FUTURE-PROOFING CYBERSECURITY: LEVERAGING STRATEGIC FORESIGHT TO ENHANCE RESILIENCE

Carola FREY
Strategic Analysis and Cooperation Department, Euro-Atlantic Resilience Centre Bucharest, Romania
carola.frey@e-arc.ro

Abstract: This paper examines the application of strategic foresight to enhance cyber resilience against evolving digital threats. The first section looks into the evolution and origins of foresight, tracing its development and significance. The study employs methods such as STEEP analysis, the high-impact high-probability tool, and the 2x2 matrix, applying them to the cyber domain to evaluate their effectiveness as instruments for building resilience. By leveraging strategic foresight, this paper aims to provide actionable insights and improve preparedness for potential cyber threats, ultimately contributing to a more secure and resilient digital ecosystem.
Keywords: Strategic Foresight, Cyber Resilience, Cyber Security, Digital Landscape, Resilience.

INTRODUCTION

This era is characterized by unprecedented yet eagerly anticipated digital interconnectivity that saturates every aspect of modern society. This extensive reliance on digital systems has elevated cybersecurity to a critical priority. As a result, states are enacting national laws and policies, international bodies are establishing norms, regulations and standards, with cybersecurity as a focal point of their activities. It has also become a new domain in which diplomats must become proficient, alongside data, AI and other emerging technologies.

The continuous advancement of cyber threats, driven by AI systems, along with emerging capabilities, vulnerable critical infrastructure, and significant societal implications, demands not only reactive measures but also a proactive, forward-thinking approach to ensure the resilience of these critical systems, which profoundly impact the current way of life. The main concern of cybersecurity is the potential for major, unexpected, or unpreventable disruptions of essential systems and services – critical infrastructures – that could have severe, even catastrophic, consequences for society. Thus, cyber resilience has emerged as a "sister concept" alongside cybersecurity. It aims to enhance the prevention of cyber incidents with strategies that minimize the impact of successful attacks and ensure the continuity of essential services post-attack (Dunn et al., 2023).

Cyber incidents, threats, attacks, etc. are a current concern and will remain highly relevant in the future. The concentrated efforts to prevent them must be complemented by an emphasis on resilience. This requires a forward-looking approach, anticipating how cyber threats may evolve, their characteristics, and how other domains or technologies might contribute to or mitigate these incidents (Flammini, 2019). This "looking ahead" endeavor in order to "bounce forward" (Russpatrick, Amarakoon & Hedberg, 2023) does not confine the understanding to a single future scenario but instead encompasses a broad array of potential futures influenced by the decisions today, or the lack thereof (Zumbrunn, 2023). This approach is akin to a digital

twin reality, allowing for stress testing of various hypotheses or variables. Consequently, this exploration can turn uncertainties into informed possibilities. Furthermore, it allows for the exploration of ways to tackle challenges and identify opportunities over time. It includes detecting "gray rhinos" – highly probable yet often ignored threats (Wucker, 2016) – and understanding how different strategies can lead to optimal outcomes. Thus, strategic foresight, and foresight methodologies over all, can be a solution to enhance cyber resilience, by setting priorities, identifying knowledge gaps, and dealing with uncertainties.

The objective of this paper is to propose strategic foresight as an instrument to enhancing cyber resilience. In the first section, a review of the existing literature on what foresight is and how it is applied will be conducted. This review will include authored books, academic articles, government and international organizations reports, and analyses by think tanks. The purpose of this review is to identify key methodologies and examine their applications, whether within the realm of cyber or other areas. The focus at this stage is to understand how these methodologies operate. Thus, through the utilization of content analysis of relevant documents and the observation of case studies and their applications, valuable insights can be gained into how foresight generates pertinent information for building resilience, particularly focusing applications within the cyber domain.

The second section will implement a commonly used scenario planning technique – the 2x2 matrix – which, in this case, but not only, offers three distinct benefits. First, it facilitates systematic thinking about future changes. Second, it fosters an understanding of how potential future changes may impact current strategies, laws, standardizations and practices. Third, it allows for a re-evaluation of the current situation, uncovering new possibilities. These benefits collectively highlight approaches to addressing resilience and constructing cyber resilience.

The 2x2 matrix will be constructed based on a high-impact, high-probability chart developed through a STEEP analysis of the field. The objective of scenario development in this context is to create multiple future scenarios to better understand potential cyber threats and assess their implications. Furthermore, insights will be gathered through a number of expert interviews and discussions at relevant conferences, drawing on the expertise of cybersecurity professionals. This approach aims to provide a nuanced understanding of the evolving cyber threat landscape and inform strategies for enhancing resilience.

The primary goal of directly applying a foresight methodology is to illustrate how it can enhance cyber resilience and demonstrate the practical application, to provide a detailed examination of it can be leveraged to anticipate and mitigate potential cyber threats, thereby improving the overall resilience. The limitations will be acknowledged and discussed, as these methodologies are not a universal panacea.

Finally, further research directions will be outlined based on the current findings. The goal is to contribute to the academic discourse on cyber resilience and to provide actionable insights for practitioners in the field.

UNDERSTANDING STRATEGIC FORESIGHT AND HOW IT CAME TO BE

In the literature, there are some commonly identified terms that may be encountered in the exploration of alternative futures. These include future studies, forecasting, future knowledge, anticipation, prediction, foresight analysis, foresight, strategic foresight, futurism, futurology, and others. These terms are frequently used interchangeably and, in many instances, inaccurately (Fergnani, 2020). Certain concepts lack precise definitions, and in some contexts, terms are treated as synonyms, depending on the school of thought or the practitioner employing them. Additionally, these concepts have been utilized by both the military/political sector and the private sector, each of which has developed its own distinct terminology system.

Strategic foresight, in a nutshell, is the systematic and multidisciplinary approach that involves analyzing potential outcomes that can shape society, technology, the economy, and the evolution of international relations. This method generates insights into the dynamic and complex nature of the international system, aiding governments in decision-making, strategy formulation, resilience building, and future preparedness. Foresight involves examining and anticipating potential future developments to shape a desirable future. Rather than attempting to predict the future, strategic foresight investigates various possible scenarios and the opportunities and challenges they may bring (*Strategic Foresight*, no date)

Originating from the pioneering work of Gaston Berger, the field foresight began to take shape in the mid-20th century. Berger's vision emphasized the importance of long-term thinking and the systematic examination of possible futures. This field emerged in response to growing concerns about the profound impacts of technological progress and social changes on society. The development of this domain was driven by the need to understand and manage the complex interplay of factors shaping the future (Berger, 1957).

