Contributions to Economics

Giuseppe T. Cirella *Editor*

Handbook on Post-War Reconstruction and Development Economics of Ukraine

Catalyzing Progress

Springer

Giuseppe T. Cirella
Editor

Handbook on Post-War Reconstruction and Development Economics of Ukraine

Catalyzing Progress

Springer

Editor
Giuseppe T. Cirella
Faculty of Economics
University of Gdansk
Sopot, Poland

ISSN 1431-1933 ISSN 2197-7178 (electronic)
Contributions to Economics
ISBN 978-3-031-48734-7 ISBN 978-3-031-48735-4 (eBook)
https://doi.org/10.1007/978-3-031-48735-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Printed on acid-free paper

Contents

Chapter 2
Utilizing Information and Communication Technology Systems for the Formation of National Security

Gevorkyan A. Yuriyovich, Olesia Solodovnik, Giuseppe T. Cirella, Ivan Parubchak, Oleksandr Dorofyeyev, and Andrii Nosyk

1 Introduction to National Security Concerns

In today's interconnected world, driven by the internet and globalization, security concerns are prevalent and pose both internal and external threats to nation-states (Asogwa, 2020; Li & Liu, 2021; Yarovenko, 2020). These concerns encompass critical information security threats, which constitute a significant aspect of a nation's security framework (Anwar et al., 2018; Ayoob, 2018; Djenna et al.,

G. A. Yuriyovich (✉)
Department of International Business and Finance, National Technical University Kharkiv Polytechnic Institute, Kharkiv, Ukraine

O. Solodovnik
Department of Finance and Credit, Kharkiv National University of Civil Engineering and Architecture, Kharkiv, Ukraine

G. T. Cirella
Faculty of Economics, University of Gdansk, Sopot, Poland
e-mail: gt.cirella@ug.edu.pl

I. Parubchak
Department of Public Administration, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies, Lviv, Ukraine

O. Dorofyeyev
Department of Public Management and Administration, Poltava State Agrarian Academy, Poltava, Ukraine
e-mail: olexandr.dorofeev@pdaa.edu.ua

A. Nosyk
Department of Multimedia Information Technologies and Systems, National Technical University Kharkiv Polytechnic Institute, Kharkiv, Ukraine
e-mail: andrii.nosyk@khpi.edu.ua

G. T. Cirella (ed.), *Handbook on Post-War Reconstruction and Development Economics of Ukraine*, Contributions to Economics,
https://doi.org/10.1007/978-3-031-48735-4_2

2021). Ukraine, in particular, faces crucial dynamics and challenges related to information and communication technology (ICT) that significantly impact its information society and overall structure. The current ICT interventions, arising from the turmoil of Russian aggression, present various challenges and threats to both individuals and the state. These challenges include the susceptibility of global communication networks to compromise online and cloud-based national security. Additionally, cross-border activities pose threats to information security, and internet-based media can negatively impact the nation's security setup (Asogwa, 2020). Recent research in Ukraine has examined the interplay between individuals, society, and the state concerning ICT-related concerns in the context of national security. Prioritizing a secure information sphere emerged as a key concern (Antoiuk, 2019), with significant findings establishing links between communication networks and progressive national security issues.

Currently in Ukraine, there is a pressing necessity to enhance the participatory involvement of civil society in understanding and utilizing ICT. Civil society, which constitutes the third sector separate from government and business and encompasses families and private individuals, plays a crucial role in facilitating the development, adoption, and implementation of ICT-related decisions. By doing so, it indirectly contributes to achieving national security objectives (Antoiuk, 2019). Emphasizing this bottom-up perspective can empower authorities to formulate strong policies and effective management decisions (Chen et al., 2020; Lewandowski & Cirella, 2022) while promoting active societal engagement at the individual and community levels. Within this context, this chapter delves into the theoretical and methodological underpinnings of how an informed and ICT-aware society can establish a resilient national security system, highlighting its urgency in Ukraine (Khaba, 2017; Malyarenko & Kormych, 2023; Ratten, 2023; Shpiro, 2023). Current advancements in this field of study underscore the need for prompt attention to two significant aspects: first, the focus on information society and second, the emphasis on public authority and administration in timely identifying, preventing, and neutralizing potential and existing information-related challenges and threats. These factors have influenced the development, direction, and relevance of Ukraine's national security, intertwining with various societal components such as the economy, built environment, and social fabric of the country.

An analysis of the literature employing ICT systems for national security formation reveals a diverse array of challenges pertaining to information protection and the development of an information society. This aspect holds immense significance for the stability of the system, as evidenced by numerous studies across various disciplines, including Khaba (2017), Nashynets-Naumova (2017), Politanskyi (2017a, 2017b), Ponomarenko (2017), Tkachuk (2017a, 2017b), Zolotar (2017), Gevorkyan et al. (2018), Simakhova (2018), Antoiuk (2019), Byrkovych (2019), Diegtiar et al. (2021), Avanesova et al. (2020), and Nepomnyashchyy et al. (2021). A comprehensive examination of these scholarly works underscores the paramount importance of theoretically and methodologically framing information security in advancing a robust national security agenda. However, certain concerns persist regarding the role of ICT in shaping and fortifying such a system, as highlighted by Shatun (2016),

Dovhan (2017), Lelechenko et al. (2020), and Marutian (2020). This chapter aims to further explore and address these issues, particularly in relation to the status and role of the information society in Ukraine. It is believed that fostering an ICT-aware citizenry is essential for recognizing the necessity of change and its profound impact on the formation and resilience of the country's national security.

