The Kosciuszko Institute

CYBERSEC
EUROPEAN CYBERSECURITY FORUM

REPORT PARTNER

Microsoft

PATRONAGE

RCB
Rządowe Centrum Bezpieczeństwa

COUNTRY'S SYSTEMIC RESILIENCE IN THE DIGITAL ERA

IZABELA ALBRYCHT, ŁUKASZ GAWRON, MACIEJ GÓRA, MICHAŁ HAMPEL, PhD, MICHAŁ KRAWCZYK, SŁAWOMIR ŁAZAREK, KRZYSZTOF MALESA, PhD, WITOLD SKOMRA, PhD, ENG.
EDITOR: IZABELA ALBRYCHT

REPORT PARTNER

PATRONAGE

A COUNTRY'S SYSTEMIC RESILIENCE IN THE DIGITAL ERA

IZABELA ALBRYCHT, ŁUKASZ GAWRON,
MACIEJ GÓRA, MICHAŁ HAMPEL, PhD, MICHAŁ KRAWCZYK,
SŁAWOMIR ŁAZAREK, KRZYSZTOF MALESA, PhD,
WITOLD SKOMRA, PhD, ENG
EDITOR: IZABELA ALBRYCHT

AUTHORS:

Izabela Albrycht
Introduction

Krzysztof Malesa, PhD
Foreword by the Report's Partner

Izabela Albrycht
State Resilience

Michał Krawczyk
Societal Resilience

Izabela Albrycht, Łukasz Gawron, Maciej Góra, Michał Hampel, PhD, Sławomir Łazarek
NATO's Seven Baseline Resilience Requirements

Witold Skomra, PhD, Eng
State resilience: the way forward

Editor: Izabela Albrycht
Copy-editor: Adam Ladziński
Layout and DTP: Wiktoria Konieczniak

PARTNERS

CYBERSEC EUROPEAN CYBERSECURITY FORUM

Microsoft

PATRONAGE

RCB Rządowe Centrum Bezpieczeństwa

THE KOSCIUSZKO INSTITUTE

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

Introduction 6

Foreword by the Report's Partner 8

State Resilience 9

Societal Resilience 15

NATO's Seven Baseline Resilience Requirements 23

State resilience: the way forward 42

Summary 43

INTRODUCTION

Izabela Albrycht

The history of humankind is interspersed with cyclically recurrent wars, calamities and cataclysms. Some of them are unavoidable, but some stem from decisions, neglect, or ignoring pessimistic scenarios. This often results from psychological reasons, from the traits human nature displays – we wish to live and behave as if nothing sinister was allowed to happen and impact our existence for the worse. The likelihood and unavoidability of similar events is set not only to persist but, realistically speaking, to substantially increase. The present decade of the 21st century, as are the decades to come, is marked by a particularly complex pattern of criss-crossing threats – military, economic, environmental, social – and by a further growth of relatively new domain bound to generate not only civilisational progress but also emerging security challenges – namely space and cyberspace. Hence, the responsibility to prevent these catastrophes or at least properly prepare for them rests with the decision-makers. The big comeback of strategic competition among the states, all-encompassing digital transition, supply chain disruptions and climate changes result in multidimensional and multiplied challenges both above and below the threshold of war appearing and demanding a strategic approach to building systemic resilience. Governments and state institutions have to develop resilience strategies, pursue them in an even more coordinated way, enlisting the cooperation of numerous entities, and stimulate the creation of indispensable resources and solutions. Building systemic resilience requires the whole society, administration and economy to be involved and the cooperation framework across many dimensions to be set up: civil, military, national, international, political, organisational, and technological. In the era of vibrant digital transformation, the last element – technology – is crucial as it may help achieve the primary goal, even if it can at the same time be the origin of unknown threats, thus requiring relevant preventive measures as well.

As the third decade of the 21st century dawns, resilience building is now recognised as a strategic approach to security enhancement, as is demonstrated by the activities both NATO and the European Union or individual countries engage in. These are designed to build resilience in both the physical and the digital layer. **State resilience** is strengthened more and more often with the use of digital technologies, which make it possible to effectively respond to crisis situations (aka **digital resilience**), and with **cyber-resilience**, which can answer the cyberspace-originating threats. A particular component is **societal resilience**, a significant dimension of security, in whose case likewise two aspects can be mentioned. The first is the disinformation resilience, accompanying cyberattacks and cyberthreats, including hybrid threats; the second represents competence growth and enhancement in the field of shared cyberspace use, which needs hardwiring the knowledge on digital technology usage and digital hygiene into our "digital DNA", but also developing the digital competences for the future that allow the state to build up its competitive stance in the digital economy and security over a longer period. Differently put, **resilience is set to impact states' geopolitical and geoeconomics rankings.**

That is why every country is facing a major challenge in this regard. In Poland, significant political backing for strengthening the resilience "of the state and its society to contemporary threats"[1] was announced in the National Security Strategy of the Republic of Poland, endorsed on 12 May 2020 by the President of the Republic. It points to the need to develop "the resilience" and the "defence abilities of Poland" at the same time as two components of the larger whole that is the security system. The document also notes that "comprehensive resilience of the state to non-military and military threats", including hybrid threats, requires the commitment of many entities, such as "state and local government institutions, education and higher education entities, local communities, economic entities, non-governmental organisations and citizens".[2] The strategy stresses the compelling need to build resilience against cyberthreats as well, including effectively countering, combatting, and responding to them through raising the level of "resilience in the public and private, as well as in the military and civilian information systems"[3].

The layers and dimensions of systemic resilience just listed intertwine and prime one other, hence they are worth having a comprehensive analysis, while the only correct approach in state resilience-boosting efforts is the whole-of-society approach.

FOREWORD BY THE REPORT'S PARTNER

Krzysztof Malesa, PhD

Resilience building is a long-term process that requires large-scale efforts and outlays, but is also plausibly the sole non-military way of repelling hybrid activities which are now a constant in the geopolitical landscape of NATO's north-eastern flank. The importance of resilience is writ large in Article Three of the North Atlantic Treaty, given prominence in the resilience-building declaration accepted in 2016 at Warsaw NATO Summit, and renewed in 2021 at the Brussels Summit. Resilience – remaining each member state's responsibility – is a key element that enables allied policy of deterrence and the mechanism of collective defence to be pursued.

Resilience building in a member state is not tantamount to armament. Quite the opposite, it's the domain of civil administration: a cross-sectional and cross-departmental task that demands coordination at the Council of Ministers level. This task is also bound to engage private entities, especially the operators of essential infrastructure.

In this field, cooperation with the private sector, often representing large international corporates, requires that the administration understands business specificity and reaches a certain level of tech maturity. Resilience strengthening in this day and age must by bolstered by digital technology.

The experiences delineated in the report provide evidence that in each of seven resilience areas as defined by NATO there is place for cloud computing, machine learning, or artificial intelligence technologies. The case studies included in the text prove how much these solutions can aid our efforts to build resilience, but they also show the proper place of technology in the management processes: it should support well-devised organisational solutions carried out by well-trained, fully knowledgeable people. These organisational solutions should in current turbulent times be the outcomes of daring, forward-looking decisions of a political nature but not only, decisions which brook no delay. Let's shore up Poland's resilience while the time allows.

1. STATE RESILIENCE

Izabela Albrycht

1.1 NATO standpoint

Building systemic resilience is one of the priorities for all NATO member states, derived from the Article 3 of its founding pact,[4] and reaffirmed with the pledge to boost resilience, agreed upon during the 2016 NATO summit in Warsaw. Resilience is first and foremost the individual duty of each ally, which needs to be strong enough and able to adjust to and deal with a whole range of crises which that the alliance can face. The sum of allies' resiliences is the shared resilience of NATO, while a single ally's lack of resilience means weakness for the whole alliance. A resilient state is less attractive as a target and thus contributes to the overall collective security for the alliance. The group's resilience, including the civil preparedness of allied states, is therefore a main goal of the NATO policy and actions.

Underscoring the importance of resilience is more and more common and stems from the changing nature of threats in the new geopolitical balance of power, as in many aspects the shapes they take are not only military but increasingly also hybrid, terrorist, or cyber. Civil preparedness, that is "supporting allied armed forces by means of civil resources and civil infrastructure in peacetime, crisis, and wartime",[5] serves three basic functions: ensures government continuity, the continuity of essential services for the population, and the civil backing for military operations. At NATO's Warsaw Summit, these three central functions were developed into seven basic resilience requirements, to be discussed in detail in Chapter 3. Generally, NATO policy on resilience and civil preparedness is governed by the Resilience Committee, which answers directly to the North Atlantic Council, NATO's main decision-making body, which highlights how significant this element of allies' cooperation is.[6]

How NATO defines "resilience"

Resilience is a society's ability to resist and easily and quickly recover to normal operation after a major shocks such as a natural disaster or armed attack. Resilience combines civil preparedness and military capacity, whose development is each member state's commitment. [7]

The June 2021 Brussels Summit stressed the importance of resilience yet again, more precisely of increasing it. The declaration affirms that, despite resilience continuing to be the duty of individual countries, to follow a more integrated and better coordinated approach across NATO is a must in accordance with the treaty obligation to reduce the vulnerability to threats and ensure allied armed forces have a chance to operate effectively, be it in peacetime, in crisis, or in wartime. It was declared that allies would draw up a proposal to establish, assess, review and monitor resilience objectives to guide nationally-devel-

oped resilience goals and implementation plans to attain them[8]. It was underscored that every ally would be at liberty to determine how to decide and pursue national resilience targets and plans to attain them, so that they would conform to a given country's – in some cases the EU's – competences, structures, processes, and obligations.[9] In the declaration, an additional turn of events serving as an acid test for NATO resilience was also underscored, namely the COVID-19 pandemic.

The NATO Madrid Summit of 2022 and the declaration issued therein confirmed the previous importance of resilience as both allied states' duty and a common like-minded countries' obligation at the same time, one that should be strengthened by pursuing the targets developed at the country level and implementation plans set up jointly within the alliance. NATO pledged to accelerate its adaptation in the face of security challenges across all domains, for military and non-military threats, boosting the cyber and hybrid threat resilience and enhancing interoperability.[10] Adopted at the Madrid Summit, the new Strategic Concept for the Alliance defines the role of resilience and its importance for collective defence and security in a similar way, as it stresses that ensuring resilience is vital for all essential tasks the alliance performs, especially since it is regularly tested by its strategic rivals and necessary in view of Russian *aggressive actions*. Resilience also forms a foundation for protecting allies, societies, and shared values.[11] What should be stressed is that resilience building is correlated in the document with the necessity to build the Alliance's tech advantage.[12] NATO highlights the need to cooperate in resilience building with the European Union as an area of common interest, but it also points out the need for cooperation between civilian and military entities. A notable novelty is the unequivocal statement that climate changes and their impact on security generate risks for resilience and civil preparedness. This was given even more prominence in the Climate Change and Security Impact Assessment, published during the Madrid Summit, where it is stated that it remains "imperative for NATO and Allies to continue strengthening national and international resilience, taking into account the impact of climate change."[13]

1.2 European Union standpoint

The Commission has taken note of the strategic importance for resilience in 2020 in its Strategic Foresight Report, regarding the need to strengthen it as a new inspiring direction in the EU policy decision-making process[14] for EU leaders that must follow from combining strategic foresight and adequate political response given to foreseeable changes and challenges as well as unpredictable events. Resilience building is a constant process of developing capacities which can help address vulnerabilities in the system and uphold the continuity of state functioning and public policy goals being pursued when facing the challenges related to social and economic transformation. Understood as a response to challenges and crises, resilience must be practiced in a sustainable, fair and democratic way, all the while following a broad, multidisciplinary approach, or a "360-degree outlook".[15]

How the European Commission defines "resilience"

The ability not only to withstand and cope with challenges but also to undergo transitions, in a sustainable, fair, and democratic manner.