Key figures in the establishment of foresight include Herman Kahn, known for his work on scenario planning and systems analysis; Olaf Helmer, who co-developed the Delphi method for expert forecasting (Helmer, 1983); Michel Godet, who advanced the field with his work on strategic anticipation and scenario planning (Godet, 2001); Jacques Lesourne, who integrated economic analysis into future studies (Lesourne & Stoffaës, 1996); Hugues de Jouvenel, who contributed to the development of prospective analysis (de Jouvenel, 2019); Wendell Bell, who emphasized the sociological aspects of future studies (Bell, 2009); and Theodore Gordon, who focused on the use of quantitative methods in forecasting (Gordon & Helmer, 1964).

Rooted in political science and sociology, foresight gained recognition between the end of World War II and the beginning of the Cold War. From relevant academic sources, it can be deduced that the origins of this field trace back to the 1940s and 1950s. Scholars such as Flechtheim (1966), Jungk (1969), and Nanus (1984) argue that these studies concretized in the 1940s, while Henshel (1981), Helmer (1970), Jouvenel B. (1967) identify the emergence of theories between 1950 and 1960. Maruyama (1978) contends that a precise date cannot be established, as the field formed over two decades starting in 1958.

Among the earliest seminal works in this field are Harrison Brown's "The Challenge of Man's Future" (1954), Frederik Polak's "The Image of the Future" (1961), Bertrand de

Jouvenel (1967) and Herman Kahn's two influential works, "On Thermonuclear War" (1960) and "Thinking about the Unthinkable" (1962). Dennis Gabor's "Inventing the Future" (1964) also stands out. The 1970s and 1980s saw notable contributions such as Alvin Toffler's "Future Shock" (1970), John Naisbitt's "Megatrends" (1984), and Dennis Gabor's "The Mature Society: A View of the Future" (1972). Winthrop's 1968 analysis, "The Sociologist and the Study of the Future," presents foresight as a sub-discipline of sociology (Winthrop, 1968). Huber and Bell (1971) discuss the rise of foresight as integral to the future of sociology, while Bell and Mau (1971) highlight sociologists' efforts to prioritize these types of methodologies.

These debates were gradually reconsidered in the mid-1990s, not before American sociologist Gilfillan proposed the idea of interdisciplinarity, emphasizing the importance of formulating alternative scenarios based on deep historical knowledge and caution in extrapolations (Ballandonne, 2020). Sociologist Ogburn contributed to the development of a contemporary approach focusing on trend analysis and the role of technology in social change, providing a conceptual and methodological foundation for studying technological innovation (Ogburn, 1933).

In his 1961 work "The Image of the Future" Polak examines how images of the future can contribute to understanding the processes of evolution and dissolution in human societies, highlighting the importance of actively shaping the future (Polak, 1961). Gabor's "Inventing the Future" posits that while the future cannot be precisely predicted, various futures can be invented. He argues that although exact predictions are impossible, humans have the power to shape and create alternative futures, emphasizing the role of human awareness in determining the course of events (Gabor, 1964).

In France during the 1960s, influential figures like Gaston Berger, Bertrand de Jouvenel, and Pierre Massé significantly contributed to the development of the field (Goux-Baudiment, 1997). During the same period, foresight courses emerged at institutions like the New School for Social Research (taught by Alvin Toffler), Yale University (taught by Wendell Bell), Virginia Polytechnic Institute (offered by Jim Dator), and Rikkyo University in Japan. Numerous associations, clubs, and institutions, including the Club of Rome, RAND Corporation, and Futuribles, were established across various countries. The RAND project and the French school of prospective are considered the two foundational sources of strategic foresight as noted by Rohrbeck, Battistella, and Huizingh (2015).

In the 1970s, strategic foresight was characterized by global discussions focusing on global futures, normative future developments, and a deeper integration into the private sector. Dror argued that these studies could significantly contribute to strategic management, inspiring new mindsets and providing necessary information for decision-making (Dror, 1970). Tolon observed that future studies during the Cold War emphasized strategic thinking, employing methods like modeling, game theory, and the Delphi method (Tolon, 2012). In the communist bloc, foresight was part of the centralized state mechanism, aiming to assess threats and risks from the Cold War conflict and potential future scenarios using Kahn's scenario method (Millett, 2003). Over time, the subjects expanded beyond government and military domains to include technology, sociology, economics, and environmental

sustainability, notably through the 1972 report "The Limits to Growth" supported by the Club of Rome. Additionally, in 1972, the Shell Group introduced foresight methods in the corporate sector, exploring the possibility of a crisis (Heijden, 1996) Possible images of future societies became a primary research theme, focusing on technological development, with private companies incorporating future vision as an essential part of their planning process (Linneman & Klein, 1979).

The increasing uncertainty, dynamics, complexity, and ambiguity, along with the challenges posed by globalized markets, brought the strategic importance of foresight back into international focus in the 1980s and 1990s (Rohrbeck, Battistella & Huizingh, 2015). During this period, it matured into a well-defined discipline. The history of this discipline is detailed in numerous publications, revealing the assumptions and viewpoints of key figures and institutions (Marien & Jennings, 1987; Coates & Jarratt, 1989).

Post-1990, foresight experienced stagnation and fragmentation, with foresight mainly applied by the private sector. Prominent authors of this period include Slaughter (Slaughter 1995, 1996a, 1996b, 2002a, 2002b) and Inayatullah (Inayatullah, 1998, 2002). The fragmentation after the Cold War made it impossible to reach a consensus on the definition and purpose. Foresight have been applied differently across regions, with varying terminologies, sometimes not even considered a standalone discipline.

Starting around 2012-2015, the academic community renewed its interest, evidenced by an increase in publications and deeper exploration of methods, theory, and empirical research. Notably, several institutes and organizations established during the discipline's development have persisted without significant changes (RAND, Institute for the Future founded in 1968, Centre for Strategic Futures, Institute for Futures Studies, etc.) Additionally, new organizations and centers, such as the School of Future Studies in Singapore (unique intellectual framework, that includes key institutions like the Centre for Strategic Futures in the Prime Minister's Office and the National University of Singapore), have emerged.

