Cybersecurity Resilience in Digital Society – the Practical Approach

Ewa Niewiadomska-Szynkiewicz <ewan@nask.pl>,

Marek Amanowicz <marek.amanowicz@nask.pl>,

Agnieszka Wrońska <agnieszka.wronska@nask.pl>,

Paweł Kostkiewicz <pawel.kostkiewicz@nask.pl>
WARSZAWA, Poland

Abstract
Modern societies are deeply dependant on information technology, which means that threats to the availability, integrity, and confidentiality of information and communications infrastructure can significantly impact the functioning of the state and the safety of citizens.

This chapter intends to present the threats connected with the widespread use of digital technologies and the mechanisms for protecting states, institutions, and citizens against these threats. It gives an overview of national and international activities and those of the European Commission to increase security and situational awareness. The authors discuss commonly used protection techniques and mechanisms and safeguard systems to increase society's resilience to cybercrime and give examples of such solutions developed and implemented in Poland. They pointed out the importance of cybersecurity certification procedures and conformity assessment schemes for increasing the resilience to cyberthreats. The chapter concludes with some remarks on the future and challenges.

Keywords:
information and communication technologies, cyber threats, society resilience, cybersecurity protection, security certification, situational awareness

1. Introduction

Information and communication technologies (ICT) have become an indispensable component of modern societies. They are deeply dependent on information and communication infrastructures in all forms of their activities, from governance and economics to the entire exercise of civil rights and freedoms. The rapid development of telecommunication and information networks, systems and applications contribute to creating new, more effective work organisation and process management forms. Advances in mobile technologies, providing anytime, anywhere access to systems and resources, support effective management and business operations and stimulate the development of novel organisational, procedural and socio-economic solutions. By facilitating broad access to global information resources, ICT becomes a stimulator of innovative forms of human communication and leads to significant reassessments in social behaviour. The numerous social networks are becoming a primary source for disseminating information and expressing opinions and views. The use of electronic means of communication is an increasingly common form of human contact.

The reliance on information technology means that threats to the availability, integrity, and confidentiality of ICT infrastructure can significantly impact the functioning of the state and the safety of citizens. At the same time, due to their complexity, modern ICT systems are increasingly vulnerable to cyber-attacks. Individual protection of autonomous systems using a simple analysis of transmitted messages is becoming insufficient. There is a clear need to create new, holistic solutions utilising a fusion of data obtained from multiple sources, integrating different methods, mechanisms and algorithms. Volume, quality, reliability and timeliness of data and information on the situation in the network, and the speed of its processing, determine the effectiveness of protection by preventing threats and identifying the type of attack and responding to their occurrence. Government institutions and commercial companies use many safeguards to protect their networks, but these are often limited in scope.

The challenge is to increase situational awareness by detecting known threats and recognising anomalies on the computing systems that may be symptomatic of malicious activities. It requires advanced frameworks and tools for distributed monitoring, reporting, and aggregation capabilities, to derive events, measures, metrics for deeper processing and analysis. Data fusion, advanced statistics, machine learning techniques and deep learning are often used to correlate a broad range of security contexts for cyber threat intelligence. A further challenge is to extend trust and integrity of

data and the execution environment by including access control, identity management, privacy and accountability in executing all processes and trust mechanisms that ensure a high level of security. When building security systems, it is essential to remember the human being in the loop. Therefore, behavioural, social and human aspects must be included in the engineering process to avoid the risk of neglecting or underestimating security threats.

The transfer of activities to the Internet and problems associated with assuring cybersecurity and the reliable functioning of states have led to significant international and national efforts. The activities included legislation, policies and cybersecurity agendas, roadmaps at the national and international levels, and initiating national and international research projects that result in innovative solutions.

On the 6th of July 2016, the European Parliament and the Council of the European Union passed the Directive on the security of network and information systems, colloquially called the NIS Directive [NIS, 2016]. The European Union Member States has issued the relevant legislation implementing the NIS Directive and adapting it to their local legal systems. On the 5th of July 2018, the Polish Parliament passed the Bill on the National Cybersecurity System (NCS) [NCS,2018] to create an efficient and secure system that should increase the protection against computer threats in Poland and enable effective cooperation with the EU Member States. NCS implements into the Polish legal system the NIS Directive. The Act on NCS appoints three institutions to serve as response teams – the Internal Security Agency (GOV CSIRT[1]), NASK – National Research Institute (NASK CSIRT[2]) and the Ministry of National Defence (MON CSIRT[3]). All these institutions work with one another and with other organs responsible for cybersecurity. Together, they constitute a coherent and complete national risk management system, combating cybersecurity threats, both sector-specific and cross-border, as well as coordinating the handling of all reported incidents. The institutions making up the national cybersecurity system form a cohesive whole, making it possible to take a wide range of practical actions to counteract threats and successfully respond to hazards. They are active participants in various national programmes and cross-border initiatives. The NASK CSIRT receives and analyses reports, takes actions and coordinates responses to incidents occurring in

1 <https://csirt.gov.pl> accessed 1 June 2021.
2 <https://cert.pl> accessed 1 June 2021.
3 <https://csirt-mon.wp.mil.pl/pl> accessed 1 June 2021.

Polish civilian cyberspace reported by key service operators, digital service providers, local authorities and individuals. It also responds to incidents involving the uploading of illegal content or poses a hazard to children and monitoring online threats and the level of cybersecurity in individual sectors and the entire country.

In 2018, the European Commission presented a proposal for establishing a European Cyber Security Competence Centre for industry, technology and research with national coordination centres. The proposal aims to stimulate the European technology and industry ecosystem and strengthen cooperation on cybersecurity between different industries and research communities. The centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes: Digital Europe and Horizon Europe for 2021-2027. The book [Felkner, 2020] gives an overview of the most important findings related to cybersecurity research analysis for two exampled regional entities, the Europe Union and Japan, in the last two decades. It highlights the progress in the legal and regulatory area within the privacy and cybersecurity domain and the number and diversity of research funding initiatives. On the other hand, the book points the potential blockers and issues to strengthen the cooperation between different regions. One of the crucial blockers is sharing data and knowledge due to the need to protect sensitive, private data and protect national interests.