In December 2021, the EC presented resilience dashboard that had been created in cooperation with the member states to perfect a tool for comprehensive evaluation of the EU and its members' resilience. They gauge the strengths and weaknesses in each of four dimensions: socio-economic, green, digital, and geopolitical. One instrument to strengthen resilience is to create a dedicated Recovery and Resilience Facility, an assistance fund within the NextGenerationEU programme, aiming to spur reforms and investment that serve further transformation of economies and societies. The dashboards will also help monitor the progress of RFF-enabled resilience strengthening. At least 20% of National Recovery Plan spending ought to be directed to supporting the digital transformation.[16] In the European Commission's opinion, digital solutions can bolster not only the recovery of economies bruised by the COVID-19 pandemic,[17] but also the social and economic resilience of the EU states ahead of possible upcoming crisis situations and upheavals. That is why RRF-related projects will also focus on digital initiatives. What emerges from analysing the RRF plans for individual members states is that many of them intend to invest in the rollout and build-up of broadband networks, the digitalisation of public administration with an emphasis on interoperability and the once-only principle, ongoing digitalisation for businesses aiming to improve production processes, and in the growth of digital literacy and transition of education systems so that they are able to rise up to the challenges the future will bring.[18] The path to achieving resilience also leads through the investments geared towards developing cutting-edge digital technologies, including artificial intelligence or blockchain.[19]

1.3 Cyber-resilience

In the transformative processes stemming from accelerated digital transition and abrupt geopolitical changes, cybersecurity and cyberdefence play a major role. Following years of their growing in importance, as the war in Ukraine broke out, they have definitely been classified as strategic challenges for the state and considered a building block of national security. We had already noticed a strong upsurge in cyberattacks after the start of the COVID-19 pandemic, since the number of people who had to start remote work and education skyrocketed along with the first lockdowns. Overnight, hundreds of millions of people all over the world switched from company-provided security sys-

tems to private networks or devices, predominantly with poor security features, and began using them for work purposes. At the same time, a range of businesses and institutions went through a sped-up digital transition process, deploying project management systems or cloud services. According to a Deloitte report,[20] a year on since the pandemic had broken out what saw a dynamic increase was the number of smartphones and computers connected to the internet infrastructure which lets billions of people stay in touch, use healthcare services, shop online. What also grew was the interest in devices for entertainment and sports, such as gaming consoles, multimedia streaming tools, smart TVs, and smartwatches. Owing to the cyberspace being filled with a larger amount of digital components, the "surface" which cyberattacks can access has widened, and the cyber-resilience challenge has heightened.

Cyber-resilience is also a major facet of security and defence, since offensive activities in cyberspace grew to be a vital component of modern-day warfare, as the Russian war against Ukraine has decisively proved. And because cyberwarfare covers operations conducted both online and with the use of networks and with physical infrastructure as the target, cyber-resilience refers not only to networks and ICT systems but also to the majority of physical objects in terms of their security. Hence, resilience in the globalised but also more confrontational and complex world will remain a never-ending issue for EU and NATO countries, requiring constant adjustments as new challenges come up and inadequate security measures are revealed, while also demanding cooperation and coordinated action that respond to the traits of digital challenges, marked by their cross-border nature. The goal of cyber-resilience has become not only to ensure operational continuity in the digital world, but also to prepare states, institutions, companies, organisations for unusual, unforeseeable events and threats emerging from cyberspace, in the times of crisis as well.

Under the circumstances, countries shore up their cybersecurity by way of building up cyber-resilience, which appears to be a 2022 key word. Such resilience necessitates the effort of joint preparation for digital threats, relevant and effective response to them, and dealing with their aftermath.

Cyber-resilience should be understood as a capability that a given enterprise possesses to manage a cyberattack and its effects in a way which retains the operational capacity. Included in it are such elements as information security, IT and OT infrastructure, business processes, and organisational continuity.[21]

A structure is deemed resilient to cyberthreats when it can adjust to known and unknown threats, challenges, and risks, meaning cyberoperations and incidents we grapple with currently as well as what due to the continual evolution of technology is likely to come up in the coming years. Thus, cyber-resilience building is and shall remain a long-term process which depending on the circumstances – resulting from the volatile nature of cyberspace and cyberthreats – is going to be modified to fit the needs and challenges. As cyberspace gets more and more saturated with subsequent technologies and billions of networked devices, the objective remains to fill it up with as many secure components as possible and to build the organisational capacities. What should be widely agreed is that cyber-resilience needs to characterise the whole digital ecosystem; that is, it needs to be deployed across all sectors and with the whole chain of interlinked parts (network, software, hardware, apps) and dimensions (administration, industry, local governments and the like) in mind. That is why global agreements for peaceful use of cyberspace were attempted, although in the current geopolitical climate signing them seems impossible. Thus, political support is necessary for regulations which boost further cybersecurity building and influence business and company operations in the EU and the transatlantic area. These ambitions can clearly be seen on the EU's side through the accelerated work over another iteration of the Network and Information Systems Directive (NIS2) or the draft Cyber Resilience Act expected in the Q3 2022. On 13 May 2022, the European Council and Parliament came to an agreement on accelerating the work on the provisions for "high common level of cybersecurity across the Union", whose task is to further increase the resilience and responsiveness of public and private sectors as well as the EU as a whole".[22] The initiative includes the decision-making process in terms of the NIS directive just mentioned as well as the Directive on the Resilience of Critical Entities with regard to its physical enhancement. The functioning of these entities can be disrupted in the wake of natural disasters, terrorism, or hybrid attacks, while the public services and internal market depend on them. The EU Digital Operational Resilience Act (DORA) is also in the legislative process, a regulation set to increase the information security of the financial sector – banks, insurers, investment businesses – through maintaining the operational security. In the digital realm, in turn, the Cyber Resilience Act is slated to help build up the security in the broadest terms, its aim being to saturate "European" cyberspace with more secure devices and solutions, less vulnerable to attacks, sabotage, or deliberate action. The Commission will thus propose "introducing common cybersecurity rules for manufacturers and vendors of tangible and intangible digital products and ancillary services".[23]

The political impulse to strengthen cyber-resilience was sent out in the 2020 EU Cybersecurity Strategy, where it was considered to be among the main areas of interest and a key goal of action. The document states that, thanks to pursuing the strategy, Europe's group resilience against cyberthreats will be reinforced, while every citizen and business will be able to use trustworthy and reliable digital services

and tools[24]. This approach is likewise visible at the member states' level. For instance in the Cybersecurity Strategy of the Republic of Poland for 2019–2024. The Strategy outlines the measures aimed to enhance cyberthreat resilience across information systems, operators of essential services and critical infrastructure, digital service providers, and the public administration[25].

As a consequence of this policy directed at cyber-resilience strengthening, it should be expected that EU countries will conduct an in-depth analysis of their whole IT ecosystem as to its security – the technology stack, meaning what comprises it in terms of hardware, software, but also service providers and human resources, and so across the supply chain and following the "know your supplier" policy. Such actions should be taken at the company level but also states and international organisations. For EU, and more broadly transatlantic, cyber-resilience building process, it is also paramount to jointly develop norms, certify products and services in terms of their cybersecurity, and back the initiatives aiming to increase software security. More effort should also be devoted to building a strong standing of domestic cybersecurity sectors in the global value and supply chains of products and services for the security of networks and ICT systems, thus involving the emerging and disruptive technologies (EDT) which impact the progress of cybertechnology, innovation in the economy, and defence capability. The European Commission strive to influence the market in this regard as well, for instance unveiling a proposal for joint action which the Commission suggest the members states could carry out in the next few years – the idea was described in the roadmap on critical technologies for security and defence,[26] now in the consultation process. Notably, technology development through innovation demands cybersecurity and cyber-resilience assessment, too, which is an investment in safeguarding the states and economies in the long term.

Operationally, what is needed is a more proactive security policy, one intended to strengthen public-private cooperation and to involve companies not only more deeply, but also in a more institutionalised way in building a cybersecurity system within both the EU and NATO. This is not only about implementing the initiatives such as Shields Up from the US, expected to mobilise companies and help them increase their cybersecurity levels, but also about being open in terms of setting up real public-private partnerships encompassing, in the first instance, cyberthreat intelligence sharing, threat hunting, better sectoral coordination on information sharing, deepening this cooperation and making it permanent, for example by creating a network of sectoral CERTs, cooperating in building SOCs (Security Operation Centres), or implementing bug bounties. There are examples of existing partnerships: Microsoft's Government Security Program or the Polish government's programme for cybersecurity cooperation (PWCyber). In turn, it was decided at the NATO Madrid Summit to create a "virtual rapid response capacity in cyberspace" based on the resources of national allies and to further cement the ties with the private sector.

2. SOCIETAL RESILIENCE

Michał Krawczyk

2.1 Societal resilience to disinformation

Disinformation is part and parcel of contemporary wars, conflicts, and rivalries, thus societal resilience is an important element of state security. The COVID-19 pandemic and Russia's invasion on Ukraine have multiplied the threats coming from the information space. Although disinformation has been a tool for policy and military action for many decades, recent years have made the growing problem of information disruption plain to see, especially the disruptive news related to digital information spaces. The consequence is a number of challenges related to countering disinformation and strategic communication. To respond to them, many new solutions and initiatives presented by governments, civil society, experts, academics, and commercial organisations have emerged. These activities range from new strategic communication solutions, such as in the context of providing vaccine information, to legislative and technological initiatives to combat disinformation. Quite a few of these initiatives are ad hoc and focus on countering a single type of threats or are limited to a specific area, defined by the target group for disinformation, the type of disinformation, or the platform through which it is spread. Importantly, the problem of disinformation goes beyond international rivalries and conflicts. Indeed, it can affect the lives of ordinary people, as exemplified especially by the COVID-19 pandemic and the associated infodemic, an unprecedented wave of fake news. In such a context, disinformation can directly affect people's health and, in extreme cases, even become life-threatening. This is why the involvement and intervention of public and international institutions and others is so significant.

The level of complexity and the breadth of the issue of disinformation and related threats means that its prevention must involve a very wide range of activities, carried out by different institutions and organisations. Therefore, a key issue in this context is building societal resilience to disinformation.

This process should be understood as collaborative, comprehensive efforts to understand the problem of disinformation, counter it, mitigate its negative effects, and educate, targeting whole of society and developed by public institutions, civil society, academia, and the private sector.

Social resilience, to be effective, must exist simultaneously at the state and society-wide level. This issue has been recognised by such bodies as national governments, NATO and the EU,

which have underscored the importance of the problem and the desire to counteract it with their actions. In the so-called Reflection Group report for NATO we can read: "NATO populations expect to be protected against new threats such as cyber and disinformation and expect their governments, supported by NATO, to develop tools for attribution and deterrence. Resilience must reside within societies as well as the state."[27]

2.2 EU activities for societal resilience

The EU appears to be a key actor in the context of combating disinformation, as its influence, derived from its position on the international stage and its economic power, allows the Union to deeply impact the private and public sectors. Each of the main EU bodies, i.e. the European Parliament, the European Commission, the European Council, and the Council of the European Union, participates in this process, targeting member states, the private and third sectors and EU citizens. In addition to them, the High Representative for Foreign Affairs and Security Policy, together with the EU Intelligence and Situation Centre (INTCEN) and its strategic communication cells, notably the East StratCom Task Force, also play an active role, as do the Union's hybrid threat actors, the Hybrid Centre of Excellence and the Hybrid Fusion Cell.

Cooperation with and attempted regulation of the private sector serve an important role in the EU's approach to combating disinformation. The EU has recognised tech companies' partial responsibility for disinformation at large, noting that private actors are responsible for the operation of the social media platforms on which disinformation campaigns are created and spread, and that their algorithm-based operation enables the spread of fake news on such a scale. The Union has openly called on the private sector to step up efforts to combat disinformation. An important element of these efforts is the 2018 launch of the EU Code of Practice on Disinformation.[28] It addresses five areas of competence for increasing transparency and accountability in the online media environment. These comprise: increasing the transparency of online advertising and control over advertisers; increasing the transparency of political advertising; intensifying the internal activities of platforms in the area of combating disinformation; promoting reliable information sources; and cooperation with the empowered research community. This was the first self-regulatory act of its kind to be voluntarily adopted by the main tech giants. However, from the outset, the expert community and the EU itself saw the need to revise the Code and insert stricter rules there. This happened in June 2022, when its second version was published.[29] The new version is more detailed (it contains 44 commitments; the 2018 version contained 21) and, according to the European Commission, draws on the experience of the past few years. The main areas the Code addresses are: demonetisation of disinformation, transparency of political advertising, minimising the manipulation methods (proactively fighting fake accounts, bots, deepfakes, etc.); user protection (developing tools to identify and report false content); creation of a pan-European fact-checking network, and allowing researchers to access data. The implementation of the Code, which failed when looking back at the 2018 document, will be overseen and monitored by the announced new transparency centre and a permanent task force.