In the current context, foresight has experienced a strong resurgence and have become a major concern in facing increasingly complex and uncertain challenges. The concept of resilience has become closely intertwined with it, focusing on the ability of systems and communities to adapt and cope with major disruptions and changes. Resilience involves not just surviving problems but also learning from experiences, reorganizing, and evolving to become stronger and more adaptable. In this sense, foresight plays a crucial role in identifying emerging trends and potential risks and threats, providing valuable information for policy formulation, decision-making, and strategic planning.

The COVID-19 pandemic and the war in Ukraine—both significant structural challenges—have elevated both the concept of resilience and the practice of foresight to new heights. These events, along with numerous other issues, underscore the critical need for heightened vigilance and foresight. Day and Schoemaker (2021) emphasize that strategic foresight has become indispensable for companies, particularly in sectors where private entities hold a monopoly, such as technology and cybersecurity. The unprecedented disruptions caused by these crises have underscored the importance of anticipating future challenges and developing robust

strategies to address an increasingly volatile and uncertain environment, often described by the acronyms VUCA (volatile, uncertain, complex, and ambiguous) or TUNA (turbulence, uncertainty, novelty, and ambiguity).

Just like VUCA and TUNA are part of the lexicon of foresight, so are "black swans" and "gray rhinos". Coined by Nassim Nicholas Taleb (2007), a "black swan" refers to an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. These events are characterized by their extreme rarity, severe impact, and the widespread insistence they were obvious in hindsight. On the other hand, the term "gray rhino", introduced by Michele Wucker (2016), describes highly probable, high-impact but still neglected threats.

"Black swans" highlight the need for institutions to build robust systems that can withstand unforeseen shocks, emphasizing the unpredictability inherent in the modern world. "Gray rhinos", meanwhile, stress the importance of recognizing and addressing obvious risks before they escalate into crises. This is particularly relevant to cyber resilience, where both types of threats must be managed proactively. Cyber resilience involves not only preparing for and responding to unexpected cyberattacks (black swans), but also addressing known vulnerabilities and risks (gray rhinos) to prevent them from becoming significant issues. By integrating these concepts into their cybersecurity strategies, the ability to protect against, respond to, and recover from a wide range of cyber threats is amplified, thereby ensuring more robust and comprehensive security measures.

In the present day, strategic foresight is experiencing a reinvention and revival, applied across a wide spectrum by states, international organizations, the private sector, think tanks, and academia. This resurgence reflects the growing recognition of its importance. For instance, Finland's Committee for the Future, established by the Finnish Parliament, engages in extensive foresight activities to guide national policy-making. Similarly, Singapore's Centre for Strategic Futures operates under the Prime Minister's Office, conducting foresight to enhance the nation's resilience and adaptability to future challenges. Furthermore, the United Nations has adopted foresight through initiatives like the UN Global Pulse, which leverages big data for real-time analytics to anticipate and respond to global crises. Additionally, the European Union employs foresight in its policy-making processes through the European Strategy and Policy Analysis System (ESPAS) and Joint Research Centre (JRC), which provides forward-looking insights to support long-term strategic planning.

In the private sector, companies like Shell and Siemens have long-standing foresight units to anticipate energy market shifts and develop sustainable business strategies and to drive innovation and long-term planning within the company. Tech giants such as Google and Microsoft utilize foresight to stay ahead of technological advancements and cybersecurity threats. Microsoft's Cybersecurity Defense Operations Center exemplifies the integration of foresight in cyber resilience, enabling the company to preemptively address potential cyber threats and protect its digital infrastructure.

APPLYING FORESIGHT TO THE CYBER REALM

For the purpose of this paper, strategic foresight will be defined as a systematic process employed by actors to envision multiple future scenarios and develop strategies to prepare for potential outcomes. Unlike traditional forecasting, which often relies on linear projections based on historical trends, strategic foresight embraces uncertainty and complexity by considering a range of possibilities and the interactions among various variables. This approach facilitates more adaptable and resilient planning, which is essential in fields like cybersecurity, where the landscape is continually evolving. Cyber threats are not only increasing in number but are also becoming more sophisticated and harder to predict. Traditional security measures, while necessary, are often reactive and insufficient in the face of evolving threats. In this context, it is felt a need for a proactive approach that can anticipate future risks and prepare accordingly.

Strategic foresight, with its holistic view, considers a wide range of factors – technological, economic, social, political, etc. – that could impact future scenarios. This approach is particularly valuable also in the face of rapid evolution of technology. Technologies such as artificial intelligence (AI), blockchain, and quantum computing can introduce both opportunities and vulnerabilities. For instance, AI can enhance cybersecurity through advanced threat detection, but it can also be used by adversaries to develop more sophisticated cyberattacks. The implementation of 5G (and maybe sooner than expected 6G) networks promises to revolutionize communications with faster speeds, lower latency, and the capacity to support a massive number of connected devices. This can facilitate the development of smart cities, autonomous vehicles, and enhanced telemedicine, among other innovations. However, the increased connectivity and reliance on 5G infrastructure will introduce new security challenges. The complexity of 5G networks, combined with their distributed nature, makes them more difficult to secure. There is also the risk of state-sponsored attacks targeting critical 5G infrastructure, which could have widespread consequences for national security and economic stability.

More importantly, the shift to biometric authentication methods such as fingerprint, facial recognition, and iris scanning, while offering more secure and convenient alternatives to traditional passwords, can lead to the theft of such data, which can be more damaging than password breaches because biometric identifiers are immutable. In addition, sophisticated spoofing techniques can sometimes circumvent biometric security measures, and there are concerns about privacy (Chassidim et al., 2021) and the potential misuse of biometric data by malicious actors or authoritarian regimes (Nebreda, 2023).

Strategic foresight can incorporate dual aspects of emerging technologies, ensuring that while their benefits are harnessed, appropriate safeguards and resilience measures are also put in place to mitigate associated risk. Furthermore, it can anticipate future trends, identify actionable steps, and recognize potential wild cards or game changers that could significantly impact the landscape.