Information sharing between national stakeholders and countries are significant activities to improve a security level. It is desirable for the parties concerned to provide each other with knowledge on tackling attacks, incident response and protection and mitigation methods. These are essential tasks of Information Sharing and Analysis Centers[4] (ISACs), non-profit organisations that provide a central resource for gathering information on cyber threats and sharing experience, knowledge and analysis. The NIS Directive groups the operators of vital services in sectors and tasks them to implement incident and threats reporting requirements. Both the Cybersecurity Act and the NIS Directive nourish the creation of sectoral ISACs within the EU. In the many EU Member States, ISAC or similar initiatives have already existed. ISACs are trusted entities to foster information sharing between the public and the private sectors about security incidents and threats, focusing on critical infrastructure. In 2018 ENISA published a report on cooperative models and best practices for ISACs [ISAC, 2018].

4 <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing> accessed 1 June 2021.

The authors intend to present the threats connected with the widespread use of digital technologies and the mechanisms for protecting states, institutions and citizens against these threats. In this chapter, we present national and international activities, and those of the European Commission, to increase security and situational awareness. We discuss commonly used techniques and mechanisms of protection and defence systems. We present examples of early warning and fraud detection systems developed and implemented in Poland.

2. *Society Resilience*

Internet originating and usage caused the greatest, since printing development, cultural change of real character, encompassing social, economic, political, and personal phenomena. The Internet has changed society and the way of learning and interacting with others. Virtual space is more and more strongly integrating with reality. Many infrastructural, economic, and social factors connected both with easier access to the web and the benefits resulting from using it comprises fast growth of Internet popularity. The development of technology made it possible to connect with the Internet from anywhere, at any level, using every device equipped with specific technology. The Internet is attractive thanks to obtaining current information fast, communicating with others, and getting access to different content sources.

What seems to be interesting is the social dimension of Internet use. With the everyday use of this tool, the borders of countries and languages disappeared. Users from all over the world can communicate with each other at any place and time. The latest data shows that digital, mobile, and social media constitute inevitable and more extensive and significant parts of daily human lives worldwide. Over 50 % of the world's population use the Internet, and the number of people who use social media exceeded 3,8 billion [ITU 2020, Digital Report 2020][5]

What is observed is the influence of the Internet on society and its particular group behaviour patterns (Wrońska, Lange 2016). The dimension of the changes is determined by habits, practices, and ways of using the Internet. That applies to both population in general and young users, which is the group that is seen as one of the most active online. Access

5 <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> accessed 1 June 2021.

to its content has two aspects. On the one hand, the web arranges free time and becomes a prime mover of personal development, initiative, and creativity, and is the place and tool of social communication.

On the other hand, it is a territory full of traps and threats with a more complex character. It has been almost thirty years since information technology had been transferred to everyday social use and has become a universal ecosystem in which children worldwide exist. As quantity studies show [Livingstone 2014, Bąk 2015, Livingstone 2017, Pyżalski et al. 2019, Lange et al. 2020], the internet initiation age in the last decade has dramatically lowered. A few years ago, the average age was ten while currently, children begin to use the Internet on their own still before starting primary school [Kirwił 2011, Tanaś 2016, Kamieniecki et al. 2018, Wrońska, Lange, et al. 2018, Pyżalski et al. 2019, Lange et al.2021]. The studies show that the vast majority of Polish teenagers use the web every day, staying online between 4 and 6 hours on average [Kamieniecki et al. 2017, Pyżalski et al. 2019, Lange et al. 2021]. They engage in various types of online activities, in which they have been ever since and constitute an inseparable element of their lives and virtual space accompanies them in their cognitive, recreational, and interactive activities [Wrońska, Lange 2016]. The Internet attracts young people because it is easy to use, it is multimedia, interactive, and hypertext.

Nearly all young internet users commonly use social communicators and services (just 0,7 % point out that they do not use the Internet this way). The young so-called 'digital natives' – quoting the famous Prensky's statement [Prensky, 2001a; 2001b] – with courage and ease, move around intuitively within the expanse of the Internet. From an anthropologist's point of view, we can talk about developing global prefigurative culture [Mead, 2020]. Younger generations presenting needs, attitudes, and behaviour and transmitting their knowledge to older ones somehow give direction to civilisational changes. Of course, it cannot happen without the participation of older generations – experts who have specific competencies provide users with technological solutions. The Internet is the tool of communication and content for the young generation. It has also become an essential attribute of social identity that lets them create daily life scenarios, affiliative strategies, and aspirational hierarchies. The Internet has changed their plans and time budgets, ways of education and spending their free time, and revolutionised the creation of so-called social identity. Smartphones and laptops have become the centre of the interaction with the world; most of the experience interactions, information, knowledge communication, entertainment are sometimes reduced and formatted to the abilities of the screen or data package.

The positive role of the Internet is undeniable, but at the same time, it is essential to remember that using the global web creates real threats. They relate to cybersecurity threats, content that occurs on the web, dangerous contacts, and more complex internet conduct. The typology (content-contact – conduct) created for the needs of a European research project concerning online dangers for kids is the best known – EU Kids Online [Livingstone et al. 2011]. Online safety and threats is a complex and inhomogeneous area. The list of threats to which a young internet user is exposed comprises an extensive catalogue of dangers. It is impossible to close it due to the incredible dynamics of web evolution. In general, the division involves the following categories of risks:

- contact with illegal and harmful content (presenting violence, physical injuries, cruelty towards humans and animals), encouraging self-destruction (self-injuries, suicides, taking harmful substances), inciting to intolerance, hostility or animosity as well as children pornography, including child sexual abuse material (CSAM),
- dangerous contacts, including child grooming,
- risky behaviour, including sexting,
- cyberbullying,
- internet addiction / problematic use of the Internet,
- risks connected with computer crime, cybercrime.

The above-presented classification does not include a growing spectrum of issues, and it may be assumed that it will be evolving in the following years. From the point of view of all threats connected with internet development, widely understood so-called anonymity and protection of internet users' privacy seem to be especially vital.

The scale of recorded threats and indicated social needs demand coordination of actions to provide safety in cyberspace. Reacting against threats in cyberspace ought to go in a few directions. One of them is initiating broad-based social activities in the scope of global education and prevention; the second one – difficult to complete because of the cross-border character of the Internet – applies to legislative actions. The necessity to guarantee the safety of the youngest internet users constitutes not only the execution of indicated in Art. 72 of the Polish Constitution the duty of children protection against violence, cruelty, abuse, and demoralisation. Regulations legitimised in criminal law which penalises various forms of online violence towards juveniles are mostly connected with crimes against freedom (e.g., persistent harassment, violation of sexual intimacy), sexual freedom and decency (e.g., sexual abuse of a minor, promotion of paedophilia). They also concern crimes against honour and physical integrity (e.g.,

defamation) and crimes against information (e.g., unauthorised access to information). It is related to compliance with regulations of international character, including recommendations of the European Strategy for a Better Internet for Children, the Comprehensive Strategy on the Rights of the Child, and the Convention on the Rights of the Child, to which Poland is the side. National and international safety policy cannot ignore any of the spaces of children and youth's activity, especially as important for personal human development, their social relations and the culture which makes cyberspace currently. In December 2020 European Committee presented long-awaited projects of horizontal regulation of actions and duties of internet services suppliers[6]. However, another step towards increasing safety on the Internet is protecting fundamental rights and establishing a solid and stable management structure in need of adequate supervision of intermediate services suppliers. Standardising European regulations should increase its effectiveness and simplify its implementation by service providers, who frequently operate internationally. When the safety of the youngest internet users is considered, it will be complementary for horizontal projects to present more precise Committee proposals dedicated to the children's rights protection.