The European Commission presented – and just as importantly led to the approval of – the Digital Services Act (DSA), a legislative proposal for an act on digital services, regulating their providers.[30] The DSA above all provides a range of tools that can be used to combat disinformation, particularly by placing responsibility for disinformation on platforms. The latter will have to operate in a more transparent manner and, crucially, will possibly be held accountable for failing to meet the guidelines. The DSA is also set to include the introduction of a user's chance to appeal a platform's decision and to see the rationale behind the moderation proceedings in question.[31] Once the European Parliament has adopted the final DSA wording, the act will still need to be ratified by the member states' national parliaments.

The EU also actively supports the activities of the NGO sector, mainly through financial instruments, including a commitment to support fact-checking organisations in particular and to promote media literacy and high-quality journalism.[32] Against that background, SOMA, the international Social Observatory for Disinformation and Social Media Analysis was established in 2018.[33] It has set up three research centres and is developing and promoting a network of organisations that diligently analyse the social media.

Another example of EU cooperation with the third sector is the European Digital Media Observatory (EDMO) network.[34] Through this network and with the European University Institute framework in Florence, the EU has created a pan-European centre with regional centres (set up by actors from different EU countries). The EDMO enables and facilitates the collaboration of fact-checkers, media literacy experts, and researchers to understand and analyse disinformation.

The above EU activities to build systemic and societal resilience to disinformation cover all major impactful elements.

CASE STUDY – UKRAINE

The Russian invasion on Ukraine is not limited to kinetic activities in the military domain, but has also included hostile activities in the cyber and information domains. Russian propaganda and disinformation activities are an important part of Moscow's art of war, while false and distorted information is used as a tool for hostilities below the threshold of war, both against Ukraine and globally. Ukraine has been a target of information war-

fare for at least a decade and, building on this experience, has developed a system of resilience against disinformation over the past years, particularly in terms of cooperation between the public sector and civil society.

Ukrainian efforts in the context of combating Russian disinformation are based on several priority areas: fighting all manifestations of hybrid activities (cyberattacks, disinformation disseminated through the media, politicians' manipulations, the Orthodox Church's propaganda, etc.); a strategic approach focusing not only on refuting Russian lies but also on endorsing Ukraine's own message; and promoting unity via cooperation between the government and civil society. This approach to the disinformation problem dovetails with the notion of building public resilience to disinformation, particularly through the Ukrainian entities' focus on cooperation between the public sector and civil society and the desire to combat all displays of disinformation.

From the very first day of the Russian invasion, Ukrainian resistance also extended to the digital world and information space. A number of technological solutions emerged, introduced by the government, private sector, and NGOs, to build public resilience to disinformation. As part of a joint effort by the Ministry of Culture and Information Policy and the Ministry of Digital Transformation, the Internet Army sprang up, bringing together some 500,000 volunteers (developers, creators, marketers, copywriters) to focus their efforts on, among other things, combating Russian propaganda online.[35] By involving volunteers from the Ukrainian communities, the common awareness of the lies and tactics used by the Kremlin is growing. The previously mentioned proactive approach to waging information warfare against Russia finds a manifestation in the use of digital technologies. Artificial intelligence (AI) is used within the Diia app to search for the social profiles of fallen Russian soldiers from their photos.[36] The profiles thus found are then used to notify the family of the fallen about their death, which has a propaganda effect in Russian society. Strategic communication plays a very important role in this broad picture of Ukraine's activities – reliable broadcasts to the whole society are supported with the Diia TV and Diia Radio applications, which are a source of official and trusted news, making it available even in the absence of a TV or radio signal.[37] The ability to present reliable information even inside the occupied zones is a very important element of disinformation resistance. A chatbot called "Mariupol now status",[38] which operates on the Telegram platform, serves the same purpose. With its help, residents of the occupied city receive up-to-date information on the situation in the city and its districts. With the bot's help, residents can also find out about the status of their relatives who they have been separated from.

As the above examples show, efficient strategic communication and the ability to inform citizens quickly play a key role in the reality of war. Technology and the government's cooperation with other sectors aid in the matter. Only by having reliable information can the citizen be immune to disinformation and propaganda. In the context of information warfare, it is equally important to create one's own narratives, based on truth, in which technology and cooperation also assist, examples being the volunteers from the Internet Army and proactive action towards the Russian public. Only such a mix is able to ensure the resilient public, resisting disinformation, and allow the true picture of the war to reach the people in the rest of the world.

2.3 Technological solutions

Building societal resilience can be supported and potentially accelerated by external measures, including technological solutions. An important element of increasing societal resilience is **fact-checking** – the EU and technology companies highlight its relevance. However, the vast amounts of content and data published at any given moment on social media platforms make effective analysis of much of it impossible. This problem is being addressed by organisations developing technological solutions to **automate some elements of the fact-checking process.** Automation is being applied at most of the stages: from attempts to introduce "live fact-checking" offered by PolitiFact,[39] which analyses videos with politicians' statements and checks the information they provide in real time by automatically comparing it to a fact-check database and displaying the result on screen; to the use of AI and machine learning to automate the analysis of information appearing in news outlets and catching those that are potentially false;[40] to web searches for repeated information that has already been fact-checked.[41] The technologies being developed for fact-checking automation can be an important part of outreach for these activities and thus contribute to developing societal resilience to disinformation. New solutions should be AI-based and address the key challenges faced by fact-checkers, while supporting the daily activities they perform. These can include:

- Searching for statements or claims worth checking.
- Detecting previously verified information.
- Acquisition and collection of evidence.
- Automatic fact-checking.

Such solutions should also include languages other than English, in order to increase the potential of fact-checking globally. The development of open-source software also seems crucial in this respect, available to all willing fact-checkers, offering tools that do not require technical knowledge, but provide effective results and work in real time. Of course, the automation of fact-checking brings a num-

ber of risks and dangers that must be taken into account. These may arise from system bias, lack of sensitivity to the context of the inspected content, and the variety of tools through which disinformation is spread, such as text, video, images, word of mouth, etc. All these must be reflected in the systems now being honed.

The modern information space is increasingly relying on digital technologies and the activities of social media platforms, which are based on AI, big data processing, and process algorithmisation. Disinformation mechanisms are also becoming more sophisticated and are based on **the latest technologies, including AI.** Therefore, the response to these threats should also involve advanced solutions to build a secure and trusted environment. AI technologies need to be included in the tool and service design for media ecosystems, allowing users greater access to reliable information, facilitating its creation and distribution, and countering advanced disinformation mechanisms. The last task can be made substantially easier through the creation of AI-based tools for quantitative analysis, automated web analytics, and doctored and deepfake content recognition. An equally important task is to include AI technologies in the creation of citizen-facing tools aimed to facilitate the navigation of the information space, the identification and recognition of disinformation, and the fight against it. Such solutions should include automated content analysis and tracking, comparison of different information sources, and context-sensitive analysis of the investigated content. AI technology can also play a key role in combating so-called computational propaganda, based on the operation of bots, trolls and other automated ways to manipulate discussions that unfold on social media platforms. Countering it focuses on detecting inauthentic web traffic, so technological solutions may be more effective than trying to automate the assessment of news veracity. Even so, it should be noted that at its current development level, AI technology serves to complement and enhance the effectiveness of humans, who are still a necessary element in the disinformation analysis process.

Automated content analysis, especially in the context of disinformation, is hampered by the particularities of individual languages, the context of the information, the concepts of irony, sarcasm or satire, and the need to take all these into account when analysing the accuracy of a given piece of information. Attempts to automate such activities use the **natural language processing (NLP)** technology. This is a research field that deals with the automation of natural-language analysis, understanding, and translation by computer systems, combining AI and linguistics.[42] Natural language processing is already leveraged to examine fake news and to try to automate the detection of false information and manipulation. Most commonly, such solutions are based on analysing vocabulary patterns, comparing them, and examining statistical correlations between news articles.[43] However, their application has considerable limitations, especially in the context of more sophisticated manipulation tricks based on using half-truths, irony, etc. Thus, resources and opportunities are needed to develop cross-sectoral projects for the use of natural language processing in the context of combating disinformation.

Disinformation is in many cases driven by **algorithms**, yet they can also be used to limit the reach of false and manipulated information. Many technology companies have taken action in this respect, successfully reducing the number of fake news items appearing on user walls.[44] In addition, platforms and technology providers are offering browser extensions and widgets that make access to verified content easier for ordinary users.

Many of the risks associated with online disinformation can be mitigated with the **blockchain** technology. This system uses a decentralised, shared, and unalterable ledger that facilitates information tracking, allows any user to verify the information, and makes it almost impossible to manipulate information that has already been created once. Its potential can be used to combat different types of disinformation, such as deep fakes, and to build transparency into the lifecycle of digital content. It can be applied in tracking and verifying sources and the content itself, e.g. by creating a ledger of reliable images, photos, information, and metadata that are published by a given publisher. A public registry would hinder the possibility of disinformation actors doctoring them. Blockchain can also be used to certify and identify the fact-checking process. The technology offers some potential solutions that could be part of building societal and systemic resilience to disinformation.

Fake-news-recognition capacity building and disinformation awareness-raising requires the development of effective ways to reach school-age people. Here, the so-called **gamification** can help, meaning the use of games and gaming mechanics for education. Its use makes it possible to maintain high engagement, build habits and shape desired behaviours, and create a positive learning environment. In the context of disinformation, the topic is constantly being explored, with new games as well as comic strips and cartoons released to help the youngest learners get to grips with the issue, and, as research shows, this way of teaching actually has the best results.[45] Games such as Get Bad News, in which players take on the role of the creators of fake news to learn the mechanisms behind it,[46] Fake News: The Game, in which players have to distinguish between real and fake news,[47] or Fake It To Make It, which shows how disinformation spreaders use it to make money,[48] are just a small part of currently available games that address the issue of disinformation. However, developing interesting and substantive games requires funding, access to technology and expertise.

2.4 Other areas for building societal resilience

In addition to the technological elements, the need to fund and support other areas of building societal resil-

ience is worth putting in sharp relief. Among the most important topics are:

- Developing media literacy and the critical thinking knowledge and introducing it into the curricula at each stage of public education.
- Conducting public campaigns highlighting the importance of the problem and presenting the mechanisms behind disinformation.
- Promoting cross-sectoral cooperation, including civil society and NGOs in the disinformation-related education and training process.
- Using "pre-bunking", i.e. the promotion of reliable and verified information as a counter to popularising fake news. In this way, the user becomes resilient to manipulation and fake news that they may come across later. This is a kind of "inoculation" against disinformation and is promoted as a counter to tedious and inefficient fact-checking.
- Underwriting cross-sectoral research on disinformation and ways to counter it. This process should involve experts, researchers, academics, the public sector, and the private sector. Research on disinformation requires thinking about different factors: technological, psychological, social, economic, etc. Hence, it is crucial to develop research that includes all of them.
- Developing new technologies with the "human-based approach" hardwired, taking into account human rights, inclusivity, and user security right from the production stage.

Building societal resilience to disinformation is the only way to effectively fight disinformation and related threats. It must involve education, legislative action, private market regulation, business initiatives, the development of new technologies, and the activities of NGOs and expert organisations. The EU has grasped it, in recent years developing activities in each of these areas and cooperating with the above-mentioned sectors and member states. One of the key elements of building societal resilience is to leverage new technologies to develop solutions and implementations that are useful in various areas: education, fact-checking, platform use and management. In all of them, this process has already started, and there are many initiatives related to the use of the latest technologies in this context and implementing the ways to apply them they have been mentioned in this chapter. However, this is only the beginning for the societal resilience building process, which requires further development, funding, and research, not only across new technologies. It is worth noting that confining the fight against disinformation to technological solutions is impossible. These can only complement human action and support individual parts of the broad approach to the problem summed up as societal resilience to disinformation.