The STEEP (Social, Technological, Economic, Environmental and Political) is a foresight method that can be used to understand developments in cyber resilience and security. By examining these five external factors, STEEP offers a comprehensive view of the influences shaping the field. This approach helps identify key drivers and trends, which can then inform

the development of strategic directions for enhancing cyber resilience. The insights gained through this method can be effectively illustrated using tables (see Table 1 and Table 2)

Table 1. STEEP analysis

STEEP digital ecosystem analysis: identification of key drivers with a focus on cyber	
Social	increased digital dependency, public awareness and behavior, demographic shifts, remote work trends, digital literacy and education, new social engineering tactics, online privacy concerns, difference in cybersecurity policies, privacy, digital divide, trust, attitudes towards legal frameworks, increased Internet penetration.
Tech	AI and machine learning, cloud computing, cyber-physical system, encryption technologies, AI-driven threats, Digital Twin, New generation Firewalls, wearable technology, network architecture, IoT, 5G, Edge Computing, Autonomous Systems.
Environmental	cyber threats to critical infrastructure, water management systems, agricultural cybersecurity, transportation networks, biodiversity monitoring, supply chain vulnerabilities, smart cities, climate change.
Economic	cost of cyber incidents, investment, market valuation impact, operational downtime, intellectual property theft, cost of public sector cybersecurity, economic incentives, cybersecurity audit, R&D investments, compliance, data breaches, cybersecurity-as-a-service, Virtual Reality cyber training facilities, increasing cost and complexity of future systems.
Political	frameworks, data flow regulations, strategies, research and innovation, economic espionage, workforce development, disinformation campaign and hybrid threats, surveillance and privacy debates, cyber sanctions, PPP, election security, digital sovereignty, cyber diplomacy, cyber warfare

From the STEEP analysis table, a series of cyber resilience solutions can be identified.

Table 2. Solutions drawn from the STEEP analysis

Cyber resilience solutions	
Adaptive security architecture	implementing a dynamic security framework that evolves with emerging threats, incorporating AI and machine learning to predict and respond to attacks in real-time.
Quantum-resistant cryptography	developing and adopting cryptographic methods that are resistant to the computational power of future quantum computers.
Zero trust security model	implementing a Zero Trust architecture where no user or device, inside or outside the network, is trusted by default. Continuous verification and least privilege access are key components.
Integrated threat intelligence	utilizing threat intelligence platforms that aggregate data from multiple sources to provide real-time analysis and actionable insights for proactive threat management.
Enhanced user education and training	conducting regular cybersecurity awareness programs and simulations to train users on recognizing and responding to cyber threats effectively.
Resilient network design	designing networks with redundancy, segmentation, and robust backup systems to ensure operational continuity in the event of a cyber incident.
Incident response and recovery plans	developing comprehensive incident response strategies that include regular drills, clear communication protocols, and post-incident recovery plans to minimize downtime and data loss.
Public-Private Partnerships	encouraging collaboration between government agencies and private sector entities to share information, best practices, and resources to combat cyber threats collectively.
Cyber diplomacy	promoting international cooperation and dialogue on cybersecurity issues through cyber diplomacy. This involves engaging with other nations to develop global norms, standards, and agreements that enhance collective cyber resilience. By fostering relationships and trust among countries, cyber diplomacy aims to create a more secure and stable cyberspace, facilitating the sharing of threat intelligence and best practices on a global scale.

When the trends from the STEEP analysis are included in a high impact, high probability chart, it facilitates a comprehensive evaluation of the current situation, with a focus on future perspectives and potential impacts. In such a chart, each trend will be evaluated based on its uncertainty and probability.

To explore the potential impact of increased digital dependency and cyber warfare on global security strategies by 2030 (noting that various combinations based on all identified drivers could be examined), the 2x2 scenario planning matrix was employed. The primary question addressed was: "*how will the increase in digital dependency and cyber warfare impact global security strategies by 2030?".* The analysis identified two key drivers: digital dependency

and cyber warfare. At its maximum development, digital dependency envisions high reliance on digital technologies across all sectors, whereas at its minimum, it anticipates low reliance and slow adoption rates. For Driver 2, representing cyber warfare, maximum development would involve frequent and sophisticated cyber-attacks, while minimum development would involve rare and low-impact cyber-attacks (see Figure 1).

The resulting scenarios can be summarized as follows:

1. **Scenario 1: high digital dependency/low cyber warfare** – organizations and all sectors exhibit a high adoption of digital technologies. Cyber-attacks are infrequent, and existing technologies are well-prepared to handle these threats. Consequently, there is a strong emphasis on improving digital infrastructure and expanding digital services.
2. **Scenario 2: high digital dependency/high cyber warfare** – there is a high adoption of digital technologies across all sectors, accompanied by frequent and highly sophisticated cyber-attacks. Consequently, there is a significant focus on advanced cybersecurity measures to protect against these threats, reflecting the high dependency on digital technologies
3. **Scenario 3: low digital dependency/low cyber warfare** – organizations and individuals have a low reliance on digital technologies, with cyber-attacks being infrequent and less sophisticated. Consequently, cybersecurity measures are basic, with a primary focus on physical security.
4. **Scenario 4: low digital dependency/high cyber warfare** – organizations and individuals have a low reliance on digital technologies. However, cyber-attacks are frequent and highly sophisticated, necessitating significant investment in defensive cybersecurity measures to protect critical assets.

