Values for the Cyber Security Strategy for a National Critical Infrastructure

Sorin TOPOR
National Institute for Research and Development in Informatics - ICI Bucharest
sorin.topor@ici.ro

Abstract: This paper provides a philosophical analysis of the values involved in developing a cyber security strategy for a national critical infrastructure. In the framework of the paper, we propose a matrix for the cyber attacks analysis that allows the establishment of some limits of cyber security in national security, with an emphasis on the ethics of using AI for the critical infrastructures' protection. Based on the proposed values in order to establish the limits of national cyber security and the analysis of the components of digital and non-digital technologies, we conclude the education and professional retraining can represent sustainable solutions for creating the digital and democratic legislative premises which are the apparent direction of modern states.
Keywords: ethical values, cyberattacks analysis, cyber security.

INTRODUCTION

Based on the tense climate on Romania's Eastern border and the changes in the global security environment generated by the unpredictable evolution of the technologies used in the war in Ukraine, our state must continue its extensive process of achieving robust defense and deterrence capabilities, a process started in 2015. They maintain their main targets of Romania transforming into a resilient state capable of withstanding and countering any hybrid aggression (Presidential Administration, 2020: art. 6). Thus, in addition to the correct dimensioning of defense capabilities, and the development of a solid national security culture, or other capabilities that ensure resilience and good governance for the benefit of all citizens, the protection of critical infrastructures remains an extremely important target that must benefit from funds for technological development and staff training.

The current known threats to critical infrastructures are of a diverse, complex and interdisciplinary nature, from physical and cyber to informational ones, with an emphasis on those in the public information environment where, based on deepfake techniques, adversaries can carry out extensive disinformation campaigns, fake news dissemination etc., with harmful and destabilizing effects, thereby generating new security challenges (Presidential Administration, 2020: art. 7-9).

In this paper, we want to present the results of our analysis of the ethical values involved in

https://doi.org/10.54851/v5i1y202309

cyber security, a basic component of national security, in particular for the protection of critical infrastructures.

As a rule, under the concept of a state's critical infrastructures, we mean a physical, non-physical and cyber resources and services that are fundamental to the minimal acceptable operation of a society and its economy (Government of Romania, 2010). A well-configured and secure ICT system, its networks and services are essential in ensuring public welfare, the economic stability of a state, ensuring energy stability, legislative security and, last but not least, the optimal pursuit of military operations.

Therefore, the stability, security and resilience of cyberspace is a national security essue. Vulnerabilities in cyberspace can be exploited to affect the operation or enact the physical destruction of one or more elements of critical state infrastructures whose operations are based on ICT networks and services. In this context, some state institutions must have privileged access to the services and networks involved. Thus, the institutions of the national defense system, such as the army, the police and the intelligence services, which have the main mission of maintaining the security and defense of the state, can act to verify compliance with the law and carry out activities to fight against crime and terrorism. However, the main dilemma is when to act, depending on the given situation. To combat crime, no matter how serious, we start with the collection of evidence and the criminal analysis only after the fact, while, in terrorism, the effectiveness of starting a post factum action can no longer lead to a prevention or thwarting of the attack. While making this observation, we understand that the privileged access of some information institutions can endanger essential values that ensure the functioning of the rule of law. Moreover, the excessive application of cyber security measures can create conditions of discrimination in citizens' access to information resources and services, with great implications for economics, freedom of comunication and movement, or which limit the autonomy of the population and violate the right to people's private lives.

The identification and discussion of ethical issues and the analysis of value conflicts involved in cyber security taking place at the national level, with influences on the international security environment, are fundamental aspects related to the understanding of cultural values and support the activity of national security organizations.

THE MAIN VALUES AGAINST WHICH NATIONAL CYBER SECURITY IS MEASURED

To solve these issues, we believe that the main milestones are the identification of vulnerabilities of a critical infrastructure and their neutralization in relation to a potential cyber security conflict and the values-based discussion it engenders. The main goal is to raise awareness of cybersecurity values and to stimulate the generation of views and discussions about cybersecurity values in the field of national security.

From the specialized papers, we have identified and accepted as a reference system two directions for the analysis of the related cyber security issues in the field of national security, namely:

- The interest and urgency in the development by the state of appropriate strategies, policies and laws for the national defense and protection of citizens against cyber attacks; and
- The difficulty and complexity of managing and implementing countermeasures against cyber attacks. It is well known that a cyber attack can cross the national borders, blocking connectivity and access to global information networks is almost impossible and produces serious economic losses, hampers the information comfort of the population and, last but not least, creates new vulnerabilities for data protection, as well as denying some surveillance measures or the stability of ICT networks and systems.