NASK National Research Institute has conducted various actions dedicated to internet safety, including the safety of its youngest users. NASK experts organise social campaigns, accomplish educational programs, conduct studies on civilisational, economic, legal, and cultural phenomena in society and technology, prepare publications, and share their knowledge during local and international meetings. NASK is the coordinator of the Polish Safer Internet Centre (PCPSI), which was established in 2005 under the European Commission's Safer Internet Programme and now operates under the Connecting Europe Facility Programme[7]. Moreover, over 15 years ago, in response to the risk of producing and distributing sexual abuse materials, the team Dyżurnet. pl has been constituted. Since 2018 it has been accomplishing tasks of CSIRT Poland under the regulation of the National System of Cybersecurity. Dyżurnet.pl is a member of INHOPE[8], the association of reacting teams, which cooperates with Interpol and technological companies. The team of Dyżurnet.pl takes and analyses reports from internet users concerning illegal content, mainly including child's se-

6 <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN> accessed 1 June 2021.

7 <https://www.saferinternet.pl> accessed 1 June 2021.

8 <https://www.inhope.org> accessed 1 June 2021.

xual abuse materials. The hotline has analysed over 133 000 incidents since 2005. Dyżurnet. pl develops tools that court experts use to identify illegal content and accomplish a project about developing automated technology to detect child sexual exploitation and abuse[9]. The team of Dyżurnet. pl analyses legal regulations which control aspects connected with fighting sexual abuse of children and prevention against the distribution of illegal content. NASK experts take actions in this scope to support government institutions with expert knowledge and experience.

The theoretical and empirical dimension of online threats and safety of the youngest Internet users in cyberspace refers to many theories and concepts related to children and adolescents' activity in the real world. An interdisciplinary approach is essential here. It is necessary to have appropriate competencies, tools, and solutions supporting protection and legislation to take advantage of the Internet's enormous potential while avoiding danger zones. The youngest Internet users require special care and support. Therefore social communication aimed at popularising and promoting the idea of taking care of their safety is a critical area of education, prevention, technology, and law.

3. ICT threats and vulnerabilities

The dynamically growing number and constantly appearing new types of threats on the Internet create many problems related to ensuring security for private network users, organisations and critical state institutions. Many types of malware attacks designed to perform undesirable operations on the victim's computer are identified. These include intercepting sensitive information and disrupting computers. When a software vulnerability is detected and maliciously exploited, the effects of the unwanted actions can affect multiple network users, e.g. by accessing an infected website. Furthermore, attackers are often responsible for automatically distributing malware from infected computers to other network users to increase the number of victims.

An exponentially growing number of cyber-attacks on Internet users occurs through malware applications installed by users from untrusted sources or even official resources provided by the operating system author (e.g. Google Play store for Android), and SMS or e-mail messages containing links to malicious applications or redirecting to fake websites. The

9 <https://dyzurnet.pl> accessed 1 June 2021.

most common threats currently targeting the digital society are phishing campaigns that target data. Check Point's research shows that the government and financial services are most vulnerable to attacks. Both areas offer attackers valuable caches, such as repositories of financial and personal information.

Cybersecurity teams from various countries confirm that a successive increase in incidents and notifications has been observed for many years. The CERT Polska team operating in the structure of CSIRT NASK handled 22 343 submissions in 2019 [CERT, 2019]. As a result of the analysis, it registered a total of 6 484 cybersecurity incidents. It is a record number and a record increase compared to the previous year (73 %). The most common type of attack was phishing, which accounted for about 54.2 % of all incidents. In second place were reports of malware - 14.9 %. Incidents in the "offensive and illegal content" category, including spam, accounted for approximately 12.1% of all recorded incidents. The use of false information is becoming increasingly common, whether for phishing sensitive data, criminal activities or propaganda campaigns. The year 2019 saw a significant increase in ransomware infections in the industrial, medical and government sectors. Ransomware is software that encrypts data to extract a ransom. An increasing number of incidents have been reports of illegal and offensive spam-like content. In Poland, the number of such reports increased by around 88 % compared to the previous year.

Distributed denial of service (DDoS)[10] attacks block the operation of important institutions for the state and citizens; their range of harmful influence is increasing. Mirkovic and Reiher provide a comprehensive taxonomy of DDoS attacks in [Mirkovic, 2004]. They classify DDoS attacks in terms of the type of exploited vulnerabilities, traffic source validity, the degree of automation required, attack rate dynamics, bots' persistence, victim type, and exerted impact. Modern DDoS attacks are complex, multidimensional attacks of time-varying dynamics, generating traffic from spoofed and highly distributed sources. Massive attacks often occur using a specific class of devices (e.g. WiFi routers, smartwatches, printers with wireless interfaces), usually from a single vendor, and exploiting a specific vulnerability. The intercepted devices are used to initiate DDoS attacks, distribute malicious software, or cryptocurrency mining depending on the attacker's intentions.

Nowadays, many industrial control systems are directly accessible from the Internet. A number of them provide remote control options. The US

10 <www.cloudflare.com/learning/ddos> accessed 1 June 2021.

Cybersecurity and Infrastructure Security Agency[11] (CISA) reports numerous incidents where attackers seek out such devices and use them as an attack vector against industrial networks.

The widespread use of Internet of Things (IoT) devices has significantly increased the interest of cybercriminals in IoT systems in recent years. The users of IoT are exposed to various new forms of attacks. Insecure IoT devices are already exploited and used in massive attacks and rapidly increase the number of victims [Zhuge, 2020], [Neshenko, 2019]. There are still many active botnets, with new ones taking advantage of increasingly common IoT devices. The most common threats listed in the Open-Web Application Security Project (OWASP) Top 10 Internet of Things list [OWASP, 2018] are weak guessable, or hardcoded passwords, insecure network services, ecosystem interfaces, data transfer and storage, lack of insecure update mechanism and device management, insufficient privacy protection. Unfortunately, removing even the well-known vulnerabilities is difficult and costly as it often requires modifications to the hardware and involves the manufacturer.