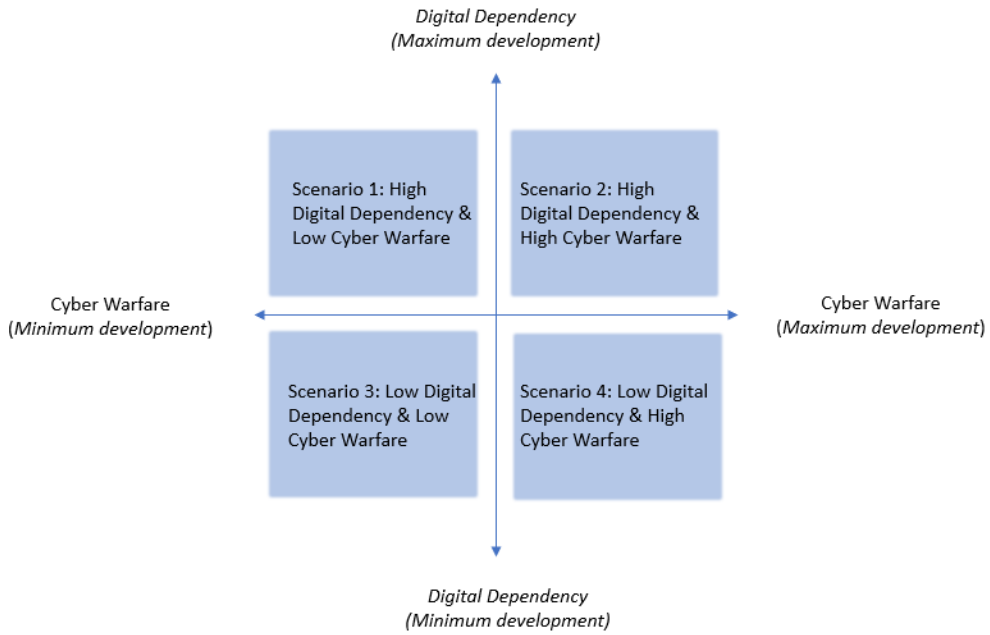

Figure 1. 2x2 Matrix

The following scenarios are developed to analyze trajectories and specific elements of their context, such as vulnerabilities, opportunities, and resilience measures. The analysis is not intended to be exhaustive and will focus on detailing the first two scenarios to demonstrate the utility of this instrument. Additionally, these scenarios are designed to be iterative and adaptable, allowing for continuous improvement. Experts can contribute further ideas and perspectives, thereby adding layers and depth to the scenarios. This approach can also be a part of international cooperation, as experts from different nations can contribute and add significant value.

Scenario 1.

The most notable aspect of this scenario is the widespread use of digital tools and platforms across all sectors. Digital technologies are embedded in daily operations. Infrequent cyber-attacks further define this scenario. The low incidence of cyber threats suggests that current cybersecurity measures are highly effective in mitigating potential risks. This relative safety from cyber-attacks allows organizations to focus on leveraging digital technologies for growth and development without constant concern over cyber threats. A significant emphasis on digital infrastructure is another key characteristic. Continuous investment in upgrading and expanding digital infrastructure is evident, as organizations seek to improve efficiency, accessibility, and service delivery. The development of robust digital services aims to enhance user experience and operational capabilities across sectors. Preparedness for cyber threats is also a defining feature. Despite the low frequency of cyber-attacks, technologies and systems are maintained at high standards to handle occasional threats. Regular updates and maintenance of cybersecurity protocols ensure that systems remain resilient and secure against potential cyber incidents.

Despite the positive aspects of this scenario, several vulnerabilities need attention. One major concern is complacency in cybersecurity. The infrequency of cyber-attacks might lead to complacency, causing organizations to neglect necessary upgrades and maintenance of cybersecurity measures. It could result in underestimation of emerging cyber threats, leaving systems vulnerable to future attacks. Another vulnerability is the overreliance on digital systems. High dependency on digital technologies poses risks if systems fail or are disrupted. Without robust contingency plans, organizations may face significant challenges in the event of digital system failures or unexpected cyber incidents. Data privacy concerns also emerge as a vulnerability in this scenario. With increased digital activity, there is a heightened risk of data breaches despite the infrequency of cyber-attacks. Ensuring data privacy and protection remains a critical challenge that organizations must address to maintain trust and security.

In parallel, several opportunities present themselves. One significant opportunity is the enhancement of digital services. The focus on improving digital infrastructure allows for the innovation and development of new digital solutions. Expanding digital offerings can reach a broader audience, improving user experience and operational efficiency. Economic growth is another opportunity. Improvements in digital infrastructure drive economic growth and competitiveness, creating new business opportunities and markets through digital innovation. The integration of digital technologies can lead to the development of new industries and economic sectors. Improved efficiency and productivity are also key opportunities. The

increased use of digital technologies can streamline processes and operations, enhancing overall efficiency and productivity across sectors. This digital transformation can result in significant time and cost savings for organizations

Building resilience in this scenario involves several key elements. Robust cybersecurity measures are an important cornerstone. Regular assessment and upgrading of cybersecurity protocols ensure that systems remain prepared to handle potential threats. Investment in advanced cybersecurity technologies and skilled personnel is essential for maintaining a secure digital environment. Comprehensive risk management is another element of resilience. Developing contingency plans and backup systems can mitigate risks associated with digital dependency. Ongoing risk assessments help identify and address vulnerabilities, ensuring that organizations remain resilient in the face of potential disruptions. Continuous improvement of digital infrastructure is also vital.

A commitment to ongoing improvement and expansion of digital infrastructure ensures its resilience. Redundancy and robust design can help prevent and mitigate disruptions, maintaining the integrity of digital systems. Awareness and training programs are essential for fostering resilience. Regular training for employees and stakeholders on cybersecurity best practices promotes awareness of digital risks and appropriate response strategies. This proactive approach ensures that individuals are prepared to handle potential cyber threats.

International cooperation is also highly relevant in this context, as cyber threats do not recognize national boundaries. Collaborative efforts between nations can enhance the effectiveness of cybersecurity measures through the sharing of intelligence, best practices, and technological advancements. Establishing and adhering to international cybersecurity standards can create a unified approach to threat mitigation, ensuring a higher level of security. Such cooperation can also facilitate quicker responses to emerging threats, as coordinated actions and shared resources can significantly improve the resilience of global digital infrastructure. By working together, countries can build a more secure and robust digital environment, safeguarding against cyber threats that transcend borders and ensuring the continued growth and development of digital technologies worldwide.

Scenario 2.

In this scenario, the most prominent aspect is the extensive adoption of digital technologies across all sectors, accompanied by frequent and highly sophisticated cyber-attacks. This scenario underscores the need for advanced cybersecurity measures due to the high dependency on digital technologies and the persistent threat landscape.

A characteristic of this scenario is the pervasive integration of digital technologies in daily operations. Digital platforms and tools are fundamental to business processes, public services, and individual activities. The digital transformation is present through all aspects of society, driving efficiency, innovation, and connectivity. However, the high frequency of cyber-attacks introduces a constant threat to the stability and security of these digital systems.

In this scenario, there is a significant emphasis on advanced cybersecurity measures. Organizations and governments invest heavily in developing and deploying cutting-

edge cybersecurity technologies to defend against the sophisticated tactics used by cyber adversaries. Continuous monitoring, threat intelligence, and proactive defense strategies are components of cybersecurity frameworks. The high threat level demands constant vigilance and rapid response capabilities to mitigate potential damages from cyber incidents.

The continuous investment in digital infrastructure remains key. Organizations strive to enhance the robustness and resilience of their digital assets. Upgrading and expanding digital infrastructure ensures that systems can withstand cyber-attacks and continue to operate effectively. Redundancy, encryption, and secure design principles are integral to maintaining the integrity of digital services.