Without considering that we have analyzed all the potential conflicts that may arise between

the ethical values specific to a crisis or cyber warfare with implications for national security, we would like to present the following points:

- One of the intensely scrutinized topics is cyber terrorism. Some authors argue that it exists and contains everything related to cybercrime performed by terrorists or extremists to promote their political and ideological goals in global cyber networks. Thus, the Internet becomes a forum for the dissemination of hate messages, for the encouragement of violence, for radicalization etc., but also for the facilitation of communication and the exchange of ideas between terrorists, between them and their sympathizers etc. Even if there are no confirmed cyber-attacks with a destructive effect carried out by terrorists on critical infrastructures, some conclusions are formulated such as that they tried to attack computer networks belonging to critical infrastructures, but also other entities such as press agencies. The worst cyber attacks attributed to cyber terrorism have been supported by state sponsors of international terrorism, known as cyber warfare. Among them we list the cases of NotPetya (2017), the cyber attack against Estonia (2007) and Titan Rain (from 2003-2007, the first information being in 2005).
- The information technology revolution has also produced changes in espionage techniques, giving rise to the so-called cyber espionage. Essentially, this is an asymmetric threat where someone illegally uses IT devices and networks to gather information about a target by exploiting its vulnerabilities. For a state an attack of this kind is a serious problem compared to the security risk for any of its institutions. A cyber espionage attack can have serious security effects on critical infrastructures for which national security planners still have no objective answers. All this is due to the increased dependence on IT systems and connections to global information networks. Therefore, governments should make commensurate investments in security, databases, networks and incident response systems to cyber espionage.
- Moreover, the lack of adequate legislation and the harmonization of existing rules with other law provisions can produce unwanted effects on national security through an ineffective approach to protection against cybercrime (Alexandru, Vevera & Ciupercă, 2019). It is known how many problems the implementation of GDPR at the European and national level has produced for the business environment. Cyber security laws are extremely important in preventing, identifying, investigating and prosecuting individuals who have committed cyber crimes, for the effective resolution of such crimes.
- Early education and the formation of a cyber security culture are about raising awareness of cyber threats and vulnerabilities, as well as understanding the impact of cyber values on society as a whole. Through proper education, raising awareness about how to behave online and protect themselves against cyber attacks, individual and corporate users will become more proficient in this issue. This is achieved not only through professional training programs but also through a variety of methods that usually belong to the field of public communication and speaking (Ciupercă, Vevera & Cîrnu, 2019).
- Moreover, the formation of appropriate behavior on the part of users of cyber systems and services represents an ethical value of national security. Through behavioral analysis, people are analyzed, classified and assessed by comparing general profile patterns. Profiling is used for a wide range of purposes and by various actors. The most well-known is the judiciary. Police officers do a behavioral analysis for the easy identification of criminals according to certain psycho-social characteristics. More recently, this technique has also started to be used by security services to identify terrorists, or by some companies to identify

consumer behavior, by banks to decide whether and to whom to offer a loan etc. As these examples already suggest, behavioral analysis techniques are used to ensure the security of some services. On the other hand, profiling can cause a multitude of unrealistic prejudices, suspicions, false accusations and even, in extreme cases, unjustified punishments. Therefore, the use of profiling techniques is useful only in the situation of the existence of a lot of information from various sources, being a method of statistical analysis of a representative database for the group to which the analyzed person belongs. For establishing profiling, the method of obtaining information may involve breaches of confidentiality. That would not be the biggest problem but the fact that, by virtue of the probabilistic nature of the information, the result may not be representative of that person. Consequently, profiling can lead to stereotyping and discrimination. The pattern of attempts to identify individuals suspected of terrorist activity solely on the basis of information provided by facial recognition technologies is well known. For example, quite a number of criminals may have physical and other characteristics in common, pertaining to a certain ethnicity, socio-economic status and personal situation, but that does not mean that any one individual fiting such a description is likely to be a criminal.

Returning to the two directions of the reference system for our analysis, related to cyber security in the field of national security, we propose a series of models as follows:

Cyber Security Related to Privacy and Data Protection

The exchange of information between private entities and the state is a critical issue with implications for achieving adequate cyber security. Insufficient information collection will distort the analyzed results and prevent the identification of an optimal defense strategy against an attack. Cyber attacks on some services provided via the Internet can make vulnerable all information stored in the cloud, can affect online surveillance applications of security companies, can distort e-mail communications etc. Moreover, given that the national cyber infrastructure is owned and operated by private entities as well, cyber security strategies should indicate norms also for the private sector, the basic reason being to reduce all risks posed by cyber security issues to systems. From the point of view of defense policies, everything seems correct. The conflict of values occurs when, through the lens of combating cybercrime and cyberterrorism, norms are violated in the most brutal ways that can affect the privacy and private life of the people in a company, of their families and those close to them.