A famous example is the Mirai botnet performing large scale DDoS attacks [Antonakakis, 2017]. Attacks on IoT devices are becoming more advanced and specialised. They often target a single vulnerability in a specific model of a selected manufacturer. The purpose of using seized devices is also changing - in addition to DDoS attacks, attackers are increasingly interested in data theft, malware distribution or cryptocurrency mining. Moreover, more and more malicious applications are being developed for mobile devices.

To summarise, the topic of IoT security is still too little researched and developed. Cyber-attacks may become even larger and more frequent if no action is taken to secure the IoT systems. It is a reason while the security of IoT and mobile devices is such important for people and industry. At the same time, numerous manufacturers neglect security aspects. They often ignore vulnerabilities found in IoT devices and software. The report [IoTSF, 2018] of the research conducted by the IoT Security Foundation shows that in the 2018 year, only 10 % of 331 IoT vendors sampled have implemented any vulnerability disclosure policy. Moreover, even vulnerabilities are identified, disclosed to vendors, and mitigated by them, and they are rarely announced to the public by the vendors themselves. Therefore, there is a meagre amount of publicly known vulnerabilities, while the total amount of vulnerabilities is supposedly large. There is no universal

11 <https://www.cisa.gov> accessed 1 Juned 2021.

way to track and mitigate them. Solving these issues would greatly benefit from a publicly available source of structured information about known IoT vulnerabilities and exploits. Currently, none of the existing solutions is satisfactory. The available repositories are not focused on the IoT, highlighting the need for new projects in securing IoT. Recently, several research projects have been initiated to develop new techniques for detecting unknown vulnerabilities and exploits [Janiszewski, 2021]. The open-access databases of publicly known vulnerabilities and exploits affecting IoT devices are under development. An example is a system created within the Variot[12] project. The challenge is to detect vulnerabilities as fast as possible and immediately notify about new vulnerabilities.

4. Cybersecurity protection methods and defence systems

Malware and security incidents detection techniques

To meet today's security requirements and maintain the continuity of an organisation's operations, it is essential to ensure efficient and effective response activities to identify and quickly respond to cybersecurity incidents. Ensuring data transmission security is one of the most crucial problems faced by computer network administrators. Quick detection of threats, especially mass campaigns, allows protecting systems from the possibility of their damage or destruction. The fundamental problem is the high rate of spreading attacks and the vast amount of data necessary to process to identify them. Analysis and classification of network data collected from various sources and identification of security incidents effectively support software systems and services that significantly enhance the security of government, state administration, institutions and citizens. Strategies and mechanisms for effective and rapid detection of threats are the main elements of many defence systems. Many malware detection techniques can be listed. The most important of these are:

– anomaly detection, which involves the detection of abnormal behaviour, including deviations from typical network traffic loads,
– signature analysis, i.e. comparing the content of a tested file with a set of previously created threat patterns.

12 VARIoT (Vulnerability and Attack Repository for IoT) CEF project founded by the European Commission, <https://www.variot.eu> accessed 1 June 2021.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are parts of the network infrastructure used to protect networks from cyber-attacks. IDS systems continuously monitor the network for signs that indicate attackers that are using a known cyber threat to infiltrate or steal data from it. IDS systems compare the current network activity to a known threat database to detect such behaviours as malware, security policy violations, and port scanners to detect unusual situations. IPS systems operate at the interface between the internal network and the outside world. They proactively deny network traffic based on a security profile if that packet represents a known security threat. IDSs/IPSs implement various architectures and different approaches to the problem of detecting threats. They also offer different levels of security. The survey of intrusion detection systems is presented in [Gupta, 2021], [Khraisat, 2019].

Security Information and Event Management (SIEM) is a set of tools and services offering a holistic view of an organisation's information security. These tools provide real-time visibility across an organisation's information security systems. SIEM combines two technologies: (i) security information management, which collects data from log files for analysis and reports on security threats and incidents, (ii) security event management, which conducts real-time system monitoring and analysing, establishes correlations between security incidents, and notifies network administrators.

In general, IDS/IPS and SIEM are responsible for data collecting, analysing and correlating. They use similar techniques in their operation. The Endpoint Detection and Response (EDR) is a more advanced technology. It is an integrated endpoint security solution that combines real-time continuous monitoring and endpoint data with rules-based automated response and analysis capabilities. Therefore, EDR looks deep into the system, gathers and analyses all activity. It allows for data fusion and correlations and different detection techniques. Moreover, EDR uses forensics and analysis tools to research identified threats and search for suspicious activities.

Most institutions, especially the key ones, establish Security Operation Centers (SOCs) – the centralised units that deal with security issues on an organisational and technical level. SOC comprises professionals with expertise in information security, processes, and technology for monitoring, analysing and protecting an organisation from cyber-attacks. SOCs help organisations respond to intrusions quickly and constantly improve detection and prevention processes.

The ability to keep the networks and systems of an organisation secure is often dependent on the knowledge of the threat landscape, new attacks and trends, new vulnerabilities and changing best practices. It also requires

specialised tools to monitor the global situation, detect security events, and provide data to network operators. The research and development teams in all countries conduct research and analyses regarding new technology applications and implementation. New services and innovative products make it possible to detect and counteract threats that significantly enhance government security, key institutions and citizens are developed. The example solutions presented in the following sections are designed to warn of cyber threats, detect DDoS attacks and prevent fraud in electronic transactions.

Early warnings of cyber threats

A crucial tool for observing attacks in the wild is a honeypot – a system deliberately exposed and seemingly vulnerable, designed to register and report connections and exploitation attempts. A significant non-technical advantage of using honeypots (apart from client-side honeypots) is that they are entirely passive endpoint systems. It is a very desirable trait in both ethical and legal contexts. By design, the honeypot is incapable of observing regular traffic. It only receives packets explicitly addressed to it – and since the honeypot offers no real services and is not advertised in any way, any traffic reaching it is suspicious. Most of this traffic will be either due to network scanning or an exploitation attempt, if deliberately addressed, or random, such as echos from DDoS attacks using source IP spoofing. The only non-malicious activity that may appear in a honeypot is either non-malicious scanning or a result of misconfiguration. In any case, the honeypot does not come in contact with any legitimate, sensitive user data.