3. NATO'S SEVEN BASELINE RESILIENCE REQUIREMENTS

Izabela Albrycht, Łukasz Gawron, Maciej Góra, Michał Hampel, PhD, Sławomir Łazarek

Since the upcoming decade is shaping to be a time when security will become an overarching priority for governments and influence the design of other public policies, first and foremost the resilience goals set by NATO at the Warsaw Summit are worth a look. Heads of states and governments pledged to strengthen resilience,[49] in particular by working towards individual member states meeting the **Seven Baseline Requirements** for resilience.

The NATO Civil Emergency Planning Committee (CEPC) has developed a set of evaluation criteria[50] for each of the seven requirements so as to standardise the methodology for assessing the implementation level of the allied guidelines and the overall resilience of member countries. NATO

The NATO's Seven Baseline Resilience Requirements are*:

1. Assured continuity of government and critical government services (the ability to maintain state decision-making in times of escalating crisis, including political-military crisis).

2. Resilient energy supplies, e.g. contingency plans and backup energy sources (internal/domestic and external/foreign).

3. Ability to deal effectively with uncontrolled movement of people, e.g. capacity to navigate refugee movements so as not to conflict with movements of armed forces.

4. Resilient food and water resources, e.g. ensuring food resources are protected from disruption and sabotage.

5. Ability to handle incidents with mass casualties and disruptive health crises, e.g. ensuring the capacity of the civilian health system to deal with large numbers of casualties, including medical supplies.

6. Assured civil communications systems, e.g. ensuring continuity of operation of communications and telecommunications systems during an emergency, including an adequate stock of back-up supplies.

7. Resilient transport systems, e.g. ensuring freedom of movement for armed forces (including VJTF, or a high-readiness units), disruption-proof information systems to support the functioning of the country's transport system.

* https://www.nato.int/cps/en/natohq/topics_132722.htm [online: 30.06.2022].

CEPC working groups are supporting member countries in developing these guidelines. The aim of the report will be to analyse the use of digital technologies to strengthen resilience in the seven areas and, as a follow-up, to develop takeaways that indicate opportunities to use digital gains to build resilience.

3.1 Assured continuity of government and critical government services

Izabela Albrycht, Maciej Góra

The list of seven baseline requirements that NATO countries have committed to meeting begins with "continuity of government and critical state processes".

Continuity of government is a coordinated effort across the executive, legislative, and judicial branches of government to ensure the management and delivery of core state functions continues before, during, and after an emergency.[51] The issue of ensuring the continuity of state authority and administration is a broad and multidimensional concept. In the United States, the foundations for the continuity of government – ensured by providing Continuity of Operations, Continuity of Government and Continuity of Constitutional Government – are the National Essential Functions, which cover eight issues: preserve the constitutional government, provide visible leadership, defend the country, maintain foreign relations, protect the homeland, provide emergency response and recovery, maintain a stable economy, and ensure the operation of critical government services.[52] The plans that determine the fulfilment of statutory tasks in public administration in times of crisis should be developed, exercised, and reviewed not only centrally but also at local and regional government levels and should be flexible and scalable to respond to threats of different form and scope and at different points of impact. The basis for developing such plans is the identification, analysis, and evaluation of risks and risk resilience assessments **in the dimensions of logistics, finances, human resources, information, time, and quality/effectiveness.**[53]

In order to cope with the multidimensionality of the resilience-building process, one of the most important tools helping to develop crisis management plans are models and simulations that invent scenarios for given risk situations arising and allow them to be tested. In this sense, models are abstract descriptions of objects taking into account their characteristics, while simulations are calculations of their values and visualisation of the results using a computer.[54] The fusion of modelling and simulation reduces the need for manual analysis, allowing different scenarios of situations with varying parameters to be examined and, following their analysis, appropriate action plans to be prepared. Modelling and statistical methodologies are widely used by governments around the world to support the authorities' operational and political decisions in complex environments[55] such as finance, energy, logistics, and transport. An important use case for these technologies in terms of maintaining continuity of government is biological modelling related to virology and disease transmission, which gained prominence during the SARS-CoV-2 epidemic and was used by many countries to create public policies in the midst of the pandemic crisis. The building blocks of modelling and simulation, which allow the appropriate scenarios to be explored, are technologies such as the Internet of Things (IoT), the big data extrapolated from them and the so-called artificial intelligence (AI) algorithms responsible for processing them.

With regard to the determinants of planning and responding to a crisis, the central role of management (understood as a decision-making process, in this case taking place under time pressure) in situations requiring the restoration of government operation continuity becomes clear. Meanwhile, information resources and their collection, processing and restoration capabilities, which should be considered a strategic attribute of security systems and a component of critical infrastructure systems, serve a key role in the management process.[56] Such data should be adequately protected against unauthorised access, theft, modification, and destruction. Therefore, in Poland's National Critical Infrastructure Protection Programme, the minister in charge of digitalisation is responsible for the system that ensures continuity of public administration operations (just as for the communication system and information and communication network system).[57] Cybersecurity and the latest solutions in this field are thus key factors in maintaining data integrity.

At the same time, the state's digital assets, especially those on which the functioning of key areas of the state depends (internal and external security, public finances, social security, healthcare, communications, energy), must also be protected from physical threats. This dimension of resilience as securing the digital continuity of the state has become a critical element of state security and sovereignty, especially in light of Russia's armed attack on Ukraine and the threat of further escalation now or in the future. The prevailing military dimension of the conflict has reminded decision-makers that resilience must also include the aspect of physically securing data and digital infrastructure elements. Therefore, more and more countries are asking themselves how to secure data centres storing digital state records and key digital data of vital economic and administrative importance in case of military threats, such as a missile attack or other events with physical consequences. Additionally, it must be assumed that the threat to the security and integrity of data physically located only on the territory of countries adjacent to Ukraine will persist for at least as long as the Russian Federation pursues an imperialist and revisionist geopolitical policy. Natural catastrophes resulting from ongoing climate change should also be considered an equally important danger. In this context, **the idea of a "data embassy"** deserves attention. This is a secure storage facility for key state data, including copies of key state records in the event of damage or loss to domestically processed data. These embassies, the data they hold, and the infrastructure in which the latter would be stored should all be placed

under the jurisdiction of their respective countries, covered by the same legal guarantees as data and servers in the home countries, and situated outside the potential theatre of war.[58] A data centre with state-of-the-art security, integrated with the government cloud, located under a ratified international agreement in Luxembourg, was already launched by Estonia. It stores encrypted backups of the country's digital data in case of attack – digital and physical.

Another way of collecting, processing, and reconstructing data, which can significantly influence building the resilience of states – understood both classically and through the lens of cyber-resilience – in terms of continuity of government operations during a crisis, is the evacuation (de-localisation) of state records to the cloud. As defined by the US National Institute of Standards and Technology, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that are available over a network.[59] Such a solution allows the investment in specific physical assets, such as servers, to be skipped, and technology services to be flexibly accessed, which is crucial in the event of threats that could potentially interrupt the continuity of government operations.

CASE STUDY

Just how important a role the cloud plays in maintaining continuity of public administration was demonstrated by the events in Ukraine taking place in late February 2022, cited by Microsoft's report *Defending Ukraine: Early Lessons from the Cyber War*. Prior to the war, Ukraine's Data Protection Law prohibited state authorities from collecting and processing data in non-governmental clouds, meaning that the state's digital infrastructure was collected on servers housed in government buildings. Recognising their susceptibility to both kinetic and cyber activities, a week before the full-scale escalation of the conflict the Ukrainian parliament passed an amendment that allowed data to be migrated to the public cloud. Within 10 weeks, critical data and processes of more than 20 ministries and 100 state agencies and state-owned companies were transferred. This protected them from destruction, as among the early targets of Russians' missile strikes and cyberattacks (using wiper malware deployed for destructive purposes) were precisely the Ukrainian government data centres.[60] According to George Dubinsky, Deputy Minister of Digital Transformation of Ukraine, more than 150 state registers have been moved to the cloud since the beginning of the war.[61] Ukraine has also signed an agreement with the UK on cooperation between the State Archival Service of Ukraine and the UK National Archives concerning the temporary transfer of cloud storage and digital backups of Ukrainian state archives in case of their possible loss.[62]

Another important component of building cyber-resilience is the so-called panic button or emergency button. Such a solution should be used in situations of threat or state officials' inability to discharge the functions and ought to perform several roles: alert the relevant persons and services of the crisis situation and track the position of the affected person, initiate the process of ensuring the continuity of state administration through the implementation of crisis response plans; finally, initiate the encryption and transfer procedure for the data which the person using this service is accountable for. Buttons should function as part of internet networks, using data transmission protection systems such as end-to-end encryption, and independently, such as via radio waves. Panic buttons should be integrated with decision-supporting applications in the event of emergencies.

One of the basic safeguards against the loss of state administration continuity is also the preparation of alternative venues for the operation of state units. Such a safeguard allows for the immediate resumption of operations following a disaster.[63] These venues should be both physical, equipped with devices that help pursue the statutory activities (power generators, ICT equipment, Internet access, etc.), and virtual, helping in remote coordination of activities from anywhere. The latter should also be strongly protected against potential integrity breaches.

3.2 Energy supplies

Łukasz Gawron

The services that ensure society's access to stable energy sources are among the most vulnerable parts of critical infrastructure. Today's economy relies on a stable supply of electricity, gas, and oil, with any disruption in supply possibly spelling catastrophic consequences for society, the economy and national security. For this reason, ensuring the security of installations that distribute or process critical energy resources is a priority. In the digital age, in addition to issues related to physical security and adequate infrastructure protection against natural disasters, terrorist attacks, or acts of war, the topic of ICT security is becoming increasingly important.

The worries about adequate security of energy infrastructure can be seen in the regulations adopted at EU level. The NIS Directive sets out measures to achieve a high level of network and information system security among Operators of Essential Services. Any enterprise identified as an OES by a given country must implement a sufficiently high level of cybersecurity in the organisation to prevent incidents, react to them appropriately, and above all maintain business continuity and rebuild the operations.[64] In Polish legislation, most large energy supply companies are listed in the catalogue of Operators of Essential Services and the 2018 national cybersecurity system act 2018 (as an transposition of the NIS Directive) imposes relevant obligations on them with respect to strengthening cybersecurity capa-

bilities.[65] In addition, the emergency management act of 2007 identifies energy, energy commodity, and fuel supply systems as parts of critical infrastructure.[66] These examples show that action at the EU and individual member state level places particular importance on the protection of energy supply, on the one hand, while it increasingly forces them to place greater emphasis on ICT security, on the other. In connection with building the cyber-resilience of energy supply organisations, we can distinguish two spheres: technological and organisational.

The technological sphere refers to the issue of implementing appropriate cybersecurity solutions that enhance the overall resilience of an organisation's ICT systems. This can refer to both physical hardware (hardware) and software (software). However, it should be noted that energy companies rely heavily on industrial operational technology (OT) systems in addition to the use of a classically understood IT infrastructure. IT and OT layers work complementarily, so an important issue that cannot be forgotten is monitoring the security at the interface between IT (i.e. the business layer) and OT (the industrial layer) systems.[67]

Cyber-resilience building solutions in the energy sector will hardly differ from other solutions used by the companies from another sector. Of these, certain topics exist that should be implemented with particular care to address cybersecurity, e.g. network infrastructure security and monitoring, end-device protection, network segmentation and encryption, remote access security, or workstation security. On the other hand, special attention needs to be paid for the security of OT installations, which, due to their specific nature, require a different approach to security and therefore other resilience-strengthening technologies.

A particular issue coming to the fore recently is security at the interface between IT and OT networks. It is obvious that IT and OT operate differently and have different objectives and risks. However, as digital systems will connect to industrial systems, they will simultaneously be exposed to more cyber threats. Industry experts predict that IT-OT will only continue to converge. This means that OT administrators should make every effort to understand the IT environment and vice versa.[68] New technologies can support both environments, and one innovative solution in this area is a probe that monitors threats across the industrial network.