Despite the focus on advanced cybersecurity measures, several vulnerabilities are inherent in this scenario. One major concern is the potential for security fatigue. The relentless nature of cyber threats can lead to burnout among cybersecurity professionals and complacency in maintaining rigorous security practices. This fatigue can result in gaps in defenses and increased susceptibility to attacks. Another significant vulnerability is the complexity of digital ecosystems. The intricate and interconnected nature of modern digital systems can create unforeseen security weaknesses. As organizations integrate new technologies and expand their digital footprints, the attack surface grows, providing more opportunities for cyber adversaries to exploit vulnerabilities. The high dependency on digital technologies also poses risks related to operational continuity. Cyber-attacks targeting critical infrastructure can disrupt essential services, causing widespread impacts on society and the economy. Ensuring the resilience of digital systems against such disruptions is a dominant concern.

Despite these challenges, several opportunities are part of this scenario. One notable opportunity is the advancement of cybersecurity innovation. The constant threat environment drives research and development in cybersecurity technologies, leading to breakthroughs in defense mechanisms and threat detection. This innovation not only enhances security but also fosters economic growth within the cybersecurity industry. Another opportunity is the strengthening of international collaboration. The global nature of cyber threats necessitates cooperative efforts among nations to combat cyber adversaries. Sharing threat intelligence, best practices, and resources can bolster collective defense capabilities and reduce the impact of cyber warfare. Improved public awareness and education manifests as contributing. As cyber-attacks become more prevalent, there is a growing recognition of the importance of cybersecurity and cyber resilience. Education initiatives and awareness campaigns can empower users to adopt secure practices and contribute to a safer digital environment.

Building resilience in this scenario involves robust cybersecurity measures. Continuous investment in advanced technologies, skilled personnel, and threat intelligence ensures that defenses remain effective against evolving threats. Regular assessments and updates to security protocols are essential for maintaining a strong security posture. Developing and testing contingency plans, backup systems, and incident response strategies help mitigate the impact of cyber-attacks. Organizations must be prepared to quickly recover from disruptions and restore normal operations. Investing in resilient and secure infrastructure designs minimizes vulnerabilities and enhances the ability to withstand cyber-attacks. Implementing redundancy and failover mechanisms ensures the continuity of critical services.

International cooperation and joint directives, such as the Network and Information Security Directive (NIS2) in the European Union, could play a role in addressing the global nature of cyber threats. Other examples include the Budapest Convention on Cybercrime and the UN's Open-ended Working Group on developments in the field of information and telecommunications in the context of international security. Cyber diplomacy, which involves international collaboration and policy-making, is essential in this scenario. It enables nations to share intelligence, establish common standards, and support each other in developing cybersecurity capabilities. Since national legislation alone may not be sufficient – particularly when countries are at different stages of digitalization – international standards and cooperation help bridge these gaps. Information sharing among countries enhances situational awareness, enabling a more coordinated and effective response to cyber threats.

Another layer that can be added to this analysis to enhance resilience is wind tunneling, a method used to simulate and test current strategies and policies against various scenarios. Wind tunneling helps evaluate how well these strategies would integrate and perform in specific situations, thereby identifying potential weaknesses and areas for improvement. Additionally, conducting a stakeholder analysis can identify the roles and actions of various actors within these scenarios, providing insights on where to intervene and what measures to implement for optimal effectiveness. These types of foresight methodologies can be implemented not only at the national level but across all levels, including regional and international. They can bring together different states and their expertise and lessons for a comprehensive approach and a common view or direction. If a common direction is not possible, they can at least foster discussions that can bring new ideas and possibilities.

For example, a foresight workshop could be used to simulate a large-scale cyber-attack scenario involving multiple countries. By doing so, each country can test its response strategies, identify gaps, and improve its policies. This collaborative approach can highlight the interdependencies between states and the need for synchronized responses to global threats. Similarly, stakeholder analysis can be employed to understand the roles of various international actors, such as government, private sector companies, and non-governmental organizations (NGOs), in a cyber incident. By mapping out these roles, countries can better coordinate their efforts and ensure that all relevant parties are prepared to act efficiently in a crisis.

In terms of cyber diplomacy, these methodologies can significantly enhance international cooperation. By engaging in foresight workshops countries can foster a shared understanding of cyber threats and develop collective strategies to address them. Moreover, international organizations can (and do so in recent period) utilize these methods to promote resilience among their members. By conducting joint strategic foresight, these organizations can identify best practices and develop standardized protocols that member states can adopt. This not only enhances individual country resilience but also strengthens the overall security posture, while advancing cyber diplomacy.

CONCLUSION

Foresight methodologies offer several advantages in strategic planning. However, over-reliance on any single tool can be problematic or restrictive if the specific limitations of that instrument are not acknowledged. Addressing these limitations enhances the effectiveness of foresight, as it is understood that foresight alone cannot encompass all aspects of cyber resilience strategies.

One significant limitation is that cyber threats are complex, dynamic, and highly adaptable to changing circumstances. They resemble a living organism, continuously evolving within a specific context. A one-size-fits-all approach will never be effective and cannot anticipate certain cyber-attacks, particularly those utilizing novel tactics or technologies, as the cyber domain is characterized by its own elements of innovation and creativity. Additionally, the possibility of delayed attacks further complicates the situation. Their unpredictability makes it challenging to develop comprehensive and foolproof strategies.

Scenario planning, such as the use of the 2x2 matrix, is effective for exploring possible futures. However, it has inherent risks, including over-reliance on specific scenarios and the potential for generating an excessive number of situations. While this variability can be beneficial, an overemphasis on preferred outcomes may lead to a narrow focus, causing some actors to overlook other potential developments. This limitation is nuanced, as foresight is inherently flexible. Scenarios should be designed to incorporate new information and emerging trends, even those that may never materialize or apply to future contexts. The primary goal is to identify actionable strategies and measures that support informed decision-making in practice, serving as a foundation rather than a definitive blueprint.

As with any information-based approach, the effectiveness of foresight methodologies largely depends on the quality and comprehensiveness of the data used, as well as the diversity of experts and viewpoints involved. Data limitations, biases, and homogeneous perspectives can negatively impact analyses and lead to inaccurate predictions. Similarly, incomplete or outdated data can be equally detrimental. Ensuring diverse perspectives and up-to-date, comprehensive data is the first step into obtaining reliable foresight.

Even when data is current and the results are insightful or innovative, a major challenge arises when translating foresight insights into practical, actionable strategies. Integrating foresight outcomes into existing frameworks and operational plans is difficult, particularly when it involves changes in policies, procedures, and technologies. This translation from insight to action can be a significant obstacle, impeding the effective implementation of the finding of foresight methodologies.