2 Framing an ICT-Friendly Information Society

Framing an ICT-friendly information society necessitates a comprehensive approach involving open-mindedness, user cooperation, and reciprocity from both bottom-up and top-down perspectives. In the context of Ukraine, four essential goals are identified to achieve this vision:

- Determine the primary criteria required to classify activities within the information society.
- Systematize the key features and provide a clear definition of "information society," specifically in relation to the utilization of ICT systems.
- Develop strategies to address and overcome threats and challenges faced by the information society when ICT is employed to enhance national security.
- Evaluate the challenges and essential methods for monitoring ICT protection, as a crucial response to the threats and challenges inherent in the evolution of the information society.

By addressing these goals, Ukraine can lay a strong foundation for building an information society that embraces ICT, fostering an environment conducive to progress and security in the digital era.

The rapid and widespread advancement of new ICT is ushering in a global information revolution with profound impacts on multiple aspects of society. This transformative phenomenon is referred to as the "information society." Figure 2.1 presents the primary criteria for designating a society as an information society (Antoiuk, 2019; Nashynets-Naumova, 2017; Politanskyi, 2017a, 2017b). The modern information society's development is closely tied to the recognition and fundamental role of ICT among individual users. Information, in its various forms, exerts an increasingly significant influence on diverse facets of public life, shaping the system of socioeconomic relationships within the state and playing a vital role in the establishment of the national security framework (Politanskyi, 2017a, 2017b). As global ICT becomes pervasive across all spheres of life, it brings about entirely new possibilities for fostering social connections, granting access to vast repositories of human knowledge, bridging digital divides, reforming public administration through e-governance implementation, and executing the country's information policy concerning interactions with civil society. Such interactions contribute to openness, transparency, and, most importantly, security at both local and national levels.

To delve deeper into the establishment and structure of an operational ICT system, this chapter also examines Ukraine's information society encompassing its

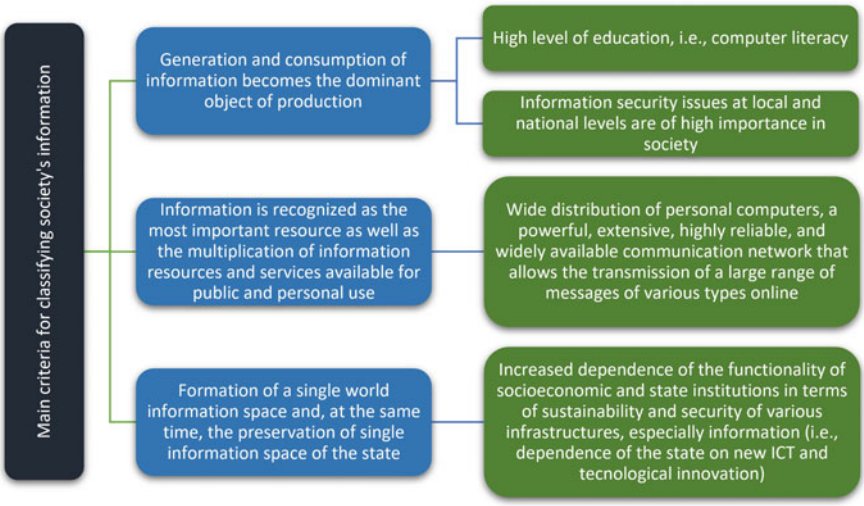

Fig. 2.1 Identification of the main criteria for assigning a society to information [Source: Adapted from Khaba (2017), Nashynets-Naumova (2017), Politanskyi (2017a, 2017b), and Antoiuk (2019)]

economic, philosophical, sociological, legal, and socio-cultural dimensions and explores its domestic and international aspirations. To enhance the theoretical and methodological significance of the research, it is essential to consolidate the findings of renowned scholars, identifying different aspects and characteristics of the information society concept. Moreover, envisioning research that inherently defines crucial categories subject to a functional ICT system for framing Ukraine's national security, as illustrated in Fig. 2.2, further enriches the chapter's value.

According to Fig. 2.2, the concept of an information society involves a complex social entity comprising individuals, economic entities, and public authorities at both local and state levels. This entity is interconnected within a global information space, leading to diverse multidimensional relationships formed through the creation, use, collection, processing, storage, and protection of ICT across various domains (Aggarwal et al., 2020; Aggarwal & Reddy, 2013; Monroe-Wise et al., 2019; Roztocki et al., 2019). The main objective is to ensure universal access to essential public information while considering necessary restrictions (Nevado-Peña et al., 2019; Zonneveld et al., 2019) that dictate conditions for the establishment and maintenance of national security. In this context, national security should be thoughtfully balanced and integrated with the socioeconomic development of communities, serving as the fundamental pillar upon which sustainable progress is built (Fu et al., 2022; Oniszczuk-Jastrząbek et al., 2020; Spring & Cirella, 2022). This holistic approach ensures that not only are we safeguarding the country's security but we are also nurturing the wellbeing of its communities and fostering a future that aligns with the principles of sustainability (Cirella et al., 2007; Cirella & Tao, 2008, 2009a, 2009b; Cirella & Zerbe, 2014a), where prosperity coexists harmoniously with environmental responsibility. In doing so, we recognize the intricate