However, cyber-resilience building cannot be based on technology issues alone. In the context of building energy sector resilience, as in any other sector, organisational security issues are an important aspect. Organisational security is understood to mean specific information security policies, the model of cybersecurity system management, risk estimation methodologies, processes, or low-level building of a cybersecurity culture within an organisation. Even the best and most bleeding-edge technologies won't be able to stop an attack and strengthen an organisation if they are not properly managed and the people responsible for security are not properly trained or do not have their roles properly assigned. Therefore, technology security should always go hand in hand with organisational implementations, and the staff responsible for this area need to be trained regularly. International standards and frameworks can be helpful in building organisational resilience, such as:

- ISO27001 – contains requirements for an information security management system (ISMS); using it enables organisations to manage in various ways the security for assets such as employee data, data entrusted by third parties or intellectual property.[70]
- NIST 800-82 – provides guidance on securing Industrial Control Systems (ICS).[71]
- ISO 22301 – describes the structure and requirements for implementing and maintaining a business continuity management system.[72]

Energy supply is a subject where another key property must be a permanent fixture, namely business continuity and recovery from disruption. In this context, it is a priority from the point of view of energy suppliers to create a business continuity plan, including the development of procedures with the responsibility delineation, the development of procedures for restoring key processes, the identification of key information systems, as well as the creation of appropriate communication procedures and the like.[73] Cloud solutions are a particularly helpful technology in the context of business continuity and disaster recovery. Disaster recovery using the cloud is a combination of cloud adoption strategies and services designed to back up data, applications, and other resources in the public or service-provider cloud. In the event of a disaster, the data, applications, and other resources affected can be restored to the local data centre – or cloud provider – and normal business operations can resume.[74]

CASE STUDY

IDSs (Intrusion Detection Systems) are solutions designed for monitoring IT networks and able to successfully fulfil their role in OT. Modern probes are distinguished by the use of dedicated predictive-analytical models that adapt to any network configuration using machine learning and artificial intelligence methods, due to which it is able to correctly detect anomalies and threats in the network. This tool is capable of monitoring, detecting, inventorying, and reporting on even the most advanced attacks passed against enterprises.[69]

This type of tool can be particularly applicable in companies whose scope of operations is mostly industrial automation systems. This catalogue includes a large part of critical infrastructure, in particular transport, energy, or drinking water supply.

CASE STUDY

Cloud disaster recovery (CDR) is a service that allows system data to be processed, stored, and recovered on a remote cloud-based platform. Cloud-based data recovery has several significant advantages over classic on-premise recovery:

- There is no need to purchase physical hardware and software to support critical operations.
- CDR scales up easily according to one's needs.
- It is more cost effective.
- Cloud-computing disaster recovery can be performed in minutes from anywhere – all the customer needs is an internet-connected device.
- Backups can be stored in multiple data centres spread across the globe.
- Cloud provider can quickly identify and correct any problems or errors.[75]

3.3 Ability to respond to mass uncontrolled movement of people

Łukasz Gawron

Crisis situations such as natural disasters or armed conflicts invariably trigger uncontrolled internal or international migrations. Particularly in times of armed conflict, the awareness of how to deal with crisis situations is crucial for building resilience and security of the state and its citizens. Properly prepared and, most of all, well-distributed information on rallying points, shelters, migration routes, etc., will build awareness among the public and publicise good practices on how to behave in emergency situations. Adequate education can help to make emergency management more efficient and minimise the risk of hazards and uncontrolled population movements.

In this age of technological advances and widespread internet access, social media is an ideal channel for communication and education. Some of the key factors determining the sensitive role of social media, in addition to universal access, are the pace of information spread, the ever-increasing number of users and the multiplicity of communication channels. Social media also allow for continuous two-way communication and 24/7 message following.[76] Still, it is important to bear in mind an important threat, a sort of side effect to the social media specificity, namely disinformation. This is why the need to build societal resilience, as discussed in chapter two, is so vital. Building resilience in the context of uncontrolled migration must start with education. Technology, which is an information distribution channel, is just a tool that can be counterproductive without proper awareness.

Crisis situations, including wars, always have the effect of causing uncontrolled internal and international population movements. For the uniformed services and the state apparatus, this is a huge challenge, but one that can be taken up with new technologies.

CASE STUDY

The Russian-Ukrainian war resulted in refugees mass-migrating to neighbouring countries, mainly Poland, Slovakia, Hungary, as well as the Czech Republic. As the war broke out and the refugee crisis started, the Ukrainian Embassy in the Czech Republic together with a business partner prepared a virtual assistant for Ukrainian citizens, which assisted thousands of refugees arriving in the Czech Republic when it came to registration, visa, employment, travel, or legal services.[77] Virtual assistants and chatbots have become a popular tool to support servicing large numbers of people in a short time, greatly simplifying formal issues related to residence in a foreign country.

Another challenge for central and local governments in managing the influx of migrants or refugees is the matter of integrating them into the national administration so that they can use the public services available in the country – offices, health services, public transport, etc. – as quickly as possible. In addition, the registration of people arriving in a country is also a security issue, so keeping adequate records is an important element.

CASE STUDY

A few weeks after Russia's aggression against Ukraine, the Polish government made it possible for refugees to obtain a PESEL number, which entitles them to health or education services in Poland, among other benefits.[78] In addition, the Polish government reached an agreement with the Ministry of Digital Transformation of Ukraine and made it possible for refugees to integrate the Ukrainian government mobile application Diia with the Polish e-gov application mObywatel. Thanks to this partnership, Ukrainian refugees have access to their digital wallet in Poland, too, and can take full advantage of the Diia functionalities.[79]

Not every citizen has access to the internet anyplace, anytime. Therefore, government information reaching the citizens during a crisis or preparing them for extreme situations should also be distributed through other mass media channels, i.e. radio, TV, last but not least text messages.

CASE STUDY

RCB Alert is an SMS emergency alert system operated by the Government Security Centre. Rolled out in 2018, the system is designed to inform citizens of a country or a particular region about potential life-threaten-

ing phenomena like natural disasters. Any citizen with a working and network-connected phone receives information about extreme weather events with brief instructions on what they should do at the moment. Such a system does not require an Internet connection to be present or an app to be downloaded.[80]

Such a simple system can also find its use during armed conflict and the resulting uncontrolled migration. Simple text messages sent from government services and administration would notify citizens about the place of refuge, the services available in a given region, or tips on formalities related to, for example, border crossings.

3.4 Food and water resources

Maciej Góra

Water and food access issues are the challenges that the developed societies of today have never had to face in recent decades. However, increasing tensions on the international stage, climate change, the rising population, and the rapid digital transformation have resurfaced a growing threat that these basic assets, whose availability is one of the elements of critical infrastructure, will become scarce.

In recent years, we could observe cyberattacks launched against food producers, with the most famous one targeting JBS S.A., the world's largest meat supplier. Ransomware malware , i.e. blackmail software, that was used, shut down JBS S.A.'s operations in the United States, Canada, and Australia, and the company had to pay USD 11 million in Bitcon in order to unblock its systems.[81] Water treatment systems have also been subjected to targeted attacks. For example, in 2021, a hacker gained access to a water treatment facility in Oldsmar, Florida, trying to poison water resources by increasing the level of sodium hydroxide (lye) from 100 parts per million to 11,100 parts per million. Luckily, the malicious attempt was thwarted by the plant operator before the toxic level of lye entered the water supply.[82] In 2019, the American Water Works Association named cyber risk the top one threat to the U.S. water supply sector. Certainly, similar threats exist in Europe, too.

Due to their specificity, these critical infrastructure elements are particularly vulnerable to cyberattacks. Water and food are basic resources, and their absence or contamination affects not only end-users, but also entire supply chains. Mass production of food, production in industrial, energy, and chemical sectors, the functioning of health and emergency services and many other sectors of the economy and critical public services is impossible without access to treated water. At the same time, access disruptions to drinking water in the summer put at risk not only crops and livestock, but also endanger human health and life. On the other hand, interruptions in the supply of basic nutritional products, such as grain, affect the availability of fodder and, by extension, of meat and dairy products. At the same time, these areas are particularly vulnerable in specific periods of time; in the case of the food industry, hacking intelligent agricultural systems during the sowing or harvesting period will result in shortages of agricultural products throughout the year, with disastrous consequences for the entire economy and food security. Finally, there are also "classic" problems in this area of critical infrastructure which digital technologies can address: food waste, cancellations of contaminated batches of products, low productivity of some areas of agriculture, logistics problems, transportation issues or climate change. These technologies are used in the Supply Chain Risk Management (SCRM) process which encompasses a wide array of strategies to identify, assess, mitigate, and monitor unexpected events or conditions that may, usually adversely, impact any part of the supply chain.[83]

One of the most widely used solutions in the field of food safety is blockchain technology. Blockchain is a digital, decentralized, and distributed ledger that saves and adds transactions in a chronological order to create immutable and tamper-resistant records.[84] In the food safety research field, blockchain technology is mainly used to ensure that data generated in the food production process is not falsified to corroborate product safety, enhance food traceability, and increase consumer confidence in food safety.[85] Considering the specific characteristics of this technology, including the impenetrable and dispersed nature of the ledger, it ensures that in times of crisis the information provided to state authorities during a potential food crisis is reliable, allowing for better planning of preventive actions. In this context, blockchain technology is integrated with the Internet of Things devices, which regulate, among others, the safe storage and transport of food.

Artificial intelligence (AI) is another technology that allows for increasing food supply chains resilience. AI enables crops to be enhanced by improving harvest yields, increasing the number of valuable databases on food production processes and analysing variables such as weather, humidity, soil composition, pesticides used, and the price of semi-finished products.[86] It is also widely applied to optimize the energy resources used; food production is an energy-intensive process, and appropriate algorithms can help reduce the demand for it. An important aspect of using Artificial Intelligence involves determining appropriate food transportation pathways that will minimize fuel consumption, and thus reduce greenhouse gas emissions, enabling food to reach end-users as quickly as possible. AI was a key technology that helped optimize alternative routes when the Suez Canal was blocked in 2021.[87]

Bearing in mind the critical and increasingly important role of food resources, their precarious nature, vulnerability to attacks and natural disasters, technologies such as AI, big data, blockchain and the Internet of Things allow for the appropriate optimization of these elements of critical infrastructure and develop civil resilience to threats.

3.5 Ability to handle incidents with mass casualties and disruptive health crises

dr Michał Hampel

Mass casualty incidents occur rarely, but in relation to their mass character they are a burden to the healthcare system in a way that far exceeds the norm. Our actions, e.g. ensuring the capacity of the civil healthcare system along with the stock of provisioned medical supplies, should consist of increasing the ability to react to the incidents of this kind in a controlled and adequate way.

The primary division among similar events is one that distinguishes multiple-casualty and mass-casualty incidents. A multiple casualty incident happens when there are many injured, but the particular need for immediate medical help and rescue actions does not overwhelm the available resources and means of the rescuers present on the scene. In contrast, a mass casualty incident occurs whenever the needs exceed the operational capacities there, in terms of the resources and means the acting services have at their disposal.

Using modern technologies can make the reaction markedly more efficient in emergencies and situations where non-standard extent of help is needed. The emergency medical services and civil protection system ought to be equipped with such tools as central database for resources and means availability in a given area, with the ability to deploy them with immediate effect. A national emergency management centre with its branches in every province seems like an appropriate structure to tackle extraordinary situations, of which mass casualty incidents are a subset.

What should be active is a centralised system gathering data on services' availability and resources, updated in real time, including the police, fire services, healthcare, and others. The information on medical entities should include the details on the availability of places in individual hospital wards from a given region, with a particular emphasis on surgery units, ICUs, and hospital emergency department occupancy levels. Coupled with additional data, such as operating theatre availability and specialised care capabilities, such information would increase the efficiency of care provided and would make help more adequate and not delayed in any respect. A major topic vis-à-vis mass incidents, in which due to a heavy load on the system shortage of care, including basic care, can be observed. It is thus vital that a patient is taken at once to a facility where they will find help with no delay, the aid will follow standards of care, and the recipient hospital will have the proper infrastructure and an empty bed at its disposal. With this, we can avoid straining the resources of individual medical centres and the situation in which delay in care provision might impact the patient's chances of survival.