Another technique of observing real-life attacks at scale involves using network telescopes, also known as darknets. Network telescopes are blocks of unused IP addresses. Like in the case of honeypots, any packets reaching them are by definition incorrect – apart from minor noise, such as misconfigured computers. However, unlike honeypots, network telescopes do not respond in any way to the incoming packets. It means that the information about the activity is limited, especially in the case of TCP. However, this also saves resources, enabling monitoring of ample address space. Also, while honeypots can often be identified and blacklisted by malicious actors due to imperfect emulation of real vulnerable services, network telescopes are indistinguishable from regular, unobserved unused IP space. The information in a network telescope is limited to single packets, which usually restricts them to a source of high-level statistics, such as top scanned ports,

etc. However, more advanced analytical capabilities allow extracting far more actionable information from the available data. The significant size of the darknet allows observing less common events and getting more accurate statistics. Monitoring all ports and being aware of the standard "background noise level" is a suitable method of spotting new activity. A sudden increase in scanning activity on a specific port may indicate that a new vulnerability has been found by malicious actors looking for exploitable services – either as potential targets that could be made part of a botnet or potential reflectors for amplification attacks. Another cause of sudden increases in activity is ongoing UDP DDoS attacks with spoofed IP addresses – with a large enough darknet, it is possible to deduce from the observed reflection both the algorithm used for IP spoofing and the estimated size of the attack. Reflexions are generally easy to identify and group into one attack, as all the packets have the same source – the target of the initial attack.

Early warning systems are a constant focus of the research and development teams at NASK and CERT Polska. Many of those systems trace back to the SISSDEN[13] project, which developed many innovative tools and systems gathering, enriching and publishing actionable threat data. Together, they can be considered a global early warning system, capable of noticing new kinds of threats and informing interested users. SISSDEN built a global network of honeypots, deployed on over 250 nodes in 58 different countries, monitoring almost a thousand IP addresses using 12 different honeypots emulating various services. Reaching this global scale economically and technically scalable way required a new approach to building the network. Instead of deploying and maintaining honeypots remotely in all locations, SISSDEN standardised on a simple, low-resource Linux node that could be obtained cheaply from many providers and ran a minimal system, tunnelling the incoming traffic from honeypot IP addresses to the honeypots deployed in the central datacentre. Hence, NASK operates one of the largest network telescopes in the region, with hundreds of thousands of addresses.

The objective of another early warning system - ARAKIS[14] is to report threats in the IT and OT network. It has been developed to build a network security landscape overview and support the detection of new network threats. Events correlated by the system are received from various

13 Secure Information Sharing Sensor Delivery event Network (SISSDEN), European Commission project, Horizon 2020, 2015-2019.

14 <https://www.arakis.pl> accessed 1 June 2021.

sources, including honeypots, darknet probes, firewalls and antivirus systems. Advanced analyses are possible due to the unique system architecture of distributed sensor network. A distinctive feature is an innovative algorithm for automatic detection of recurring patterns threats and creating SNORT[15] signatures describing detected attacks based on machine learning and advanced network engineering methods. Unique algorithms correlating the data collected by sensors with the unique set of signatures for reactive systems generated by ARAKIS enable comprehensive threat analysis and quick reaction to detected threats, including zero-day.

Information on threats and malicious applications delivered through many channels and received from early warning systems is collected and available on the net. They are created by local CERTs, such as the n6[16] system developed at NASK, or databases created by user communities, such as Koodous[17]. Expert groups continuously monitor and analyse multiple sources of information about cyber threats that can affect the integrity and availability of IT systems of protected organisations and their customers. Multi-level threat analysis, both technical, behavioural, and contextual, is performed based on data sources such as darknet, honeypot, sinkhole, spampot, spamtrap, and other open and closed monitoring sources non-indexed Internet layers (Deep and Dark Web). Collective threat intelligence service (CTI) is the continuous acquisition and delivery of information from external sources regarding cyber threats. This service increases the protection of organisations against new and targeted attacks, supports internal security teams of SOC and protection systems: SIEM, IDS/IPS, EDR.

DDoS defence systems

Many cybersecurity systems protect network resources against distributed denial of service (DDoS) attacks. A comprehensive overview of defence systems is presented in [Zargar, 2013]. The defence mechanisms can be characterised by preventive and reactive activity levels, deployment location and degree of required cooperation with other network mechanisms and services. Most systems focus only on attack detection. More advanced provide mitigation services. Reactive mechanisms differ in attack response strategies, including source-based or flow-based packet dumping, routing

15 <https://www.snort.org> accessed 1 June 2021.
16 <https://n6.cert.pl> accessed 1 June 2021.
17 <https://docs.koodous.com> accessed 1 June 2021.

reconfiguration, and attack rate-limiting. However, in all cases, the efficiency of attack mitigation depends on packet filtering methods and their efficiency.

The design of DDoS detection and mitigation mechanisms is a subject of many surveys. Authors point to significant practical challenges, such as separating the attack from legitimate traffic and implementing response tools in the network environment. In particular, packet filtering and rate-limiting are primary mechanisms to respond against the DDoS attack traffic [Kalkan, 2016]. In general, the detection of attacks is based on pattern matching algorithms. The observed flows of packets are compared with known attack fingerprints. A flow consists of packets that match conditions describing packet attributes, i.e. IP source and destination addresses, source and destination port numbers, or protocol. Next, a malicious detected flow is redirected to a scrubbing centre to be cleaned from malicious components. The standard model of DDoS protection is based on managed security services delivered by ISPs or DDoS Protection Service (DPS) providers.

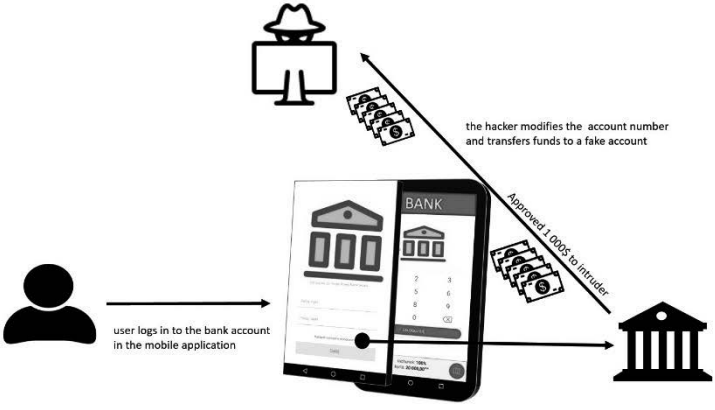
The FLDX[18] system is fast and highly effective in protecting the availability of network services in case of a volumetric DDoS attack or a sudden increase in user activity. Maintaining a fair distribution of network bandwidth is the primary goal of the system, achieved in an unrivalled time of even several seconds. The FLDX system uses machine learning algorithms to dynamically self-adjust filters to the current situation. This approach allows for a speedy response to observed changes in network load, as well as their forecast. FLDX is not only a protection tool - it is also a network knowledge discovery tool. The FLDX detection module offers high-resolution multidimensional monitoring of network activity, providing essential knowledge in near real-time. An extensive reporting system provides detailed descriptions of cybersecurity incidents, showing geolocation of sources, network connection structure and packet construction statistics. The speed and precision of the FLDX system is the result of years of research in the fields of control theory and adaptive signal processing.

