.un.org/sg/en/content/sg/speeches/2018-11-12/address-internet-governance-forum.



CYBERSECURITY: KEY REGULATORY ASPECTS

One of the main goals of the European Union is to facilitate cross-border exchange of goods, services and people. Playing an important part in this exchange are information systems, including the Internet. Because of the transnational nature of many such systems, disruptions in their operation – caused by cyberattacks, among other things – may affect individual Member States as well as the entire EU. Security of network and information systems therefore affects efficiency of internal markets.

In recent years, an increase in the number of incidents posing threats to the operation of network and information systems has been observed in the European Union.

Answering such incidents on the part of EU legislation is Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive). The final date for implementation had been set to 9 May 2018; in some EU states (Poland, among others) the Directive was implemented late.
The Directive sets out certain obligations for the states as well as imposes obligations connected with network security on a large group of entrepreneurs. Five main categories of tasks related to cybersecurity are regulated by the Directive.

First, for all Member States it lays down an obligation to adopt a **national strategy on the security of network and information systems.** That strategy should define strategic objectives, and appropriate political and regulatory means of achieving and maintaining a high level of security of network and information systems, covering at least the essential service and the digital service sectors defined in the Directive.

Second, the NIS Directive created a **Cooperation Group**, in order to support and facilitate strategic cooperation and exchange of information between Member States, and to develop trust and cybersecurity confidence among them. The Cooperation Group is composed of representatives of Member States, of the Commission and of the European Union Agency for Network and Information Security (ENISA). The task of the Group is, above all, to exchange information, best practice and experience related to cybersecurity.

Another important aspect of the NIS Directive is the creation of a **computer security incident response teams network** (CSIRTs network), in order to contribute to the development of trust and confidence between Member States, and to promote swift and effective operational cooperation. Each state designates one or more CSIRTs which are to comply with the requirements set out in the Directive. That team's duties include managing risks and handling cybersecurity incidents.

Furthermore, the NIS Directive sets out **security and incident reporting requirements for operators of essential services and digital service providers**. Essential services are the services of sectors such as energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure. Operators of essential services are identified by competent authorities, based on criteria indicated in the NIS Directive, including whether provision of a service depends on network and information systems and whether an incident would have significant disruptive effects on the provision. Digital services are online marketplaces, online search engines and cloud computing services.

Ultimately, the NIS Directive regulates Member State obligations concerning designation of **competent authorities, single points of contact and CSIRTs** whose tasks are related to network and information system security.

In the Directive the term "incident" is defined as any event having an actual adverse effect on the security of network and information systems.

Poland's Act of 5 July 2018 concerning national cybersecurity strategy is an example of implementation of the NIS Directive. Three computer security incident response teams operating on a national level have been appointed by the Act, run by Head of the Internal Security Agency (CSIRT GOV), by the Minister of National Defence (CSIRT MON) and by the national research institute Research and Academic Computer Network (CSIRT NASK) respectively.

The Act defines rules of designating operators of essential services as well as competent authorities to designate those operators, and describes the operators' responsibilities in detail. Accordingly, responsibilities of an operator of essential services include, among other things:

1. regular assessment of incident risk, and managing the risk;
2. implementation of state-of-the-art technical and organisational measures which are adequate and commensurate with the results of risk assessment;
3. gathering information about cybersecurity threats and susceptibility to incidents of the information system used for providing the essential service;
4. incident handling;
5. taking measures to prevent and limit the effect of incidents on security of the information system used for providing the essential service;
6. using such means of communication which allow normal and secure communication in line with the national cybersecurity strategy.

It is an operator's responsibility to maintain records on cybersecurity of the information system used for providing the essential service. The operator should either establish an internal hierarchy for the purposes of cybersecurity or enter into agreement with an entity which is providing

such services. A security audit of the information system used for providing the essential service should be performed at least once in two years.

Digital service providers are not designated by decision, and the scope of their responsibilities is narrower than that of operators of essential services.

It is a provider's responsibility to implement adequate and commensurate technical and organisational measures defined in executive order 2018/151 for managing risk of information systems used for providing the digital service. The provider also has several incident-related responsibilities.

Ultimately, the Act expressly applies to certain public entities. Their responsibilities are limited to appointing contact persons for national cybersecurity strategy entities, and to the handling of incidents.

The Act has established the office of Government Plenipotentiary, whose role is to coordinate activities and pursue government policy as regards ensuring cybersecurity. The Plenipotentiary is appointed and dismissed by the Prime Minister. Furthermore, a dedicated Council of Ministers committee acts as consultative-advisory body for cybersecurity and the related activity of CSIRT MON, CSIRT NASK and CSIRT GOV, of sector-specific cybersecurity teams and of competent cybersecurity authorities. The Prime Minister is the committee's chairman, with Ministers and other high-ranking officials being members of it. The establishment of the bodies mentioned above as well as their membership proves how much weight is attached in Poland to the security of network and information systems.