Such a system should be integrated with other services' systems, and information about the mass casualty incident should give rise to launching the actions of relevant services – and, should their means and resources be temporarily limited, give the adjacent regions an opportunity to be engaged. An emergency management centre and the relevant services should have the capacity to geolocate individual units in real time with the type of unit, staff, abilities being listed and to deploy tools of direct contact.

Importantly from the perspective of public safety and appropriate reaction to mass casualty incidents, what should be developed is an application for citizen with the functionality of signalling a dangerous situation (a mass accident, a terrorist attack, an explosion), which can significantly shorten the time of informing the relevant services. Such an app should give the possibility to make everyone near the incident aware that it occurred, relay information on the need to prepare for evacuation or directly on its commencement. Taking into account the present-day public transport system, the Underground, urban transportation, and other carriers that use apps to arrange rides, what should exist is the ability to centrally restrict driving near the hazard area and the spot of the incident. This would greatly reduce the risk for third parties and increase the efficiency of rescue action conducted directly on the spot. Bearing in mind the current situation related to the war in Ukraine and the resulting dangers, the app should also include information on the closest shelters, medical care points, aid facilities.

Such a system should also itemise warehouses and their supply stocks relevant for mass casualty incident occurrence.

CASE STUDY

Among millions of Ukrainian refugees, there exist people for whom the outbreak of war cut short the treatment started in Ukraine. These people most often are not in possession of medical records, which were destroyed in acts of war. Nor is there a possibility of recovering records from bombarded Ukrainian hospitals. In such cases, many time-consuming test and examinations have to be done from scratch and risky decisions have to be taken, especially regarding a suddenly interrupted oncological treatment. Such a situation is a detrimental influence on the patients' health. The states of affairs just described shows how big the impact of delocalisation on data security is. In the cloud computing technology, the data is stored in the so-called availability zones – physically isolated locations within the region of cloud service operation. The physical separation of AZs ensures cloud resilience to local failures, natural disasters, or extreme emergencies such as a bomb going off or a rocket striking down. Each item of information stored in the cloud is synced simultaneously in three AZs connected in an efficient network.
The cloud computing technology can not only safeguard the security of medical data but also greatly ease access to such data. Combining data processing centres into a global ecosystem enables clients to use them at any point on the globe. Medical data can in this setup follow the patient, with the cloud provider taking a large part of responsibility for its protection over from the hospital.

3.6 Ensuring civil communications

Łukasz Gawron

Fast and reliable telecommunications are the foundation of today's digital world. Currently, most of the population has access to telecommunications networks or wireless Internet. The Internet underpins the operation of many governmental administration systems, the military, critical infrastructure and other types of services. Therefore, strengthening the cyber resilience of telecommunications infrastructure should be considered critical for increasing the resilience of the entire state. Moreover, just like energy supply, communications are considered a critical infrastructure of the state and any disruption of communications, especially in crisis situations, can have catastrophic consequences for its functioning. This approach is reflected in the announcement made by NATO defence ministers in November 2019. The member states agreed to revise the basic requirements of the Alliance regarding civil telecommunications to reflect emerging concerns about 5G technology[88] and its impact on the civil preparedness of the Alliance.

Strengthening the resilience and reliability of telecommunications infrastructure is also the subject of regulation in individual countries of the European Union and the United Kingdom. The Cabinet of the UK's Prime Minister has put forward five basic principles of telecommunications infrastructure cyber resilience, which can also be successfully applied by other Allies.[89]

1. Look at processes and organizations, beyond technical solutions:
   - → When considering resilient telecommunications infrastructure, great emphasis is placed on technical solutions, such as broadcasting stations or mobile phones. However, the processes and the way in which market actors organize themselves to respond to emergency situations should be considered holistically.

2. Identify and review critical communication operations that underpin the crisis response arrangements
   - → Critical communication operations should be identified as the basis for crisis response processes (e.g. designation of appropriate contact persons and exchange of information between safety-critical institutions)

3. Ensure diversity of your technical solutions
   - → For critical operations, increasing the diversity of technological means of communication may be considered. However, it may be difficult to assess the true diversity of technical solutions due to the inherent dependence of one technical solution on another.

4. Adopt emergency "layered solutions"
   - → No technical solution will be available at all times. Availability is a consequence of system reliability (related to faults and their repair) and its ability to cope with overload (resulting from excessive demand). Adopting a layered emergency approach to the process of selecting technical solutions helps to reduce unavailability.

5. Plan for appropriate interoperability
   - → Cooperation among services, business, public administration in order to better coordinate crisis response

Communication infrastructure is also prone to damage caused by natural disasters and military operations. Therefore, another key factor which strengthens resilience in this respect may be the use of alternative means of communication, i.e. satellite communications. Satellite-based communication enables fast and reliable communication even in unfavourable conditions. A perfect example of a successful implementation of the solution during an armed conflict is the use of the Starlink satellite Internet designed by a U.S. company, SpaceX.

CASE STUDY

Shortly after the Russian aggression began, the Minister of Digital Transformation of Ukraine, Mykhailo Federov, asked the founder of SpaceX, Elon Musk, to access Starlink's proprietary high-speed satellite Internet. It is a system of low orbiting satellites (currently approx. 2,200) that provides Internet connection when other communication channels are unavailable. Starlink proved extremely useful when Russians began to intentionally destroy the telecommunications infrastructure. SpaceX responded to the request of Minister Fedorov and sent appropriate terminals to Ukraine to connect it to the satellite Internet. Starlink terminals were first deployed to critical infrastructure facilities: hospitals, banks and energy companies[90]. Currently, approximately 150,000 people in Ukraine use Starlink's system every day[91].

Reliable telecommunications are also indispensable for services to run their operations in crisis situations. When conducting rescue operations in a poorly urbanized areas during a naturally occurring hazard event, the services cannot take advantage of the existing infrastructure due to the absence of or damage to the infrastructure in that area. The problem may be solved by quickly setting up a 4G/5G portable network.

CASE STUDY

Mission Critical Network in the Box (MC-NIB) is a solution designed for emergency services, critical infrastructure operators and the military. It was created to ensure communication in crisis situations, such as natu-

ral disasters, threats to public security, large-scale failures of telecommunications or energy infrastructure. It is a 4G and 5G solution that provides special connectivity for industries requiring reliable and secure connections, such as fire brigades or the military. It is an independent communication system that allows for a quick set up of a 4G or 5G telecommunications network for use in any situation and in any conditions, even the most extreme ones. Portable MC-NIB can be quickly deployed by uniformed services, and easily fits inside a suitcase or a backpack.[92]

We cannot forget about ensuring the continuity of digital communications, particularly for government entities. In the digitalisation era, maintaining uninterrupted Internet access is just as important as sustaining traditional telephone communication channels. During a military conflict, apart from the likelihood of the Internet infrastructure being destroyed, there is also a risk of sensitive government resources being taken over by aggressors. In addition, in the event of a military operation in a state's territory, its government administration must maintain continuity of operation. Due to such a large number of armed conflict risks, which have a direct impact on maintaining the continuity of communications, and thus the continuity of the government administration's work, it is necessary to build cyber resilience by preparing proper contingency plans.

CASE STUDY

Cloud computing is a solution that ensures the preservation of digital communications and the continuity of government services. On 16 March 2022, the Ukrainian government adopted a law on cloud services which allows government agencies to use cloud services, and introduces the Cloud First principle. The principle talks about the need to transfer the core IT services used by the state administration to the cloud. This decision enabled the Ukrainian government to easily perform its duties while minimizing the risk of purchasing compromised hardware and significantly reducing budget expenditures.[93]

3.7 Transport systems

Sławomir Łazarek

The last but not least element. Just as an effective communication system is the "nervous system" indispensable to ensure military force command (for national and allied forces), state apparatus management (for central and local administration), continuity of essential services for the state and its citizens, and functioning of society as a whole, the state's transport system delivers a sort of "circulatory system" to ensure all of the above. In keeping with the principle that serves as a motto for transportation and troop movement personnel, "nothing happens till something moves". Importantly, it should be noted that ensuring the Freedom of Movement or Military Mobility depends to a large extent on civilian support. The military relies on civilian means of transport, on civilian re-loading capacities, and on civilian traffic-control-related solutions. Ensuring deconfliction of civilian populace migrating away from the warzone versus military movement towards the fighting areas hardly plays a smaller role.

Mobility and ability to move are crucial for everyone. From everyday rides of private citizens to the correct functioning of global commodity supply chains to commercial outlets and for industrial production needs. Transport is a factor that makes the economic but also social life go round.

The crisis tied to the COVID-19 pandemic demonstrated how big a role the transport plays and how large the social, health, and economic costs are of severely restricting or completely freezing the free movement of people, goods, and services. Maintaining supply chains and a coordinated international approach to connectivity and transport are key to overcoming any crisis and strengthening the resilience of states and their societies.

Nowadays, to ensure that all the previously mentioned areas of state and societal functions do operate, it is essential for a country to have an efficient transport system that is resilient to all kinds of threats, especially hybrid and cyber dangers.

The civil transport system in recent years has been subject to a rapid digital transformation. In fact, the entire transport system depends on ICT support. Traffic control and management systems in every mode of transit, freight and passenger handling systems, transshipment management systems in seaports, airports, cargo terminals are basically all dependent on modern IT systems. And this is the case on the local, national, and international/global scale alike. The degree of their digitalisation is only set to increase.

The management of cargo and means of transport, the optimisation of routes, and the handling of orders are increasingly taking place through IT systems. This is par for the course especially for large transport operators with a dense interdependency network in the market. Unfortunately, an adequate level of cybersecurity in the IT systems used is not the standard in transport yet. The systems and their protections in place against cyberattacks vary from carrier to carrier and from one transport infrastructure manager to another. The transport system is characterised by an extensive network of dependencies across the global supply chain. This means that a cyberattack against one operator automatically paralyses the operations of its suppliers and partners – a cascade effect.

Gaps in security systems and the lack of uniform standards to protect against cyberattacks, as well as the processing of valuable data on transported cargo – these are the main reasons why the freight system is currently so vulnerable to cyberattacks. It is valuable

and profitable for cybercriminals who want to use the data obtained in this way, for example for illicit (ransomware extortion) or terrorist activities (e.g. attacks on railway stations or disruptions of military traffic). Transportation details are also used as a means of competitive warfare, to destabilise or break supply chains or to generate significant financial losses in specific companies. It is also an obvious target for warfare-attendant attacks.

CASE STUDY

In June 2017, a cyberattack using the NotPetya virus unfolded, affecting among its victims the Danish transport company A.P. Moller-Maersk – the world's largest container shipping operator. The company's IT systems were unavailable for several days. During this period, Maersk was forced to shut down part of its fleet management and order processing systems. No theft of sensitive data took place. Despite this, the attack paralysed the company's operations, caused significant financial losses (the operator's quarterly profit was reduced by USD 300 million) and led to disruptions in the global supply chain as well. The incident, along with a few episodes of a similar nature, involving cybersecurity breaches targeting large transport, shipping, and logistics companies, led Thales and Verint to rank transport as fourth on the list of sectors most frequently attacked by cybercriminals in 2019.[94]

It is worth noting that the "hostile and intentional" actions of cybercriminals are not the sole source of threats to the proper functioning of a country's transport system. Such threats also arise from the vulnerability of IT systems to "operational malfunctions – equipment failures", which, as the use of certain equipment and components from a single manufacturer can be intensive, might even result in global disruptions to the movement of people and goods. In addition, in such cases it should be pondered (even once the relevant committees and official services deem such an incident to be a "component failure") whether our adversary was potentially behind the "failure". Deliberately triggering an "incident" could significantly impede or prevent, for example, the timely movement of allied reinforcement units.

CASE STUDY

On 17.03.2022, a disruption occurred across Poland's rail network, affecting 19 of 33 local Control Centres equipped by Alstom. A multinational French manufacturer of rolling stock, Alstom is active worldwide in rail transport markets. In Poland, it is the largest manufacturer in the rail industry. At first, PKP PLK and the government plenipotentiary for cybersecurity did not rule out the possibility of this being the work of hackers. However, as it turned out, the problem had to do with the company's software. Its announcement reads: "Alstom confirms that there was no cyberattack or security issue related to the time-formatting error which occurred on 17 March 2022. Time-formatting errors are a known phenomenon."