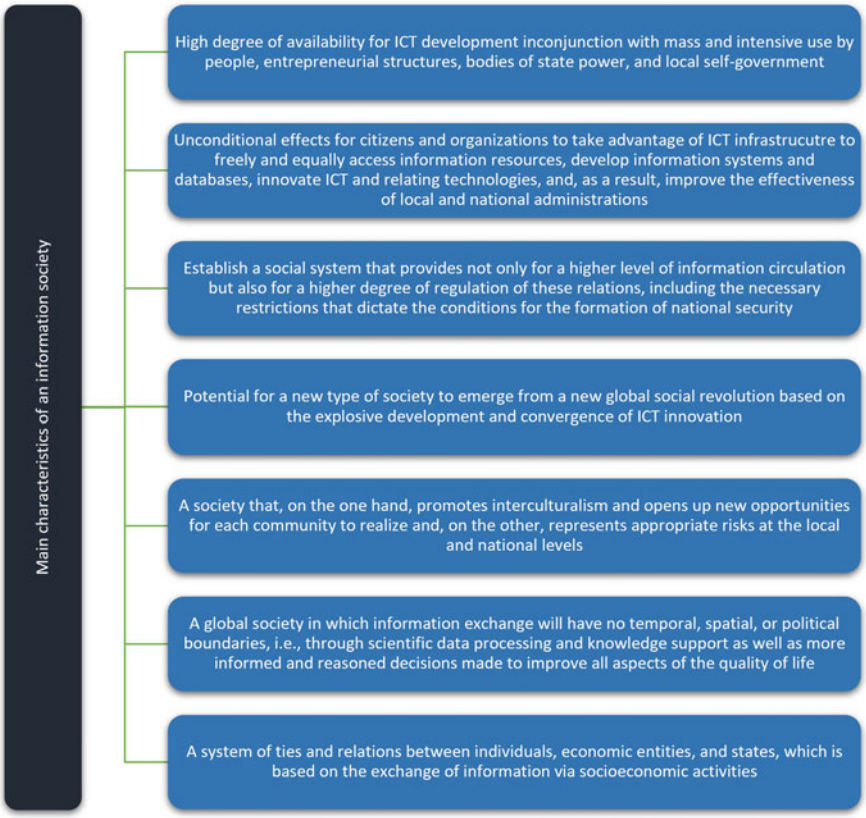

Fig. 2.2 Main characteristics, categories, and definition of an information society [Source: Adapted from Nashynets-Naumova (2017), Tkachuk (2017a, 2017b), Gevorkyan et al. (2018), Simakhova (2018), and Avanesova et al. (2020)]

relationship between human-nature relations and the environment (Cirella, 2020, 2022; Cirella et al., 2020), acknowledging that prosperity can only thrive when it coexists harmoniously with environmental responsibility (Cirella & Zerbe, 2014b). By addressing these interconnected aspects, we not only secure the nation's safety but also acknowledge the profound impact of our actions on the delicate balance between humanity and the natural world.

To achieve successful and effective development of an information society, every information user must have comprehensive access and inclusive involvement in all informatization processes (Potnis, 2014; Van Cuilenburg, 2016). Therefore, ICT systems should be user-friendly and accessible, taking into account the needs and preferences of individuals. This necessitates the active integration of local and state authorities, especially concerning information security at the local and national levels (Roller et al., 2019). In the current state of Ukraine, there exists an unsatisfactory level of support for this protocol in the country's information sphere

(Eichensehr, 2022; Shimchenko, 2019; Streltsov, 2017; Svintsytskyi, 2022; Willett, 2022), hindering the modernization of innovative ICT security measures. Nonetheless, Ukraine's information society protocols are still in developmental stages, showing promising signs of improvement to strengthen and safeguard national security processes (Potii et al., 2015). However, the continuous development and enhancement of the ICT system in Ukraine, especially since the post-24 February 2022 Russian Federation attack, remain burdened by the war effort and bureaucratic complexities. This vulnerability may leave unprepared users susceptible to modern cyberattacks and threats, particularly through the internet (Diorditsa et al., 2020; Eichensehr, 2022; Potii et al., 2015; Streltsov, 2017; Sullivan & Kamensky, 2017; Willett, 2022) and, for example, via the energy grid (Cirella et al., 2021; Goncharuk & Cirella, 2020; World Data and UN, 2023; Zinets & Williams, 2019) or the export of grain (Arndt et al., 2023; Bazhal & Koutchma, 2022; Odiwuor, 2022; Pereira et al., 2022).

3 Formulating an ICT Framing for Ukraine's National Security Apparatus

Targeted cyberattacks can result in a scenario where the cyberattacker, i.e., referred to as a hacker, gains complete control over a mobile or stationary information and communication device, thereby accessing all the information stored on that device, including sensitive and confidential data. When such attacks occur on a large scale, they directly threaten a country's national security. These focused attacks often target specific users, such as political figures, high-profile individuals with financial influence, or others who possess critical national information. To counteract these threats, it is essential to categorize the primary types and forms of cyberthreats and propose effective strategies to mitigate them. Table 2.1 presents an overview of how the information society protocol, through ICT, contributes to the formation and reinforcement of national security.

In reference to Table 2.1, a structured framing can be deduced and modeled around the suggested requisites of potential information society threats. By utilizing ICT for the formation and strengthening of Ukraine's national security, a constant monitoring and control, i.e., a comprehensive assessment of the state of protection of information and communication relations, can be established by considering both negative internal and external impacts. The main tasks of monitoring the information and communication environment of a country should take into account the following procedures:

- Improve the effectiveness of legal instruments.
- Strategically plan for the development of operational systems for the protection of national security in the information sphere.
- Systematize information legislation and continuously (i.e., in an ongoing manner) improve it.

Table 2.1 Types and forms of threats to the information society and ways to overcome it for the formation and strengthening of national security

Types of threats	Threat forms	Comprehensive ways to address threats for building and strengthening national security
Entity (or government body) pursuing the subject that implements the threat	• Influence on the consciousness and psychological state of a user of the information society • The provision of destructive effects which may harm the health of the individual • Taking possession of personal (i.e., confidential) information for the purpose of using it for illegal purposes • Dissemination of the ideology of terrorism and radical ideas in information and communication networks • Financial fraud • Development of antisocial behavioral stereotypes	• Identifying the user that implements the threat and taking appropriate measures to suppress their unlawful actions • Explaining of the information society the main ways of avoiding threats and the foundations of democracy and freedom, i.e., the main political course of the country • Introduction of economic and financial security mechanisms
Source of the threat	• Criminals and criminal groups whose activities are aimed at stealing information, personal data, and embezzlement of other people's property through fraud in the information sphere • Criminals and criminal groups that spread various forms of sexual violence and trade in illicit narcotic drugs and psychotropic substances in the global information space	• Continuous monitoring of information and communication sources with a view to detecting and preventing violations of the administrative and criminal laws of the country in the field of dissemination of prohibited information • Creation of new and improvement of existing media security tools for dissemination to information and communication subjects
Internet threats	• Dangerous internet sites (i.e., several search services provide various ways to inform users about the level of reliability of a site) • Phishing sites • Malicious software • Spamming • Fraudulent sites advertised for profit (i.e., financial pyramids, so-called false virus, fake online stores, etc.) • Internet sites aimed at influencing the individual consciousness of young people (e.g., websites that promote cybersuicide,	• Improving the country's legal framework for controlling the internet and disseminating prohibited information and websites • Improving information literacy of the society and economic entities in the protection of personal and corporate information from criminals • Complete blocking of suspicious sites that may threaten the national security of the country • Identification and prosecution of persons involved in the dissemination of prohibited information and fraud on the internet