An opportunity in cyber diplomacy exchanges and information sharing, which forms the basis of some foresight methodologies, can also present challenges. When cyber threats transcend national borders, foresight must account for interdependencies and integrate diverse perspectives, necessitating a multifaceted approach and parallel analysis. Additionally, it is important to recognize that even in the best diplomatic or public-private partnerships, some vulnerabilities may remain undisclosed, as entities may prioritize their own interests. This

inherent limitation can affect the comprehensiveness and reliability of the foresight process.

If these limitations are taken into account, along with any others that may arise during the application of foresight methodologies, the outcomes can significantly aid in building resilience. There are numerous methodologies available, all of which can be applied in various ways – from large group settings to specialized workshops. One effective approach is to organize foresight workshops with experts. Backcasting is an interesting method to test in this context. By drafting reports and developing policy recommendations based on the findings from these workshops, the overall resilience of society can be enhanced. These initiatives can also serve as a first step toward establishing deterrence.

Developing a set of wild cards could also be beneficial, offering unexpected scenarios for consideration. Additionally, hosting conferences where experts discuss findings, share best practices, and exchange lessons learned can further enhance the effectiveness of these efforts.

Furthermore, the Delphi method can be highly effective in this domain when executed properly. By gathering insights from a diverse range of experts, the Delphi method can help refine strategies and ensure they are robust and well-rounded. Implementing these techniques and continuously improving upon them can lead to more resilient and adaptable strategies in the face of evolving cyber threats.

A key finding from the application of foresight methodologies, in this case, is the high relevance of cyber diplomacy and international cooperation in enhancing cyber resilience. Cyber threats often transcend national borders, necessitating a coordinated response. Cyber diplomacy, which involves international collaboration and policy-making, enables nations to share intelligence, establish common standards, and support each other in developing cybersecurity capabilities. This international cooperation can lead to the creation of norms and agreements that enhance collective cyber resilience. By fostering relationships and trust among countries, cyber diplomacy aims to create a more secure and stable cyberspace, facilitating the sharing of threat intelligence and best practices on a global scale.

Furthermore, international cooperation can enhance the effectiveness of cybersecurity measures through collaborative efforts. Such cooperation allows for quicker responses to emerging threats and ensures a more coordinated and effective defense against cyber adversaries.

Another significant finding is the crucial role of public-private partnerships in building cyber resilience. By encouraging collaboration between government institutions and private sector entities, it is possible to share information, best practices, and resources more effectively. Such partnerships can lead to the development of innovative cybersecurity solutions, improve threat detection and response capabilities, and ensure a more coordinated approach to mitigating cyber threats.

Foresight methodologies, while not capable of predicting the future, are exceptionally valuable in addressing the complexities of the cyber realm. They provide the tools and insights needed to steer the waters of the digital world, helping organizations and nations alike to prepare for and adapt to the ever-evolving landscape of cyber threats. Implementing strategic foresight enables the charting of a course towards a safer and more resilient digital future.

REFERENCE LIST

Ballandonne, M. (2020) The history of futures studies: A note on Gilfillan's early work. *Technological Forecasting and Social Change*. 157, 119983. doi: 10.1016/j.techfore.2020.119983.

Bell, W. (2009) *Foundations of futures studies. Volume 1: History, purposes and knowledge*. Human Science for a New Era Series. 5th ed. Piscataway, New Jersey, U.S.A., Transaction Publishers.

Bell, W. & Mau, J. A. (eds.) (1971) *The Sociology of the Future. Theory, Cases and Annotated Bibliography*. New York, U.S.A., Russell Sage.

Berger, G. (1957) Sciences humaines et prevision. *La Revue des Deux Mondes (1829-1971)*. 417-426.

Brown, H. (1954) The Challenge of Man's Future. *Engineering and Science*. 17(6), 22-32.

Chassidim, H. Perentis, C., Toch, E. & Lepri, B. (2021) Between privacy and security: the factors that drive intentions to use cyber-security applications. *Behaviour & Information Technology*. 40(16), 1769–1783. doi: 10.1080/0144929X.2020.1781259.

Coates, J. F. & Jarratt, J. (1989) *What Futurists Believe*. Bethesda, Maryland, U.S.A., World Future Society.

Day, G. S. & Schoemaker, P. J. H. (2019) *See Sooner, Act Faster: How Vigilant Leaders Thrive in an Era of Digital Turbulence*. Cambridge, MA, U.S.A., MIT Press.

de Jouvenel, B. (1967) *The art of conjecture*. New York: Basic Books

de Jouvenel, H. (2019) Futuribles: Origins, Philosophy, and Practices—Anticipation for Action. *World Futures Review*. 11(1), 8–18. doi: 10.1177/1946756718777490.

Dror, Y. (1970) *A Policy Science View of Future Studies: Alternative Futures and Present Action*. Santa Monica, U.S.A., RAND Corporation.

Dunn, C. M., Eriksen, C. & Scharte, B. (2023) Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research*. 26(7), 801–814. doi: 10.1080/13669877.2023.2208146.

Fergnani, A. (2020) Futures Studies, Foresight, Futurism, Futurology, Futures Thinking…What Name???. *Medium*. https://medium.com/predict/futures-studies-foresight-futurism-futurology-futures-thinking-what-name-3b3863ceab8c [Accessed: 16th July 2024].

Flammini, F. (2019) *Resilience of Cyber-Physical Systems: From Risk Modelling to Threat Counteraction.* Cham, Switzerland, Springer International Publishing.

Flechtheim, O. K. (1966) *History and Futurology*. Meisenheim am Glan, Germany, Anton Hain.

Gabor, D. (1964) *Inventing the Future*. London, U.K., Secker & Warburg.

Gabor, D. (1972) *The Mature Society: A View of the Future*. New York, U.S.A., Praeger Publications.

Godet, M. (2001) *Manuel de prospective stratégique*. Paris, France, Dunod.

Gordon, T. J. & Helmer, O. (1964) *Report on a Long-Range Forecasting Study*. Santa Monica, U.S.A., The RAND Corporation.

Goux-Baudiment, F. (1997) Bertrand de Jouvenel: A futures thinking open mind. *Futures*. 29(9), 865–868. doi: 10.1016/S0016-3287(97)90133-6.