Another example. On 27 February 2022, the Belarusian Railways were paralysed, which meant the transport of troops and supplies became severely hamstrung. The action was reported at the time by the anonymous Cyberpartisan Group from Belarus. The rail traffic control system was hacked and switched off and this caused the need to switch to manual control, prompting very long railroad delays throughout the country. Nor was this the first hacking effort targeting Belarusian railways. On 25 January 2022, the state carrier's servers were encrypted, with the demand that Russian troops which were setting the stage for the war against Ukraine needed to withdraw from Belarus.

4. STATE RESILIENCE: THE WAY FORWARD

Witold Skomra, PhD, Eng

Until the computers and digital technologies came on the scene, all areas of security were treated as separate environments, with physical security (keeping third parties away) seen as the main goal of the actions performed. The integrative potential of digital technologies has for over a dozen years made the security of both organisations and whole states multidimensional in nature. In Poland, the document that defined this is the National Critical Infrastructure Protection Programme. As per the document, security comprises six intertwining areas. These are the physical, technical, personal, cyber (IT and OT), legal security, and continuity of operations. According to the NCIPP, physical security remains the core of this multidimensional grid of dependencies.

The digital transition and the deepening dependence of modern societies on civilisational advances and emerging technologies means that the approach NCIPP proposed needs a significant correction. The transition just mentioned is pursued in individual, group, and nation-wide dimensions alike. Individually, few realise that by using a dedicated app, they become participants in the internal processes of a bank, an energy supplier, or a concert organiser. The nation-wide dimension of the digital transition matters much more. The interdependencies in processes, managed by individual entities both in either a standalone or shared way, make the state a single organisational structure requiring joint governance. The tool-seeking process for governing the state security can be divided into several stages. The stage of autonomous entities' functioning, of system management, and ultimately of management for a system of systems[95]. The difficulty in managing systems of systems comes from the fact that individual users might even be oblivious that their processes are part of a wider structure. At the same time, even seemingly minor disturbances in a complex system can, via a domino or cascade effect, cause difficult or impossible to predict consequences in fields that appear unrelated.

The observation that the whole of society starts to function as a single organism, with a whole interweaving network of interdependencies that put digital technologies to use or are supported with them, strongly calls for a change in the strategy for building public security. The bottom-to-top approach, present to date, meaning that we focus on the security of individual organisations (and sometimes just of particular facilities), must be replaced with a top-to-bottom approach. The new strategy assumes the social goals and the results of their disruption to be defined first, and only later do individual entities (operators of essential services) on this basis adjust to the demanded availability level for the services they offer.

An attempt to include this strategy in legal regulations informs two draft EU directives. These are the NIS 2 Directive, mentioned many times before, involving cybersecurity, and the draft Directive on the Resilience of Critical Entities (CER)[96], touching on other realms of security. A regulation tied to these two is DORA, which takes into account the specificity of the banking sector. The three basic legal acts along with their implementing rules are set to create a brand-new landscape for building public security. The new strategy following the drafts will be deployed in several stages. At first, EU member states are to identify the essential processes and the risks related to their disruptions. This part of the work ends with preparing a strategic document that shows what level of resilience to disturbance the state is intending to achieve. In the next step, the operators of essential services are assigned, and in the CER Directive case, so is the critical infrastructure these operators are managing. An added element in the new strategy is the comprehensive risk assessment process. The process accounts for the specificity of particular operators, but its main value is the administration-governed mitigation process for the risks deemed unacceptable for state interests. At bottom, it involves individual operators having to implement organisational, technical, and security measures that are relevant and proportionate to the risk they are exposed to.

To sum up, what needs to be highlighted is that changes in the security landscape, coupled with the ongoing tech revolution, make it necessary to use new management strategies for the field of public security. With no inter- and supra-ministerial solutions, attaining the appropriate level of state resilience seems hard or next to impossible. And such a level we took upon ourselves to achieve as part of the NATO alliance, by accepting seven baseline resilience requirements. At the same time, the first and indispensable condition to build state resilience when faced with the present challenges is to have decision-makers realise in advance the need to adjust to the new circumstances. The present Report is an important component in this awareness-raising.

SUMMARY

In the current geopolitical situation, with its attendant undertone of threats to the national security of the EU and NATO states, resilience needs to be perceived as a holistic challenge, incorporating a military and a civilian dimension, which in these circumstances increasingly permeate, reinforce, complement each other. Resilience building – in all its renditions: digital, cyber, and societal – requires intersectoral and multidimensional co-operation both across individual countries and the whole international community.

BIOGRAPHIES

Izabela Albrycht

CYBERSEC Forum co-creator and Chair of its Programme Committee, member of the Advisory Board to the Polish Cybersecurity Cluster #CyberMadeinPoland. Political scientist, for years she has been specialising in the topics of strategic aspects of security, including cyber and technology. Member of NATO's Advisory Group on Emerging and Disruptive Technologies and Poland's Council for Digital Affairs. Since January 2022, member of the Council on Security and Defence in the Chancellery of the President of Poland. From 2020 to 2022, member of the Board for DIGITALEUROPE, representing Polish ICT industry bodies there – PIIT, Digital Poland, and KIGEIT; currently in DIGITALEUROPE she is part of the Digital Resilience Executive Council. Member of Supervisory Board in Asseco Poland S.A. and in ComCERT. A former Chair of the Kosciuszko Institute from 2010 to 2021.

Maciej Góra

Project Coordinator at the Kosciuszko Institute. He studied National Security at the Jagiellonian University, Cybersecurity at the AGH University of Science and Technology (both in Kraków), and International Relations at the Charles University, Prague. During his tenure at the Kosciuszko Institute he coordinated multiple initiatives and projects, creating and operationalizing multiple points of agenda of European Cybersecurity Forum – CYBERSEC, leading the Institute engagement during Internet Governance Forum 2021 and IGF Poland 2022, co-authoring the anti-disinformation textbook for high schoolers and teachers, participating as guest and as a host in the General Talks podcast, and more. His research and professional interests include digital and cyber issues on a micro (reducing digital footprint, personal online safety) and macro scale (geopolitical dimension of cybersecurity, cybersecurity management, digitalization-related social processes, futurology).

Michał Hampel, PhD

Doctor, specialist in general surgery, works in the Gastroenterology and Transplantology Clinic of the Ministry of Internal Affairs and Administration's Central Clinical Hospital in Warsaw, lectures at the Cardinal Stefan Wyszyński University in Warsaw. Since 2019, emergency-team doctor at the Polish Centre for International Aid. In 2020, he took part in setting up the temporary hospital at the National Stadium in Warsaw. He created and coordinated the operation of the largest Populace Vaccination Point against COVID-19 at the National Stadium. Acts as the Medical Coordinator of the National Stadium in Warsaw, responsible for ensuring medical support during mass events. Participated in many medical missions related to counteracting the spread of and combatting the effects of the pandemic, took part in the post-explosion rescue mission in the port of Beirut, Lebanon, the evacuation mission in Afghanistan, performing the medical support tasks for the Polish task force and the evacuees, and coordinated the efforts to launch and operate the medical train for evacuating Ukraine citizens to Poland.

Michał Krawczyk

Disinformation analyst and project coordinator at the Kosciuszko Institute. Graduate of the Jagiellonian University in Kraków, majoring in National Security, where he dealt with the issue of building societal resilience to disinformation. Participant of the Changing Security and Hybrid Threats summer school at the University of Jyväskylä and graduate of the Digital Sherlocks programme run by the Atlantic Council. At the Kosciuszko Institute, member of the Prozodia research team, author of publications in the area of disinformation analysis, and host of the General Talk podcast.

Sławomir Łazarek

Chief of International Cooperation Unit in Poland's Government Centre for Security; Master's degree in road and bridge construction at the Military University of Technology in Warsaw and postgraduate study in economics of defence at the War Studies University in Warsaw. Retired colonel of Polish Armed Forces (PAF) and former Deputy Chief of Polish national Movement Coordination Centre. Previously, over his 32 years of military service, promoted to various positions responsible for preparation of transport system for defence purposes. In cooperation with the civilian management of transport infrastructure of Poland, involved in the development of minimum military requirements for the transport network and transport requirements for military armaments and equipment as well as in the development of rules, procedures, and instructions for the movement and transport system of PAF, in the preparation and securing of M&T by all modes of transport. Polish representative to the NATO Movement and Transportation Group. Now responsible for coordination of crisis management and civil planning issues at the national and international levels, in particular crisis response systems, resilience strengthening, and civil-military engagement.

Krzysztof Malesa, PhD

Board Member, National Security Officer at Microsoft Poland. Expert in the field of crisis management, critical infrastructure protection, and resilience. From 2010 to 2021, he worked in the Government Centre for Security. He was the head of the Polish delegation to the NATO Civil Emergency Planning Committee and the national delegate in the working group preparing the European Union Directive on Critical Entities Resilience (CER). Krzysztof Malesa graduated in Baltic philology at the University of Warsaw, where he also obtained a PhD in linguistics. He is a sworn translator of the Lithuanian language.

Witold Skomra, PhD, Eng

Adviser and concurrently the director to the Critical Infrastructure Protection Department in the Government Security Centre. Expert in civil planning, crisis management, and critical infrastructure protection. Poland's delegate to the working group for drawing up the Critical Entities Resilience Directive and to the OECD's High Level Risk Forum. Lecturer of the Faculty

of Management at the Warsaw University of Technology. His classes tackle the continuity of operations, risk management, managing public security, and protecting the critical infrastructure. He is a former firefighter – Chief Commandant of the State Fire Service, graduate of the Main School of Fire Service and of the National Defence University.

ENDNOTES

1 National Security Strategy of the Republic of Poland, 2020, p. 10.
2 Ibidem, p. 15.
3 Ibidem, p. 20.
4 "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack" – Art. 3 of the North Atlantic Treaty, done at Washington April 4, 1949, https://www.nato.int/cps/en/natolive/official_texts_17120.htm, [online: 29.06.2022].
5 Współpraca w ramach NATO, https://www.gov.pl/web/rcb/wspolpraca-w-ramach-nato#_ftn2, [online: 29.06.2022].
6 Previously the Civil Emergency Planning Committee (CEPC) worked in the similar formula. *Resilience and civil preparedness – Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, [online: 29.06.2022].
7 *Resilience and civil preparedness – Article 3*, https://www.nato.int/cps/en/natohq/topics_132722.htm, [online: 29.06.2022].
8 The National Security Strategy of the Republic of Poland refers to the seven baseline NATO resilience requirements directly, as it draws attention to the necessity to increase resilience "predominantly" in these areas, cf. The National Security Strategy of the Republic of Poland, p. 16.
9 Brussels Summit Communiqué issued 14 June 2021, https://www.nato.int/cps/en/natohq/news_185000.htm, [online: 29.06.2022].
10 Madrid Summit Declaration issued 29 June 2022, https://www.nato.int/cps/en/natohq/official_texts_196951.htm, [online: 29.06.2022].
11 NATO's Strategic Concept, https://www.nato.int/strategic-concept/, [online: 29.06.2022].
12 "We will enhance our individual and collective resilience and technological edge", ibidem, [online: 29.06.2022].
13 NATO releases its Climate Change and Security Impact Assessment, https://www.nato.int/cps/en/natohq/news_197241.htm, [online: 29.06.2022].
14 *Strategic Foresight Report*, https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2020-strategic-foresight-report/resilience-dashboards_en, [online: 24.06.2022].
15 *Resilience*, https://joint-research-centre.ec.europa.eu/resilience_en, [online: 24.06.2022].
16 An in-depth analysis of National Recovery Plans for 12 Central and Eastern Europe EU member states can be found in the report *Three Seas United in Cyber Power*, https://ik.org.pl/publikacje/premiera-raport-three-seas-united-in-cyberpower/, [online: 24.06.2022].
17 The pandemic resulted in visible reduction of the global GDP, decrease in industrial production, growth in joblessness levels, increase of public debt, drop of exports.
18 *Digital path to recovery and resilience in the European Union*, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/news/digital-path-recovery-and-resilience-european-union, [online: 24.06.2022].
19 *Ibidem*, https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/news/digital-path-recovery-and-resilience-european-union, [online: 24.06.2022].
20 "The average U.S. household now has a total of 25 connected devices, across 14 different categories (up from 11 in 2019)", more: *Connectivity & Mobile Trends 2021 Survey*, Deloitte, https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-pandemic-stress-tested-digital-home.html, [online: 24.06.2022].
21 J. De Groot, *What is Cyber Resilience*, https://digitalguardian.com/blog/what-cyber-resilience, 2019,