(continued)

Table 2.1 (continued)

Types of threats	Threat forms	Comprehensive ways to address threats for building and strengthening national security
	concerted suicides, porn sites, chats, forums that use pedophiles, etc.)	
Threats to national security in the information sphere of the latest type	• Threats from cookies that may directly or indirectly affect political views in the information society as well as other threats to national security • Threats to cryptocurrency (e.g., Bitcoin) traffic • Privacy threats due to the latest online advertising technology real-time bidding	• Development of new technologies to block downloads of cookies on information and communication devices • A possible ban on cryptocurrency throughout the country due to the inability to control it by authorized state authorities • Timely response to emerging threats and hazards in a changing information and communication space

Source: Adapted from Ponomarenko (2017), Byrkovych (2019), Diegtiar et al. (2021), Lelechenko et al. (2020), Shevchenko et al. (2020), and Nepomnyashchyy et al. (2021)

- Improve the effectiveness of measures to detect information offenses (Dovhan, 2017).

Moreover, it has been shown that the main methods to facilitate effective monitoring for the formation and strengthening of national security are via the skilled and apt use of ICT by all end user stakeholders (Fig. 2.3).

The continuous monitoring of ICT by authorized state authorities will play a crucial role in promptly identifying both internal and external threats. By providing reliable protection to the information society and other entities (Smolyanyuk, 2018; Tkachuk et al., 2020), this process will significantly enhance the overall national security level of Ukraine. It will also establish a protocol-friendly system, considering both top-down and bottom-up perspectives (Tkachuk, 2017b; Tkachuk et al., 2020). According to Smolyanyuk (2018), the national security of Ukraine is a matter of vital interest, hinging on two main systems: the national security system itself and the system for ensuring national security. These two systems must be harmonized to empower Ukrainian citizens with adequate knowledge about the fundamental principles of national security and offer practical assistance to counter potential negative actions or consequences.

A pressing area of research involves addressing national security concerns in the context of the Russian Federation's aggression against Ukraine, as it is central to transforming the nation's security landscape and ensuring its survival and longevity (Eichensehr, 2022; Liu & Shu, 2023; Smolyanyuk, 2018). This approach necessitates the involvement of leading specialists, policymakers, and scientists in the realms of information security and lawmaking. Moreover, it calls for a

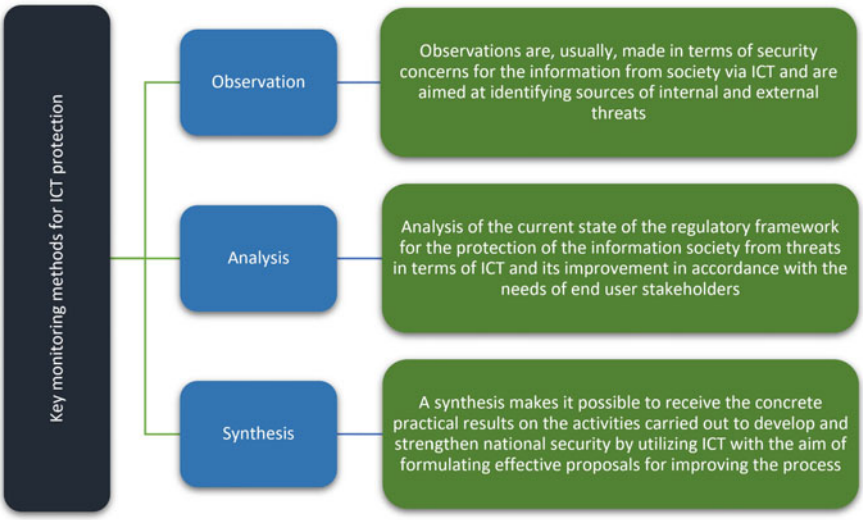

Fig. 2.3 Key monitoring methods for ICT protection [Source: Adapted from Shatun (2016) and Marutian (2020)]

well-informed population proficient in ICT relations. To achieve this goal, policy initiatives should focus on highlighting the key roles of the information society at all levels, aiming to reduce cyber vulnerabilities and bolster nationwide protections. In practical terms, the implementation of such mechanisms should encompass the following measures:

- Minimize security hazards in terms of ICT in the global information society apparatus.
- Improve the legal culture of the information society by implementing protections via ICT—in a general sense—with particular emphasis on information media.
- Effective and mutually agreed cooperation between the various public services on the implementation of national security mechanisms in the field of ICT—with specific interests that incorporate the information society with economic entities.

By adhering to this approach, the country can establish a robust framework for safeguarding its national security and countering potential threats in an effective and coordinated manner.