The NIS Directive is only one of the recent examples representing further transnational steps aimed to enhance European cyber resilience. The 2017 revision of EU Cybersecurity Strategy produced the so called "EU Cybersecurity Package", which proposes a wide-ranging set of measures, focusing on three key achievements: (1) **resilience**, (2) **deterrence** and (3) **defence**.

(1) **Resilience**:

Regulation on the "Creation of an European Cybersecurity Industrial, Technology and Research Competence Centre":

Part of the 2017 Cybersecurity Package, the scope of the Regulation is to develop the technological and industrial cybersecurity capacities and increase the competitiveness of the Union's cybersecurity industry. Among others, the Competence Centre should facilitate joint investment by the Union, Member States and industry, and should contribute to the implementation of the cybersecurity part of the "Digital Europe" and "Horizon Europe" Programs. The Regulation will also establish a Community, seeking to gather all relevant European actors involved in cybersecurity technology – in particular research entities, supply-side industries, demand-side industries and the public sector.

According to the initial proposal, companies outside Europe could be potentially excluded from contributing their expertise to improve cybersecurity research and competence in Europe, because only EU-established entities would qualify as members of the Community. Yet the global nature of the ICT supply chain cannot be neglected and excluding global partners can become counterproductive.

Research, innovation and the development of any new capacities require the involvement of all stakeholders in the supply chain – customers, the research community and the private sector. Without granting a platform for industry to provide valuable input, the proposal will be faced with challenges in addressing market shortages of cybersecurity solutions, resources and instruments.

Furthermore, the Centre and the Community could represent an opportunity for the EU to establish a comprehensive framework for

managing vulnerabilities in collaboration with ENISA. We have recently seen how unpatched software flaws, glitches or weaknesses can cause significant damage. There is a growing market for the purchase of vulnerabilities, where governments also play an increasingly large role. To reduce (and ideally prevent) exploits being used in such attacks, more effective vulnerability disclosure policies are needed, by which governments would report vulnerabilities they discover directly to vendors.

(2) **Deterrence:**

Council Conclusions on a **"Framework for a joint EU diplomatic response to malicious cyber activities"** (Cyber Diplomacy Toolbox):

Initially proposed in 2015, the Council adopted the Conclusion on the "Cyber Diplomacy Toolbox" in June 2017. The EU is concerned by the increased ability and willingness of state and non-state actors to pursue their objectives through malicious cyber activities. Such activities may constitute wrongful acts and could give rise to a joint EU response. Since then, the Council is continuing discussions on how to best operationalise this Toolbox, i.e. which kind of coordinated response the EU should consider.

Today, there is little accountability for perpetrators of such attacks. There are no obligations for states to refrain from targeting civilians and the essential infrastructure that underpins our societies, and no clear obligations to prevent the use of one's own territory for cyberattacks. Information about who is responsible for an attack is rarely made public, and even when information is shared, the data that underpins it is not. Establishing and clarifying such a framework for joint responses to cyber activities is a first essential step to deter cybercriminals and increase the cost of coercive cyber operations. However, deterrence rests on improving cyber attribution. Without effective attribution, we cannot hold those who violate the rules to account, nor can we deter them from continuing their activities.

(3) **Defence:**

Cyber Situation Awareness Package Project:

The 2013 Cybersecurity Strategy emphasizes that "Cybersecurity efforts in the EU also involve the cyber defence dimension." Consequently, the European Council adopted a "Cyber Defence Policy Framework" in November 2014, highlighting five priorities, e.g. promotion of civil-military cooperation and synergies with the private sector in the field of cyber defence. However, as cyber defence and cyber diplomacy are outside EU competences, this third pillar of EU action has not particularly progressed compared with other areas of cybersecurity.

Among different issues – including cyber ranges and cyber simulations for military personnel – the European Defence Agency (EDA) is currently working on cyber defence situation awareness for military operations, meaning it is trying to integrate cyber defence in the conduct of any military missions.

In particular, in order to enable military commanders at all operational levels to understand and manage the risk of cyberattacks, three contributing Member States – Spain, Germany, Italy – recently launched a **"Cyber Situation Awareness Package Project"** conceived as the first step in order to set up a full Cyber Situation Awareness operational capability to ultimately assist military decision-makers in cyberspace.

The next step should be to focus on better collaboration with the tech industry in these efforts. With cyberthreats becoming more and more complex, early detection of the most advanced Advanced Persistent Threats (APTs) and sharing of information have become crucial components for an effective response to cyberthreats. Therefore, establishing a strong partnership between the public and private sectors remains an essential element of not only enhancing resilience, but also reinforcing defence.