18 <https://fldx.pl> accessed 1 June 2021.

Prevention of fraud in electronic transactions

The common threats currently targeting the digital society are phishing campaigns that target data, including personal information and users' financial resources. Theft of personal data occurs every 2 seconds[19]. Fraud can be committed in many different ways and many different settings. Fraud often affects banking, insurance, government, and healthcare sectors. The standard type of fraud in online banking is customer account takeover, through illegally gains access to a victim's bank account using bots. The current trend of threats consists of injecting malware (web injection) into web browsers allowing for modification of the bank's transaction site on the user's side (Man-in-the-Browser). The attack is depicted in Figure 1.

Fig. 1. Man-in-the-Browser attack.



Web fraud attempts detection is a set of processes and analyses that identify and prevent unauthorised financial activity. The primary reason to use data analytics techniques is to tackle fraud since many internal control systems have serious weaknesses. The dedicated mechanisms for predicting conventional tactics and uncovering new, sophisticated schemes of fraud attacks have been developed. They apply predictive and adaptive analytics techniques, including data mining, statistics, clustering, machine learning

19 <https://mobilitynews.pl/raport-symantec-urzadzenia-mobilne-zagrozone-cyberatakiem> accessed 1 June 2021.

and deep learning [Babu, 2020], [Shirodkar, 2020]. The real-time monitoring is combined with big data gathered from multiple sources processing.

The BotSense[20] system enables real-time detection of all Web fraud attempts caused by a change of the transaction service content on the bank's customers' desktop or mobile device. The system's effectiveness is based on a signature management mechanism and dynamic analysis of the Document Object Model (DOM) structure for behaviours exceeding the regular operation of the electronic banking transaction system. It generates JavaScript code that detects web-injects on the bank customers computers based on the signatures of cyber-attacks. BotSense allows the banks to detect and monitor individual customers infected by malware and protect their customers against attempts to steal funds or sensitive data.

5. Global situational awareness

Protecting against a constantly growing number of increasingly sophisticated and complex cyber-attacks requires, as has been mentioned earlier, new functionalities enabling detection, assessing and preventing them. It also demands the achievement of a reliable cyber situational awareness picture, online delivering validated information on identified threats and risks and their impact on the behaviour of systems and related processes and services. It denotes particularly to those vital to the state security, public and economic order, functioning of public institutions, civil rights and freedoms, and human life and health. However, as presented in several works, for instance [Rinaldi, 2001], [Zimmerman, 2004], [Nieuwenhuijs, 2008], [Setola, 2016], the situation complicates the strong systems' dependencies and shared information and communications technology resources. The various infrastructures are complex in themselves, especially when factors such as markets, government regulations, policies, legal and other socio-technical aspects must be considered. However, infrastructures do not exist in isolation of one another – the malfunction of a single system can trigger a cascading effect leading to extensive failures, which can have significant economic consequences for a single entity or even an entire nation. For example, telecommunications networks require electricity; industrial systems use sophisticated computer control and information systems; electricity generation requires fuels, and so on. Such interrelations are of different and complex nature [Petit, 2016], which precise identification is

20 <https://botsense.pl> accessed 1 June 2021.

crucial for identifying threats in cyberspace and assessing their impact on the state's security.

Many authors like [Stergiopoulos, 2016] or [Han, 2019] confirm the need for analysing the network of interdependent infrastructures enabling identification of its security-critical components and better understanding the scale and scope of potential threats. Such an approach allows early identification of the threat propagation early and disseminates the warnings for pre-emptive actions to mitigate the related risk. However, effective threat response requires establishing procedures, a cooperation framework for reporting threat incidents and coordinating entities' activities, as presented by [Settanni, 2017], [Puuska, 2016] or [Turoff, 2016]. It enables a safe and reliable online collaboration of the IT security analysis and management teams from all interdependent entities. However, it should be noted that the scope and level of detail of threat information sharing are often limited in practice. It is most often due to fear of compromising the security or vital interests of the party providing the data, which it considers as sensitive information. Therefore it is also desirable to create mechanisms to encourage these entities to cooperate and ensure that their vital interests are protected. These activities should be supported by technical solutions that enable the efficient acquisition, processing, and dissemination of verified information about cybersecurity threats and their potential impacts.

Ensuring global protection against computer threats is possible not only by preventing unauthorised access to systems or protection against malicious software. In addition, new functions need to be built to detect cyber events early, assess potential threats and their propagation within interconnected infrastructure with an assessment of associated negative consequences, and implement appropriate preventive countermeasures. Thus, achieving a global and reliable situational awareness picture in the cyberspace of interconnected networks and systems is the basis for effective response to ongoing and potential threats.

Recently, many efforts and case studies have been undertaken internationally and nationally to achieve a global situational awareness to improve the reliability and continuity of systems and services essential to safety and broadly understood the state's economic interests. They are mainly stimulated by the NIS Directive [NIS, 2016] or national strategies for the security of networks and information systems. In addition, some stimulating approaches to improve an organisation's ongoing awareness of the risk posed to its business by cybersecurity attacks have been developed within

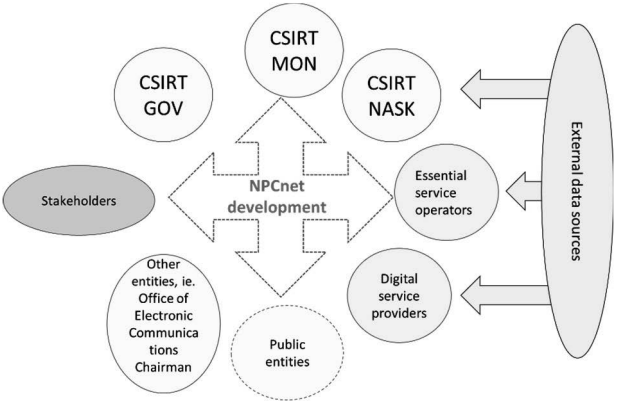
European Union research projects like CS-AWARE[21] or PROTECTIVE[22]. The first one focuses on creating solutions dedicated to the local public, providing tools for automatic detection, classification, and visualisation of computer incidents in near-real-time. The latter enables raising cyber situational awareness by enhancing security alert correlation and prioritisation, linking the relevance of an organisation's assets to its business.