The advancement of information on a global scale, the establishment of transnational information infrastructure, and the rise of the information society present numerous intricate challenges to national security concerning the use of ICT. Addressing many of these issues requires enhancements in national legislation and extensive international cooperation. Implementing consistent proposals is essential to bring potential sources of threats to information security under both national and international control (Shemayeva et al., 2019; Tkachuk et al., 2020; Yemelyanov & Bondar, 2019). In the context of Ukraine, legislation needs to align with several

crucial aspects of the national security apparatus, encompassing domestic policy, foreign policy, military and defense spending and development, social cohesion, humanitarian provisions, economic growth, scientific and technological innovation, information safeguarding and assurances, and environmental planning and protection. The apparatus must also integrate vital components such as "state security, civil protection of the population, [and] security of the state border" (Smolyanyuk, 2018). Various governmental entities have a responsibility to ensure the national security of Ukraine, including the President of Ukraine, the Parliament of Ukraine, the Cabinet of Ministers of Ukraine, the National Security and Defense Council of Ukraine, ministries, central executive authorities, the National Bank of Ukraine, courts of general jurisdiction, the Prosecutor's Office of Ukraine, the National Anti-Corruption Bureau of Ukraine, local state administrations, local self-government bodies, the Armed Forces of Ukraine, the Security Service of Ukraine, the Foreign Intelligence Service of Ukraine, the State Border Guard Service of Ukraine, and other designated officer formations committed to upholding the country's laws (Smolyanyuk, 2018).

Tkachuk et al. (2020) emphasize the significance of addressing information risks and violations of information security. They advocate the development of criteria to counterbalance the potential negative impacts on information security. To achieve this, legislative consolidation, which remains unresolved in Ukraine, must be coupled with ongoing scientific discussions throughout the country. The formulation of national objectives in the information sphere should align with the country's core values and harmonize with the current state of its development.

4 Security Forecasting and Future Outlook

This chapter introduced concepts specific to creating a comprehensive, theoretical, and methodological examination of the problems with ICT systems in terms of protocols specific to the information society process. Case research specific to Ukraine looked at the impact of these concepts in terms of the formation and strengthening of its national security. Detailed features of the analysis parallels Yemelyanov and Bondar's (2019) assessment of cybersecurity as one of the top components of national security in Ukraine. Legislative and regulatory support must be prioritized to curb cyberattacks, of any sort, against critical infrastructure and, in general, against any offshoot of civil society. Cyber defense in Ukraine should be focused on internal government corruption, Russian interference, and weak infrastructure. Utilizing international standards, e.g., from the European Union, would be an appropriate approach to developing a proper cyber defense strategy. Key to the strategy would be to develop well-rounded cyber defense mechanisms that incorporate critical infrastructure, private enterprises, and mass media within an overarching umbrella at the national level. Different agencies within the country should be allowed to share information for transparency and quick action. International support and cooperation should be sought when combating cross-border cybercrime with

joint experts from non-hostile nations and partners. This could include an exchange of experience, ICT support, and findings from "cybersecurity experts, mutual financial support, coordinated joint systemic response of countries to cybercrime, introduction of new world standards for cybersecurity, and information security, [i.e.,] national and international strategies, that respond to new cyber challenges" (Yemelyanov & Bondar, 2019). The following synthesis and conclusions are derived from a theoretical and methodological point of view. It recommended that policymakers in Ukraine consider the following four protocols when utilizing ICT systems specific to national security concerns.

First, the main criteria of classifying aspects of an information society should be properly defined and integrated into the advancement of Ukraine's modernization process—i.e., the development of an ICT-friendly population. It should be stressed that an information society is largely connected with the awareness of individual ICT users and an ICT-aware, conscious, and active community is needed as an integral part of a national security system. This point, in reference, should also consider that information, i.e., in various forms, can influence vast aspects of public life, determine the system of socioeconomic relations in the state, and act as an important factor in the formation of national security.

Second, the features, identification, and classification of Ukraine's information society should be systematized and based on its definition as noted by Nashynets-Naumova (2017), Tkachuk (2017a, 2017b), Gevorkyan et al. (2018), Simakhova (2018), and Avanesova et al. (2020). In this chapter, the complex social entity of individuals, economic entities, and public authorities at the local and national level should be combined into a single unified information space by creating a set of multidimensional relations. This structuring will allow for the creation, use, collection, processing, storage, and protection of ICT at all levels. It should provide each entity with universal access to the necessary public information as well as consider the necessary restrictions which dictate the conditions for the formation and maintenance of a robust national security system. This should also shape a balanced and integrated socioeconomic community—in parallel with the first protocol.

Third, extensive development, especially internationally, has been made in combatting threats and challenges to the global information society structure. Ukraine should ally itself with non-hostile nations and partners and, within reason, share and cooperate to combat this global threat. ICT-related risks should also be integrated into a preplanned protocol and backup systems secured and developed. The national security apparatus should consider negative phenomena as likely to happen with recurrent threats. A comprehensive and mutually agreed interaction of Ukraine's main ICT users will alleviate some of this risk.

Fourth, the process of continuously monitoring ICT by authorized state authorities will allow for the timely identification of threats of an internal and external nature and provide the information society and others with reliable protection of their information. This will, directly, increase the overall level of national security and form a security structure in line with international cyber defense standards.

Since the global nature of information development, the formation of transnational information infrastructure, and the information society in general create

several novel and problematic concerns related to safeguarding national security, a sensible stance would be to incorporate the precautionary principle whenever possible. According to Elishakoff (2004), the principle manifests itself as a factor of safety versus reliability. For policymakers, the possibility of harm from making certain decisions must be acknowledged—especially regarding the progress of science and technology and ICT innovation. The practical implications of implementing the four protocols will encourage Ukraine's national security apparatus to (1) minimize security hazards when using ICT at the macro level, (2) improve the legal culture of the information society in terms of protecting information and information media (i.e., primarily via the internet), and (3) agree to effectively and mutually establish cooperation between various public entities to better unify the country's security structure as well as create an ICT-compliant information society prone for economic growth and development. Many of these steps can be achieved only by implementing relevant national legislation and multilateral international cooperation, i.e., consistent with proposals that can bring sources of threats to information security under national and international control.