Another important regulatory aspect of cybersecurity on the EU level is **standardisation**. In connection with implementing security solutions and handling incidents, Member States should use European or internationally accepted standards and specifications relevant to the security of network and information systems. Important is the role of ENISA, which – in collaboration with Member States – draws up advice and guidelines regarding the technical areas to be considered in relation to the implementation of such solutions as well as regarding already existing standards, including Member States' national standards.

The so-called **Cybersecurity Act**, on which the European Parliament, the Council and the European Commission reached a political agreement in December 2018, will broaden the role of the Agency: the competence of ENISA will be strengthened, especially as regards certification of various IoT devices, services and processes in terms of immunity to cyberattacks. In order to remedy the current situation where a patchwork of cybersecurity certification schemes and initiatives exists in the EU, ENISA will create and implement a European certification framework encompassing a comprehensive set of rules, technical requirements, standards and procedures. Certificates will be applicable in the entire European Union, thus reducing the barriers to and the potential fragmentation of the Digital Single Market. As certification will undoubtedly contribute to the development of a higher EU-wide cybersecurity level, it will also greatly stimulate the completion of the Digital Single Market, enhancing competitiveness through reduced time and cost of certification and in the end contributing to the promotion of a chain of trust between vendors and end-users. Extending the mandate of ENISA and increasing its resources will also encourage a stable and continuous work to increase cybersecurity in the EU and foster cooperation and coordination among Member States in this field.

There are also other steps which confirm that cybersecurity is very high on the EU political agenda: the entry into force of the **General Data Protection Regulation**[38] in May 2018, the **ePrivacy Regulation** (the proposal for a regulation that would repeal the 2002 Directive on Privacy and Electronic Communications),[39] the revision of the **Open Data Directive**, on which an agreement was reached in January 2019,[40] the 2017 recommendation of the European Commission on **Coordinated Response to Large-Scale Cybersecurity Incidents and Crises**,[41] and ever deeper discussions on the latest technological challenges such as 5G, blockchain, AI or HPC.

38 European Commission, *2018 reform of EU data protection rules* [on-line]. Available at: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#aboutthereg-ulationanddataprotection.

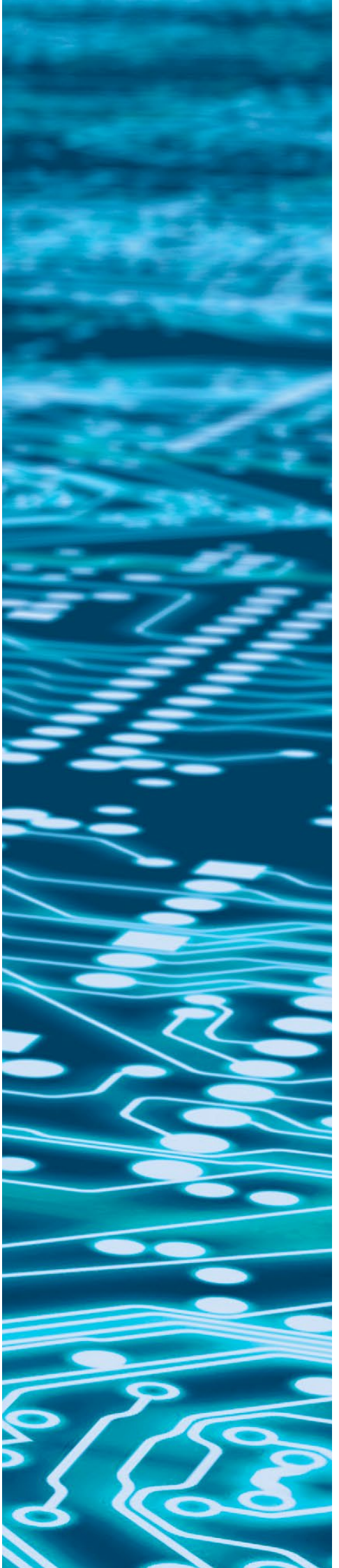
39 i-scoop, *The new EU ePrivacy Regulation: what you need to know* [on-line]. Available at: https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/#Next_steps_and_WHEN_the_ePrivacy_Regulation_might_be_applied_which_is_not_the_same_as_entering_into_force.

40 European Commission, *Proposal for a revision of the Public Sector Information (PSI) Directive* [on-line]. Available at: https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive.

41 European Commission, *Cybersecurity* [on-line]. Available at: https://ec.europa.eu/digital-single-market/en/cyber-security.

THE KOSCIUSZKO INSTITUTE

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank) founded in 2000. The Kosciuszko Institute aims to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic Alliance. Studies conducted by the Institute have been the foundation for both important legislative reforms as well as content-related support for those responsible for making strategic decisions. The Kosciuszko Institute is the originator and organizer of the European Cybersecurity Forum – CYBERSEC, an annual conference dedicated to the strategic aspects of cyberspace.



PARTNERS OF THE REPORT:

Microsoft

pwc

THE KOSCIUSZKO INSTITUTE