[online: 24.06.2022].
22 https://www.consilium.europa.eu/pl/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen, [online: 24.06.2022].
23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en, [online: 24.06.2022].
24 Cf. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy, [online:28.06.2022].
25 Por. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024, [online:28.06.2022].
26 https://www.eesc.europa.eu/pl/our-work/opinions-information-reports/opinions/roadmap-security-and-defence-technologies, [online: 24.06.2022].
27 *United for a new era*, 2021, p. 19, [online]: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.
28 European Commission, *2018 Code of Practice on Disinformation*, 16 June 2022, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation, [online: 29.06.2022].
29 European Commission, *2022 Strengthened Code of Practice on Disinformation*, 16 June 2022, https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, [online: 29.06.2022].
30 European Commission, *The Digital Services Act package*, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package, [online: 29.06.2022].
31 EU Disinfo Lab, *Tackling disinformation online: the Digital Services Act opens the era of accountability*, 25 April 2022, https://www.disinfo.eu/advocacy/tackling-disinformation-online-the-digital-services-act-opens-the-era-of-accountability/, [online: 29.06.2022].
32 K. Mikulski, *European Union*, [in]: *Europe vs disinformation: resilience building in selected countries*, Instytut Kościuszki, Kraków 2021, p. 16, https://ik.org.pl/wp-content/uploads/europe_vs_disinformation.pdf, [online: 29.06.2022].
33 *Ibidem*.
34 *Ibidem*.
35 StrategEast, Ukrainian Digital Resistance to Russian Aggression, 2022, p. 6, https://www.strategeast.org/all_reports/Ukrainian_Digital_Resistance_Report_web.pdf, [online: 29.06.2022].
36 *Ibidem*, p. 9.
37 *Ibidem*, p. 10.
38 *Ibidem*, p. 11.
39 PolitiFact, https://www.politifact.com/.
40 DebunkEU, https://debunk.eu/about-debunk/.
41 Full Fact, https://fullfact.org/about/.
42 R. Oshikawa, J. Qian, W. Yang Wang, *A Survey on Natural Language Processing for Fake News Detection*, 2020, https://aclanthology.org/2020.lrec-1.747/, [online: 29.06.2022].
43 *Ibidem*.
44 K. Wagner, *Facebook found a new way to identify spam and false news articles in your News Feed*, Vox, https://www.vox.com/2017/6/30/15896544/facebook-fake-news-feed-algorithm-update-spam, [online: 30.06.2022].
45 J. Cook, Building Resilience Against Misinformation Through a Cartoon Game, https://www.aaas.org/programs/center-public-engagement-science-and-technology/reflections/building-resilience-against, [online: 30.06.2022].
46 Get Bad News, https://www.getbadnews.pl/#intro, [online: 30.06.2022].
47 Fake News: The Game, https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/fake-news-the-game.html, [online: 30.06.2022].
48 Fake It To Make It, https://www.fakeittomakeitgame.com/, [online: 30.06.2022].

49 *Deklaracja końcowa szczytu NATO w Warszawie*, 9 July 2016 r., https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf, [online: 30.06.2022].
50 PO(2020)0189-Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria.
51 *Guide to Continuity of Government for State, Local, Tribal and Territorial Governments*, Federal Emergency Management Agency, July 2021, p. 4.
52 *Ibidem*, p. 3.
53 P. Zaskórski P., K. Szwarc, *Modelowanie procesów zapewniania bezpieczeństwa i ciągłości działania organizacji administracji publicznej*, http://sbn.wat.edu.pl/pdf-129871-56756?filename=MODELING%20OF%20THE%20PROCESSES.pdf, pp. 337–340, [online: 27.06.2022].
54 K. Pietryka, *Nowe technologie informacyjno-komunikacyjne w zarządzaniu kryzysowym*, [in]: Danielewska A., Maciąg K., eds., *Wybrane aspekty kryminologii, kryminalistyki i bezpieczeństwa w wymiarze narodowym i międzynarodowym*, Wydawnictwo Naukowe TYGIEL, Lublin 2021, p. 25.
55 *Managing uncertainty in government modeling*, https://www.turing.ac.uk/research/research-projects/managing-uncertainty-government-modelling, [online: 27.06.2022].
56 P. Zaskórski, K. Szwarc, *Modelowanie procesów…*, op. cit., p. 337.
57 Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity, p. 18.
58 Izabela Albrycht, the speech during the "State of emergency – securing ICT systems" seminar, https://youtu.be/SHRwsiMW3P4 [online: 28.06.2022].
59 P. Mell, T. Grance, The NIST Definition of Cloud Computing, *Special Publication 800-145*, National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, [online: 27.06.2022].
60 Defending Ukraine: Early Lessons from the Cyber War, a Microsoft report, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK, p. 5, [online: 27.06.2022].
61 K. Sikorski, *Ukraina przechowuje wrażliwe dane w Polsce w specjalnie zaprojektowanej chmurze. Chroni je przed cyberprzestępcami i rakietami wroga*, [online]: https://polskatimes.pl/ukraina-przechowuje-wrazliwe-dane-w-polsce-w-specjalnie-zaprojektowanej-chmurze-chroni-je-przed-cyberprzestepcami-i-rakietami/ar/c1-16435809, [online: 27.06.2022].
62 *The Ukrainian Digital Resistance to Russian Aggression*, https://www.strategeast.org/ukrainian-digital-resistance-to-russian-aggression-report/, [online: 27.06.2022].
63 P. Zaskórski, K. Szwarc, *Modelowanie procesów…*, op. cit., p. 353.
64 Directive (Eu) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
65 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
66 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
67 Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa sektora energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, Ministerstwo Klimatu i Środowiska, wrzesień 2021 r.
68 *IT vs OT Security: The Operational Technology Guide for Professionals*, https://www.otorio.com/blog/it-security-vs-ot-security-the-operational-technology-cybersecurity-guide-for-industry-professionals/, [online: 28.06.2022].
69 Scandanve XP, https://www.icsec.pl/scadvance/, [online: 28.06.2022].
70 *ISO/IEC 27001 Information Security Management*, https://www.iso.org/isoiec-27001-information-security.html, [online: 28.06.2022].
71 *Guide to Industrial Control Systems (ICS) Security*, National Institute of Standards and Technology, U.S. Department of Commerce, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final, [online: 28.06.2022].
72 *ISO 22301: 2019 Business continuity management system*, https://www.iso.org/standard/75106.html [online: 28.06.2022].

73 Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa sektora energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów, Ministerstwo Klimatu i Środowiska, wrzesień 2021 r.
74 *Cloud disaster recovery (cloud DR)*, https://www.techtarget.com/searchdisasterrecovery/definition/cloud-disaster-recovery-cloud-DR, [online: 28.06.2022].
75 J. Reed, *Disaster Recovery in Cloud Computing: All you need to know*, https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/, [online: 28.06.2022].
76 M. Kotas, *Media społecznościowe w zarządzaniu kryzysowym organizacji*, Uniwersytet Ekonomiczny w Katowicach.
77 *Virtual assistant launched to help Ukrainian refugees access key services in Czech Republic*, https://www.ibm.com/blogs/southeast-europe/virtual-assistant-launched-to-help-ukrainian-refugees-access-key-services-in-czech-republic/, [online: 28.06.2022].
78 *Ćwierć Miliona numerów PESEL dla obywateli Ukrainy!*, https://www.gov.pl/web/cyfryzacja/cwierc-miliona-numerow-pesel-dla-obywateli-ukrainy, [online: 28.06.2022].
79 *Ukraińcy mogą korzystać z aplikacji mObywatel. Co zrobić, by ją aktywować?*, https://www.portalsamorzadowy.pl/smart-city/ukraincy-moga-korzystac-z-aplikacji-mobywatel-co-zrobic-by-ja-aktywowac,362053.html, [online: 28.06.2022].
80 *Alert RCB – Najważniejsze Pytania i Odpowiedzi*, https://www.gov.pl/web/rcb/alert-rcb---najwazniejsze-pytania-i-odpowiedzi, [online: 28.06.2022].
81 Batista F., and Hirtzer M., *JBS Paid Hackers $11 Million After Hack Crippled Meat Plants*, https://www.bloomberg.com/news/articles/2021-06-09/jbs-paid-11-million-in-ransom-to-resolve-cyberattack-dj?sref=CIpmV6x8#xj4y7vzkg, [online:28 June 2022].
82 Magill J., *U.S. Water Supply System Being Targeted By Cybercriminals*, https://www.forbes.com/sites/jimmagill/2021/07/25/us-water-supply-system-being-targeted-by-cybercriminals/?sh=4fc9b32728e7, [online:28 June 2022].
83 Baryannisa G., Validib S.,Danib S., Antonioua G., Supply Chain Risk Management and Artificial Intelligence: State of the Art and Future Research Directions, International Journal of Production Research, 57:7, 2179-2202, DOI: 10.1080/00207543.2018.1530476, p. 1.
84 Treiblmaier H., *The impact of the blockchain on the supply chain: a theory-based research framework and a call for action*, Supply Chain Management: An International Journal, Vol. 23 Issue: 6, pp. 545-559, https://doi.org/10.1108/, p. 547.
85 Zhou Q., Zhang H., Wang S., *Artificial intelligence, big data, and blockchain in food safety*, International journal of food engineering, 18, 1-14. doi: 10.1515/ijfe-2021-0299, p. 10.
86 *What is the Impact of AI in the Food Supply Chain?*, https://adroitna.com/what-is-the-impact-of-ai-in-the-food-supply-chain/ [online:28 June 2022].
87 *Ibidem*.
88 2019 NATO Leaders' Meeting: In Brief, Congressional Research Service, November 27, 2019
89 Resilient communications, https://www.gov.uk/guidance/resilient-communications, [online:28 June 2022].
90 Ukrainian Digital Resistance to Russian Aggression, StrategEast Center for a New Economy, 2022
91 About 150,000 people in Ukraine are using SpaceX's Starlink internet service daily, government official says, [online]: https://www.cnbc.com/2022/05/02/ukraine-official-150000-using-spacexs-starlink-daily.html, [online:28 June 2022].
92 Innovation for emergency services and the military: 4G / 5G connectivity in crisis situations, https://www.is-wireless.com/news/innovation-for-emergency-services-and-the-military-4g-5g-connectivity-in-crisis-situations/, [online:28 June 2022].
93 Ukrainian Digital Resistance to Russian Aggression, StrategEast Center for a New Economy, 2022
94 Thales, Verint, report entitled The Cyberthreat Handbook, 2019, https://www.thalesgroup.com/en/group/journalist/press-release/cyberthreat-handbook-thales-and-verint-release-their-whos-who, [online: 29.06.2022].
95 I. Eusgeld, C. Nan, S. Dietz, "System-of-systems" approach for interdependent critical infrastructures, Reliability Engineering and System Safety, 96(2011) 679–686.
96 https://home-affairs.ec.europa.eu/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resiliance_en [online: 28.06.2022].

The Kosciuszko Institute is a leading non-governmental non-profit research and exploration centre established in 2000. Our mission is to work towards social and economic development and security of Poland as an active member of the European Union and NATO. The Institute specialises in providing strategic recommendations and directions of development for key public policies to serve as actionable support for Polish and European political decision-makers. The Kosciuszko Institute is the initiator and main organiser of the European Cybersecurity Forum – CYBERSEC, an annual conference dedicated to strategic aspects of cyberspace.

ik.org.pl InstytutKosciuszki @ikosciuszki Instytut Kosciuszki

REPORT PARTNER PATRONAGE

© The Kosciuszko Institute 2022