In Poland, the National Cybersecurity System (NCS) [NCS, 2018] imposes, among others, on the cabinet minister the responsibility to develop and maintain the global cybersecurity awareness system supporting cooperation of all the national cybersecurity system entities. The prototype of such a system has been developed within the research project entitled "National Platform for Cybersecurity" (NPC) carried out within the framework of the CybeSecIdent Program on "Cybersecurity and e-Identity", supported by the National Centre for Research and Development. After extensive tests and several extensions, the system was entered to force in January 2021 under the S46 name. The system integrates components of the national cybersecurity system (Fig. 2), including three Cybersecurity Incidents Response Teams (CSIRT), essential and digital service providers, public entities and stakeholders exchanging information over the dedicated NPC secure network.

The S46 contains the mechanisms for integrating the security management systems used by various institutions and companies and aggregation of a distributed knowledge from numerous databases. In addition, it delivers procedural and technical mechanisms to ensure secure sharing and dissemination of information about events that could adversely affect cybersecurity. The exchange of data is carried out within the following basic functional processes, i.e., surveying the system's entities, handling incident reports, building global cybersecurity awareness and risk assessment at the national and company level, exchanging information on security events, warning on threats and risk, knowledge sharing, exchange of information on vulnerabilities and issuing recommendations.

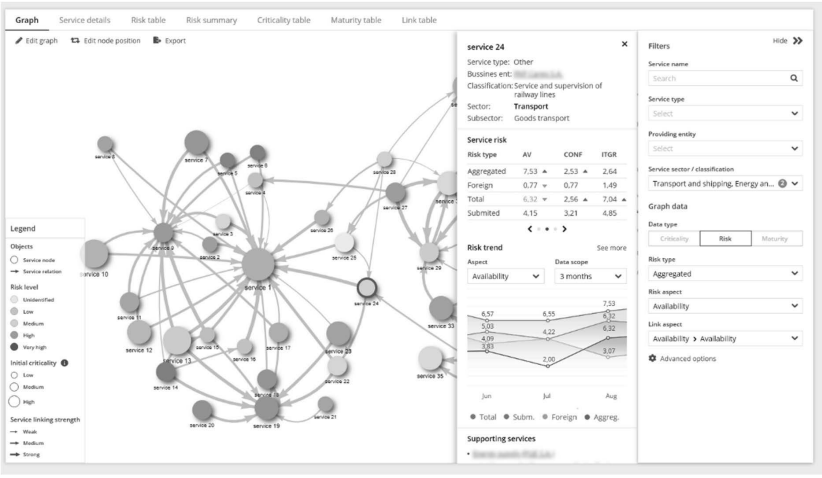
21 <https://cs-aware.eu> accessed 1 June 2021.
22 <https://protective-h2020.eu> accessed 1 June 2021.

Fig. 2. S46 ecosystem



Achieving consistent and trustworthy cybersecurity awareness at the national level requires that all S46 users apply a uniform approach to cyber threat assessment. Therefore, the S46 applies a dedicated risk assessment methodology. It covers the users' dynamic risk assessment procedure and the static and dynamic risk analysis procedures carried out by the CSIRTs [Janiszewski, 2019]. The risk assessment results performed at CSIRTs (Fig. 3) are visualised on a network of interdependent services depicted in [Kamola, 2019]. The colours of the nodes correspond to the current risk values for the services. The width of the edges reflects the strength of the impact of a given service. By clicking on the selected node, one can get more detailed information. The panel to the right in Fig. 3 shows details of the selected service (indicated by the blue border), including the risk value and its trend.

Fig. 3. The visualisation of risk assessment



By correlating the results of analyses conducted by CSIRTs appropriately, it is possible to create a global picture of cybersecurity awareness. Elements of the global situational awareness picture are shared with S46 users, enabling them to obtain the necessary data to react promptly when threat symptoms appear in cyberspace and select appropriate measures to eliminate or reduce their impact.

Lessons learned from the implementation of S46 confirm that creating and understanding real cybersecurity awareness depends on the ability of all actors involved to effectively detect and effectively respond to cyber threats and their willingness to share cyber threat information. The presented solution offers effective mechanisms ensuring the expected level of trust of the system's users in external relations. It delivers tools for strengthening the users' collaboration, supports secure sharing of the threat data and building a shared cybersecurity awareness picture. All these lead to better understanding the threats and risks and increasing the protection against significant damage to the state's security, public order, and economic interests.

6. Conformity assessment and certification

Cybersecurity is of undeniable impact to all branches of industry, each public administration level and – as well – citizens. Combined with geopolitical interest, it has become an inherent part of legislative initiatives, formal and informal (status quo) regulations, industry-specific or sector-wise private and public standards and – last but not least – the vital aspect of supply chain characteristics. Be it private funding or public spending; no other security-related parameter has more impact on procurement decisions.

The pillar of trust and the basis of choice is the recommendation of an authority we trust. The problem to define the authority and set-up a well-programmed qualification system is well known. The recitals of Cybersecurity Act (European regulation) state: "A European cybersecurity certification framework is established to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity." In technology, quality control, technical supervision, attestation or calibration mechanisms are widely used. We are not surprised that a weighing scale measures correctly and perfectly in line with another unit; to observe the attestation mark on facilities and devices such as fire extinguishers or elevators.

On the contrary, we intuitively and subconsciously know a systematic solution behind this predictable way of working. Rightly so, weighting scales are subject to calibration and elevators to inspection and periodic control. These are the elements of the "conformity assessment systems" as well as "market surveillance" that stand behind and ensure the quality (efficiency, performance, accuracy) of the equipment and services available on the market.

Preparing, setting, and introducing a similar systematic approach for cybersecurity has become a vital challenge to the market. Complaints about the below-expectations performance or unpredictable behaviour of IT equipment like computers or smartphones are common. Misbehaviour of such kind provokes the observation – it is possible that a device used hundred times daily (phone) and for most working hours of a week (computer) is not subjected to any systematic and regular control or tests. Furthermore, at the same time, we entrust these devices with personal data, sensitive information, financial transactions, professional and private secrets. On the contrary, devices responsible for the safety of the work and life environment (like fire extinguishers) are not likely to be used and are subject to check procedure at least once a year. What makes things even worse, a common approach has been developed to answer the persistent

requests of antivirus software to run scheduled scans and operating system prompts for updates by choosing the "postpone" action. The above-described context of conformity assessment for cybersecurity is a combination of rules for development, acquisition, deployment and safe (secure) usage. Setting up a unified approach that would encompass and enforce all these rules is not an easy task.