References

Aggarwal, B., Xiong, Q., & Schroeder-Butterfill, E. (2020). Impact of the use of the internet on quality of life in older adults: Review of literature. *Primary Health Care Research & Development, 21*, 1–6. https://doi.org/10.1017/S1463423620000584

Aggarwal, C. C., & Reddy, C. K. (Eds.). (2013). *Data clustering: Algorithms and applications* (1st ed.). Chapman and Hall/CRC.

Antoiuk, V. P. (2019). Zaluchenist′ Naselenaya Ukrayiny proty. In Pobudova informatsiinoho suspilstva, resursy i tekhnolohii: Mat-ly XVIII Mizhn. nauk. prakt. konf. UkrINTEI, Kyiv (pp. 13–17).

Anwar, M. A., Rongting, Z., Dong, W., & Asmi, F. (2018). Mapping the knowledge of national security in 21st century a bibliometric study. *Cogent Social Sciences, 4*, 1–18. https://doi.org/10.1080/23311886.2018.1542944

Arndt, C., Diao, X., Dorosh, P., Pauw, K., & Thurlow, J. (2023). The Ukraine war and rising commodity prices: Implications for developing countries. *Global Food Security, 36*, 100680. https://doi.org/10.1016/j.gfs.2023.100680

Asogwa, C. E. (2020). Internet-based communications: A threat or strength to national security? *SAGE Open, 10*, e4580. https://doi.org/10.1177/2158244020914580

Avanesova, N. E., Mordovtsev, O. S., & Serhiienko, Y. I. (2020). The Theoretical-Methodical Principles of Identification and Interrelation of the Influence of Destabilizing Factors on the Economic Security of an Industrial Enterprise. *Business Inform, 9*, 20–28. https://doi.org/10.32983/2222-4459-2020-9-20-28

Ayoob, M. (2018). The security problematic of the third world. *World Politics*, *43*, 247–273. https://doi.org/10.2307/2010473

Bazhal, M., & Koutchma, T. (2022). Ukraine as a food and grain hub: Impact of science and technology development on food security in the world. *Frontiers in Food Science and Technology, 2*, 34. https://doi.org/10.3389/FRFST.2022.1040396

Byrkovych, T. I. (2019). Mechanisms of public administration in the field of digital transformation. *Derzhavne Upr Udoskon Ta Rozvyt, 9*, e1488. https://doi.org/10.32702/2307-2156-2019.9.2

Chen, Y., Pereira, I., & Patel, P. C. (2020). Decentralized governance of digital platforms. *Journal of Management, 47*, 1305–1337. https://doi.org/10.1177/0149206320916755

Cirella, G. T. (2020). *Sustainable human-nature relations: Environmental scholarship, economic evaluation, urban strategies*. Springer.

Cirella, G. T. (2022). *Human settlements: Urbanization, smart sector development, and future outlook*. Springer.

Cirella, G. T., Russo, A., Benassi, F., Czermanski, E., Goncharuk, A., & Oniszczuk-Jastrząbek, A. (2021). Energy re-shift for an urbanizing world. *Energies, 14*, 5516. https://doi.org/10.3390/en14175516

Cirella, G. T., & Tao, L. (2008). Measuring sustainability: An application using the index of sustainable functionality in south East Queensland, Australia. *The International Journal of Interdisciplinary Social Sciences: Annual Review, 3*, 231–240. https://doi.org/10.18848/1833-1882/CGP/v03i08/52680

Cirella, G. T., & Tao, L. (2009a). An adaptive quantitative method to measure sustainability: An application for the State of Queensland, Australia. *The International Journal of Environmental, Cultural, Economic, and Social Sustainability: Annual Review, 5*, 127–139. https://doi.org/10.18848/1832-2077/CGP/v05i01/54563

Cirella, G. T., & Tao, L. (2009b). The index of sustainable functionality: An application for measuring sustainability. *World Academy of Science, Engineering and Technology, 3*, 268–274. https://doi.org/10.5281/zenodo.1330369

Cirella, G. T., Tao, L., & Mohamed, S. (2007). An application of an adaptive quantitative method to measure the sustainability of the Gold Coast, Australia. *Journal of Coastal Research, SI50*, 52–56.

Cirella, G. T., Wanjiku, S., Paczoski, A., & Tiruneh, S. (2020). Human-nature relations: The unwanted filibuster. In G. T. Cirella (Ed.), *Sustainable human–nature relations: Environmental scholarship, economic evaluation, urban strategies* (pp. 3–22). Springer.

Cirella, G. T., & Zerbe, S. (2014a). Index of sustainable functionality: Application in Urat front banner. In G. T. Cirella & S. Zerbe (Eds.), *Sustainable water management and wetland restoration in settlements of continental-arid Central Asia* (pp. 137–155). Bozen University Press.

Cirella, G. T., & Zerbe, S. (2014b). Quizzical societies: A closer look at sustainability and principles of unlocking its measurability. *International Journal of Science in Society, 5*, 29–45. https://doi.org/10.18848/1836-6236/CGP/v05i03/51427

Diegtiar, O.A., Gevorkyan, A.Yu., Cherepovska, T.V., Kuzmenko, S.H., & Mozhaykina, N.V. (2021). Adaptation of municipal governance mechanisms to European standards. *Public Policy and Administration*, *20*, 574–584. https://doi.org/10.13165/VPA-21-20-5-02

Diorditsa, I. V., Telestakova, A. A., Koval, O. M., Nazarenko, O. A., & Nastiuk, A. A. (2020). Information interventions as a new dimension of Ukraine's cyber-vulnerability. *Linguistics and Culture Review, 5*, 152–166. https://doi.org/10.21744/lingcure.v5nS2.1337

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*, e4580. https://doi.org/10.3390/APP11104580

Dovhan, O. D. (2017). Informatsiina bezpeka: Stan, problemy, tendentsii. In *Informatsiini resursy, intelektualna vlasnist, komunikatsii v osvitno-naukovii ta innovatsiinii sferakh: Filosofsko-pravovi ta prykladni aspekty materialy kruhloho stolu* (pp. 31–39). Vydavnychyi dim ArtEk.