Helmer, O. (1983) *Looking Forward: A Guide to Futures Research*. SAGE Publications.

Helmer, O. (1970) *Report on the future of the future-state-of-the-union reports*. Middletown, CT: Institute for the Future.

Henshel, R. (1981) Evolution of Controversial Fields: Lessons from the Past for Futures. *Futures*. 13(5), 401–412. doi: 10.1016/0016-3287(81)90125-7.

Huber, G. & Bell, W. (1971) *Sociology of the Future*. New York, U.S.A., Russell Sage Foundation.

Inayatullah, S. (1998) Macrohistory and futures studies. *Futures*. 30(5), 381–394. doi: 10.1016/S0016-3287(98)00043-3.

Inayatullah, S. (2002) *Reductionism or layered complexity? The futures of futures studies*. Futures. 34(3-4), 295–302. doi: 10.1016/S0016-3287(01)00045-3.

Jungk, R., & Galtung, J. (Eds.). (1969). *Mankind 2000*. London, Allen & Unwin.

Kahn, H. (1960) *On Thermonuclear War*. Princeton, New Jersey, U.S.A., Princeton University Press.

Kahn, H. (1962) *Thinking about the Unthinkable*. New York, U.S.A., Horizon Press.

Linneman, R. & Klein, H. (1979) The Use of Multiple Scenarios by US Industrial Companies. *Long Range Planning*. 12(1), 83–90. doi: 10.1016/0024-6301(79)90034-7.

Lesourne, J. & Stoffaës, C. (1996) *La prospective stratégique d'entreprise: Concepts et études de cas.* Paris, France, InterEditions.

Marien, M. & Jennings, L. (eds.) (1987) *What I Have Learned: Thinking about the Future then and now*. New York, U.S.A., Greenwood Press.

Maruyama, M. (1978) Introduction. In: Maruyama, M. & Harkins, A. (eds.) *Cultures of the Future*. The Hague, The Netherlands, Mouton, XVII-XXII.

Meadows, D. H., Meadows, D. L., Randers, J., & Behrens, W. W. III. (1972) *The limits to growth*. New York: Universe Books.

Millett, S. M. (2003) *The future of scenarios: Challenges and opportunities*. Strategy & Leadership, 31(2), 16-24.

Naisbitt, J. (1984) *Megatrends*. New York, Warner Books.

Nanus, B. (1984) *Futures Research–Stage Three*. Futures. 16(4), 405–407. doi: 10.1016/0016-3287(84)90104-6.

Nebreda, P. (21 March 2023) The Role of Biometrics in Cybersecurity: Threats and Solutions. *Alice Biometrics*. https://alicebiometrics.com/en/role-of-biometrics-in-cybersecurity-threats-and-solutions/ [Accessed: 16th June 2024].

Ogburn, W. F. (1933) *Recent Social Trends in the United States. Report of the President's Research Committee on Social Trends*. New York, McGraw-Hill.

Polak, F. L. (1961) *The Image of the Future*. Amsterdam, Elsevier Scientific Publishing Company.

Rohrbeck, R., Battistella, C. & Huizingh, E. (2015) Corporate Foresight: An Emerging Field with a Rich Tradition. *Technological Forecasting and Social Change*. 101, 1–9. doi: 10.1016/j.techfore.2015.11.002.

Russpatrick, S., Amarakoon, P. & Hedberg, C. (2023) Bounce forward resilience attributes: Information system strengthening in response to crisis. In: Proceedings of the 31st European Conference on Information Systems, ECIS 2023, 11-16 June 2023, Kristiansand, Norway, pp. 3-4.

Schoemaker, P. J. H., & Day, G. (2021). Preparing organizations for greater turbulence. California *Management Review*, 63, 66-88. https://doi.org/10.1177/00081256211022039.

Slaughter, R. A. (1995) The Foresight Principle: Cultural Recovery in the 21st Century. London, Adamantine.

Slaughter, R. A. (1996a) Futures studies: From individual to social capacity. Futures. 28(8), 751–762.

Slaughter, R. A. (1996b) The Knowledge Base of Futures Studies. Hawthorn, Victoria, Australia, DDM Media Group.

Slaughter, R. A. (2002a) Futures studies as a civilizational catalyst. Futures. 34(3-4), 349–363.

Slaughter, R. A. (2002b) Futures studies as an intellectual and applied discipline. In: Dator, J. A. (ed.) Advancing Futures: Futures Studies in Higher Education. Westport, Connecticut, U.S.A., Praeger Publications, pp. 91–108.

Strategic foresight (no date). Available at: https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight_en [Accessed: 30 July 2024].

Taleb, N. N. (2007) *The Black Swan: The Impact of the Highly Improbable*. New York, Random House.

Toffler, A. (1970) *Future Shock*. New York, Random House.

Tolon, K. (2012) Futures studies: A new social science rooted in cold war strategic thinking. In: Solovey, M. & Cravens, H. (eds.) *Cold War Social Science, Knowledge Production, Liberal Democracy, and Human Nature.* New York, Palgrave Macmillan.

van der Heijden, K. (1996) *Scenarios: The art of strategic conversation*. Wiley.

Winthrop, H. (1968) The Sociologist and the Study of the Future. *The American Sociologist.* 3(2), 136-145.

Wucker, M. (2016) *The Gray Rhino: How to Recognize and Act on the Obvious Dangers We Ignore*. New York, St. Martin's Press.

Zumbrunn, L. (2023) Resilience through Foresight: Implications for the Public Sector. *Swiss Yearbook of Administrative Sciences*. 14(1). 45–57. doi: 10.5334/ssas.183.

Carola FREY is an expert with deep knowledge and hands-on experience within the Strategic Analysis and Cooperation Department of the Euro-Atlantic Resilience Centre and coordinates the International Relations and Protocol Compartment. She specializes in conflict analysis, futures studies, and emerging and disruptive technologies. She has solid experience in the government sector, with previous employment in the Romanian Ministry of Defence, Ministry of Foreign Affairs, and Ministry of Research, Innovation and Digitalization. In addition, Carola Frey has been active in academia since 2014, publishing numerous articles and participating in national and international conferences and workshops. From 2021, she is a PhD Candidate with a thesis that aims to investigate China's foreign policy in the new world order using futures studies methods. She is part of the Communities of Interest: Communication Systems and Novel Technological Ecosystems.

This is an open access article distributed under the terms and conditions of the Creative Commons Attribution-NonCommercial 4.0 International License.