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cyber-Security Agency) and on ICT cybersecurity certification, concerning the European Cybersecurity Certification Framework (The European Cybersecurity Act) provides for the creation of certification schemes at different levels of trust justification (national and European).

Currently, there is no functioning common certification scheme in cybersecurity evaluation in the European area. The European Commission developed the first draft program based on the ENISA document and the SOG-IS[23] input. It will be a certification scheme based on the Common Criteria standard. The subsequent schemes that can be expected to appear will be dedicated to cryptography, 5G technology, cloud solutions and the Internet-of-Things. The security of 5G networks is one of the most important issues being considered globally, in Europe and nationally (COMMISSION RECOMMENDATION (EU) 2019/534 of 26 March 2019, Cybersecurity of 5G networks)[24]. Furthermore, the European Commission encourages EU member states to give high priority to the issue of cooperation to certify 5G devices and networks (Press Release /19/4266, 19.07.2019).

[ECSO, 2020] "Certification scheme as defined in the EU Cybersecurity Act provides a framework within which a sound certification ecosystem can be organised. A European certification scheme is made of security requirements, a corresponding evaluation methodology and governance rules. The Cybersecurity Act suggests considering and referring to two main sources: (1) European, international and industry standards that define evaluation methodologies for a given vertical or context. (2) 'Security Profiles' that could be defined within a scheme or standard, and define precise requirements tailored for a given use case, product category, or vertical."

---

23 SOG-IS - Senior Officials Group Information Systems Security, <https://www.sogis.eu> accessed 1 June 2021.

24 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019H0534> accessed 1 June 2021.

A certificate confirms that the product, or sometimes only the product's design or its manufacturing process, is compliant with specific requirements. Verification of compliance with requirements established by standards is a common procedure. Note that neither in Poland nor Europe is normalisation obligatory. That means that both creating standards and applying them are voluntary [IK-GEOPOL, 2020]. Nevertheless, "standardisation translates directly and indirectly into the offered IT products as it may significantly influence the selection of technologies or manufacturing techniques. This influence is caused by the market pressure that treats compliance with standards as a quality indicator and a method of verification whether the product will be successfully launched and put into use. That is where the issue of conformity assessment appears" [IK-GEOPOL, 2020].

It should be remembered and understood that certification is one of the elements (stages) of a working conformity assessment system. Certainly an important one, often crucial for the manufacturer (when required for entering the domestic market or sale in a particular branch). Let us remember that issuing a certificate (attestation decision) without implementing control mechanisms that enforce continuant compliance with requirements will not guarantee the quality for the end-user (stability of features). That requires "mechanisms to demonstrate continued compliance with the specified cybersecurity requirements" – as required by Article 54 of [CSA, 2019]. In reality, the regular and systematic inspection regime applies to the most extent to industrial machinery and equipment. Operational quality (accuracy) is not given for an indefinite period. Due to the ageing of mechanical and electronic components, changes in the operating environment and ambient conditions, the performance and quality is constantly changing, usually for the worse. For this reason, the obligation of constant technical supervision, monitoring of parameters, quality control is being introduced.

On the European level, the above-mentioned systematic and unified approach that applies to the cybersecurity of devices intended for the general market (individual consumers) is at very early stages. At the same time, we observe a strong need to implement fail-safe mechanisms ("framework") that would lead the development of IT solutions towards building secure-by-design solutions. Several mature initiatives that support this line of thinking are worth mentioning:

– Microsoft's concept called Microsoft Security Development Lifecycle has been developed since 2004 as an integral part of the entire software development process. M-SDL is promoted among developers, partners,

and customers of the company, who are encouraged to apply the principles of SDL in the development process and incorporate the best practices described in the Operational Security Assurance (OSA) approach. Microsoft's strategy of "embedding" the approach of the SDL software development strategy benefits with the significant share of certificate products in the portfolio, including core technologies like operating system and database engine[25]

- Safecode[26] initiative, which makes available several influential publications offering software security guidance, led by its flagship paper "Fundamentals of Secure Software Development",
- The white paper [NIST-SSDF, 2020] introduces a software development framework (SSDF), a mine of knowledge on mature practices on secure software development.

IT products are assessed and certified in Europe (and other countries) against requirements of Common Criteria standard (also ISO/IEC 15408). Thanks to the international agreements SOG-IS (Europe) and CCRA (world) signed by NASK, Poland joined the group that recognises certificates based on this standard. Poland is willing to elevate the certification potential; thus, a certifying authority (NASK[27]) was established to evaluate IT products for compliance with the Common Criteria standard.

7. Future perspectives and open issues

Cybersecurity is of strategic importance to countries' security and involves protecting critical sectors of the economy, citizens and businesses – this requires constant development and advancements. It is an ever-evolving industry, a permanent arms race. The malware developers attack, and the defence counters with better anti-attack technology. It is an often repeated pattern.

There is a consensus among network security experts that effective detection of network attacks requires collecting and processing as much data containing malware samples as possible. Due to the complexity and number of analysed data, developing advanced algorithms and building efficient computer systems to support the analysis process is necessary. Statistical methods, numerical analysis, data mining, machine learning, risk

25 <https://www.commoncriteriaportal.org/products> accessed 1 June 2021.
26 <https://safecode.org> accessed 1 June 2021.
27 <https://en.nask.pl/eng/activities/certification> accessed 1 June 2021.

analysis, signal processing, decision and control theory are widely used. Deep learning combined with big data processing and new computing paradigms (cloud, fog, edge, dust computing) can be expected to dominate in the near future. These techniques can be successfully used to correlate a broad range of security contexts and knowledge mining to create cyber threats intelligence in anticipation of cyberattacks.

Every year more and more devices are connected to the Internet, the number and complexity of cyber threats will also increase. The internet community is growing, the age of people connecting to the global web is decreasing. It raises enormous social risks. The global network, allowing knowledge and experience to be shared on an unprecedented scale, accelerates innovation and development, increases social inequalities, undermines economic stability, and poses severe threats to entire societies and individuals. Ensuring cybersecurity is and will be a huge challenge for governments, social organisations, education. The critical tasks to be tackled include:

- raising public awareness of online threats,
- adopting legislation to the changing reality,
- international cooperation of government representatives and commercial companies,
- investment in research and exchange of knowledge and experience.

It is not the aim to control the Internet - attempts to control such a dispersed system are somewhat doomed to failure. The objective is to limit the threats to which users of the global network will be exposed.