Eichensehr, K. E. (2022). Ukraine, cyberattacks, and the lessons for international law. *American Journal of International Law, 116*, 145–149. https://doi.org/10.1017/aju.2022.20

Elishakoff, I. (2004). *Safety factors and reliability: Friends or foes?* Springer Science.

Fu, Y., Yang, X., Wang, T., Supriyadi, A., & Cirella, G. T. (2022). Spatial pattern characteristics of the financial service industry: Evidence from Nanjing, China. *Applied Spatial Analysis and Policy, 15*, 595–620. https://doi.org/10.1007/s12061-021-09409-z

Gevorkyan, A. Y., Druhova, O. S., & Klepikova, S. V. (2018). Faktory, shcho vplyvaiut na vyznachennia investytsiinoi pryvablyvosti ta vartosti biznesu. *Visnyk Natsionalnoho Tekhnichnoho Universytetu "Kharkivskyi Politekh Inst", 19*, 131–134.

Goncharuk, A. G., & Cirella, G. T. (2020). A perspective on household natural gas consumption in Ukraine. *Extractive Industries and Society, 7*, 587–592. https://doi.org/10.1016/j.exis.2020.03.016

Khaba, R. S. (2017). Destruktyvni informatsiini vplyvy v suchasnykh umovakh. *Informatsiina Bezpeka Liudyny Suspilstva Derzhavy, 1*, 216–224.

Lelechenko, A. P., Diegtiar, O. A., Lebedinska, O. Y., Derun, T. M., & Berdanova, O. V. (2020). Mechanisms of inter-state communications for solving sustainable development problems. *Asia Life Science, 22*, 1–14.

Lewandowski, R., & Cirella, G. T. (2022). Performance management systems: Trade-off between implementation and strategy development. *Operations Management Research, 16*, 280–295. https://doi.org/10.1007/s12063-022-00305-4

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/J.EGYR.2021.08.126

Liu, Z., & Shu, M. (2023). The Russia–Ukraine conflict and the changing geopolitical landscape in the Middle East. *China International Strategy Review, 5*, 99–112. https://doi.org/10.1007/s42533-023-00134-5

Malyarenko, T., & Kormych, B. (2023). Russian policy towards the economy of occupied Ukrainian territories: Crawling de-modernization. *Eurasian Geography and Economics, 64*, 220–237. https://doi.org/10.1080/15387216.2023.2167097

Marutian, R. R. (2020). Ekhanizmy intelektualnoho zabezpechennia polityky natsionalnoi bezpeky Ukrainy: Zmist ta struktura. *International Academy Journal Web of Scholar, 1*, e6883. https://doi.org/10.31435/rsglobal_wos/31012020/6883

Monroe-Wise, A., Kinuthia, J., Fuller, S., Dunbar, M., Masuda, D., Opiyo, E., Muchai, B., Chepken, C., Omwenga, E., Oboko, R., Osoti, A., Masys, D., & Chung, M. H. (2019). Improving information and communications technology (ICT) knowledge and skills to develop health research capacity in Kenya. *Online Journal of Public Health Informatics, 11*, e22. https://doi.org/10.5210/OJPHI.V11I3.10323

Nashynets-Naumova, A. Y. (2017). *Informatsiina bezpeka: Pytannia pravovoho rehuliuvannia*. Vydavnychyi dim Helvetyka.

Nepomnyashchyy, O. M., Marusheva, O. A., Prav, Y. H., Medvedchuk, O. V., & Lahunova, I. A. (2021). Certain aspects of the system of public administration of universities: World practices and the Ukrainian dimension. *Journal of the National Academy of Legal Sciences of Ukraine, 28*, 99–105.

Nevado-Peña, D., López-Ruiz, V. R., & Alfaro-Navarro, J. L. (2019). Improving quality of life perception with ICT use and technological capacity in Europe. *Technological Forecasting and Social Change, 148*, 119734. https://doi.org/10.1016/J.TECHFORE.2019.119734

Odiwuor, F. (2022). The price of Russia's Ukraine invasion: Africa's food security. *Africa Up Close*. Retrieved August 19, 2022, from https://africaupclose.wilsoncenter.org/russia-ukraine-africa-food-security/

Oniszczuk-Jastrząbek, A., Czermanski, E., & Cirella, G. T. (2020). Sustainable supply chain of enterprises: Value analysis. *Sustainability, 12*, su12010419. https://doi.org/10.3390/su12010419

Pereira, P., Bašić, F., Bogunovic, I., & Barcelo, D. (2022). Russian-Ukrainian war impacts the total environment. *The Science of the Total Environment, 837*, 155865. https://doi.org/10.1016/J.SCITOTENV.2022.155865

Politanskyi, V. S. (2017a). Svitovi modeli ta fundamentalni pryntsypy informatsiinoho suspilstva. *Nauk Visnyk Uzhhorodskoho Natsionalnoho Universytetu Seriia Pravo, 43*, 34–39.

Politanskyi, V. S. (2017b). Informatsiine suspilstvo v Ukraini: Vid zarodzhennia do sohodennia. *Nauk Visnyk Uzhhorodskoho Natsionalnoho Universytetu Seriia Pravo, 42*, 16–22.

Ponomarenko, L. V. (2017). Innovatsiini pidkhody do poperedzhennia radykalizatsii nastroiv i proiaviv ekstremizmu v konteksti zabezpechennia staloho demokratychnoho rozvytku. *Informatsiina Bezpeka Liudyny Suspilstva Derzhavy, 1*, 74–81.

Potii, O. V., Korneyko, O. V., & Gorbenko, Y. I. (2015). Cybersecurity in Ukraine: Problems and perspectives. *International Journal of Information Security, 32*, 71–94. https://doi.org/10.11610/ISIJ.3201

Potnis, D. D. (2014). Beyond access to information: Understanding the use of information by poor female mobile users in rural India. *The Information Society, 31*, 83–93. https://doi.org/10.1080/01972243.2014.976687

Ratten, V. (2023). The Ukraine/Russia conflict: Geopolitical and international business strategies. *Thunderbird International Business Review, 65*, 265–271. https://doi.org/10.1002/tie.22319

Roller, V., Gogonyants, S., & Koropatnik, I. (2019). Legal background of cyber defence in Ukraine. *Journal of Scientific Papers Social Development & Security, 9*, 74–86. https://doi.org/10.33445/SDS.2019.9.4.5

Roztocki, N., Soja, P., & Weistroffer, H. R. (2019). The role of information and communication technologies in socioeconomic development: Towards a multi-dimensional framework. *Information Technology for Development, 25*, 171–183. https://doi.org/10.1080/02681102.2019.1596654

Shatun, V. T. (2016). Informatsiina bezpeka: Nevidiemna skladova natsionalnoi bezpeky Ukrainy. Nauk Pr Chornomorskoho Derzhavnoho Universytetu Im Petra Mohyly Kompleksu. *Kyievo-Mohylianska Akad, 267*, 174–180.

Shemayeva, L. G., Shemayev, V. V., Franchuk, V. I., Sidak, V. S., & Dragan, I. O. (2019). Estimation of ICT impact on indices of foreign trade security of a state. *Financial and Credit Activity Problems of Theory and Practice, 3*, 414–422. https://doi.org/10.18371/FCAPTP.V3I30.179820

Shevchenko, I. Y., Nepomnyashchyy, O. M., Marusheva, O. A., Medvedchuk, O. V., & Lahunova, I. A. (2020). Marketing communications management in the public administration system. *International Journal of Criminology and Sociology, 9*, 2882–2890. https://doi.org/10.6000/1929-4409.2020.09.353

Shimchenko, L. (2019). Cyber-threats in Ukraine as a problem in conditions of geopolitical rivalry. *University Economic Bulletin*, 70–76. https://doi.org/10.31470/2306-546X-2019-40-70-76

Shpiro, S. (2023). The United Nations and the Ukraine war: The limits of international conflict resolution. *Security Science Journal, 4*, 25–36.

Simakhova, A. O. (2018). Sotsialni perspektyvy rozvytku nauky ta tsyfrovoi ekonomiky v Ukraini. *Sotsialna Ekonomika, 56*, 216–221.

Smolyanyuk, V. F. (2018). Systemic principles of national security of Ukraine. *Nyuu Bulletin of Yaroslav the Wise: Series: Philosophy, Philosophy of Law, Political Science, Sociology, 2*, 107–126.

Spring, C., & Cirella, G. T. (2022). Fostering sustainable development: Green energy policy in the European Union and the United States. In *Human settlements: Urbanization, smart sector development, and future outlook* (pp. 101–137). Springer.

Streltsov, L. (2017). The system of cybersecurity in Ukraine: Principles, actors, challenges, accomplishments. *European Journal for Security Research, 22*(2), 147–184. https://doi.org/10.1007/S41125-017-0020-X

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal, 30*, 30–35. https://doi.org/10.1016/J.TEJ.2017.02.006

Svintsytskyi, A. V. (2022). The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova, 20*, 287–305. https://doi.org/10.21830/19006586.903

Tkachuk, T. Y. (2017a). Informatsiina bezpeka: Suchasni pidkhody do vyznachennia katehorii. *Aktual Pyt Publichnoho Ta Pryvatnoho Prava, 2*, 45–54.

Tkachuk, T. Y. (2017b). Skladnyky informatsiinoi bezpeky: Analiz kryteriiv. *Visegrad Journal on Human Rights, 4*, 153–158.

Tkachuk, T. Y., Chystokletov, L. G., Pavlov, D. M., Shyshko, V. V., & Ostapenko, L. O. (2020). Formation of axiological system of information security of the state: Experience of Ukraine. *Rivista di Studi sulla Sostenibilita, 2*, 50–62. https://doi.org/10.3280/RISS2020-002-S1005

Van Cuilenburg, J. J. (2016). The information society: Some trends and implications. *European Journal of Communication, 2*, 105–121. https://doi.org/10.1177/0267323187002001006

Willett, M. (2022). The cyber dimension of the Russia–Ukraine war. *Survival, 64*, 7–26. https://doi.org/10.1080/00396338.2022.2126193

World Data, UN. (2023). Country comparison: Russia/Ukraine. *Worlddata.info*. Retrieved August 8, 2023, from https://www.worlddata.info/country-comparison.php?country1=RUS&country2=UKR

Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management, 18*, 195–210. https://doi.org/10.21511/PPM.18(3).2020.17

Yemelyanov, V., & Bondar, H. (2019). Cyber security as a component of national security and cyber protection of critical infrastructure of Ukraine. *Public Administration and Regional Development*, 493–523. https://doi.org/10.34132/PARD2019.05.02

Zinets, N., & Williams, M. (2019). No gas? No votes. Subsidy cuts imperil Ukraine leader's reelection bid. *Reuters*. Retrieved August 28, 2023, from https://www.reuters.com/article/us-ukraine-election-economy-insight-idUSKCN1QH0TF

Zolotar, O. O. (2017). Dosvid pravovoho zabezpechennia informatsiinoi bezpeky v krainakh skhidnoho partnerstva. *Lex Portus, 3*, 70–80.

Zonneveld, M., Patomella, A. H., Asaba, E., & Guidetti, S. (2019). The use of information and communication technology in healthcare to improve participation in everyday life: A scoping review. *Disability and Rehabilitation, 42*, 3416–3423. https://doi.org/10.1080/09638288.2019.1592246