However, security is an essential condition for ensuring confidentiality in the field of national security, especially for the protection of data, for their ownership, for the control of access to information, for the security of systems etc. The level the compromise we will reach on these values can only be determined through analysis, communication and awareness.

Individual Security in Relation to State Security

When discussing topics related to the security of critical infrastructures, the personnel of that system is considered a systemic element and is not analyzed individually. In order to achieve national security, the requirements for achieving systemic security must be harmonized with those specific to individual security. Failure to consider people's security values will have a detrimental effect on the entire system. We are not only referring to the identification of people who can sabotage the activity of the system in order to express their individual frustrations, dissatisfactions or unfulfillments, but also to simple errors produced by fatigue, inattention or other uncommunicated personal causes etc., the effects of which can produce vulnerabilities that can be exploited by an aggressor.

Accessibility and Connectivity in Relation to National Security

It is clear that cyber attacks cross national borders and are increasingly difficult to combat and manage. That is why more and more states are creating and implementing strategies, rules or initiatives aimed at defending and protecting against cyber attacks (Dinu, 2022). Moreover, it increases accessibility of information. More and more consumers have access to global information markets for economic and international communication purposes. However, many Internet users are not fully aware of the reality of cyber threats and are not trained to protect themselves against these threats, becoming victims or perpetrators of online vulnerabilities themselves, thus increasing insecurity in cyberspace.

Connectivity in Relation to Equity in Access to Digital Information

Today, a modern society is characterized by global communication and access to digital information. However, not all individuals in a state have the same level of access to digital information and communications technology. The reasons can be multiple, starting with the effort to create a network infrastructure in a different geographical area and continuing with network traffic speed. Regardless of the reasons, the inclusion and equity of access to digital information, connectivity, accessibility of consumers and producers to global informational and economic markets, transnational communication, learning and entertainment should be guaranteed to all citizens of a modern state.

Confidentiality in Relation to Trust

Confidentiality prevents disclosure of information to unauthorized persons or systems. The impact of cyber threats could reduce public access and damage confidence in Internet transactions. Thus, it is necessary to ensure an adequate information and communication infrastructure that fosters trust in technology and demonstrates that it is able to withstand attacks that affect privacy and to thereby protect their privacy.

Even if the generalization of the analysis report of national digital security in relation to ethical values, we believe that the establishment of several models will lead to the limitation of conflicting states in various fields that circumscribe the state of national security. We do not advocate the use of excessive cyber security measures, but optimal and appropriate ones. In this regard, we would like to recall the extensive discussions generated by the requirement of some governments and intelligence services to access encrypted communication from applications such as the WhatsApp and the Tor network. Even if the main motivation of the requester was fully justified and consisted in identifying information that would detect and avoid potential terrorist attacks, there were a number of opponents who invoked the lack of confidentiality, damage to democracy and the effort to undermine the authorities of totalitarian and suppressive regimes. It is well known that Tor users have hacked the Democratic Party's computer system during the US election (Nl#times, 2017). The Tor server is owned by Rejo Zenger, an employee of Bits of Freedom which is a Dutch digital rights organization that defends privacy and freedom of communication in the digital networks. While Zenger acknowledges that Tor servers can be used by criminals/terrorists and pose a cybersecurity threat, he believes that this is a price worth paying, not only for privacy reasons, but also because these servers can be critical for alarm signals about abuses. Therefore, the ethical value is not only a value for the state of privacy but also for a number of civil liberties that are considered crucial for a democracy and a democratic process.

Another aspect revealed by the conflict between ethical values and national cyber security comes from the facilitation of economic and political power imbalances. Economic monopolies or oligarchies are not specific to a democratic system. Democracies are based on

the balance of political power between citizens and their government, an important factor in a healthy economy. Having information about citizens and their behavior can give more power to some actors, a situation that will lead to political, social and/or economic imbalances. Campaigns to collect information about users and their behaviour made by Google and Facebook have generated extensive stances, even if their main motivations have been of economic not political origin. It should be noted that these techniques are unethical even if the data is anonymized or if individuals have given their informed consent to the collection, storage and use of their data. Consequently, even when privacy concerns are properly addressed, the accumulation of large amounts of data for a given actor can be considered a problem for both economic and political reasons.

THE CRITICAL INFRASTRUCTURES CYBER SECURITY

There are many definitions of critical infrastructure. The Romanian government has regulated the field of critical infrastructure protection by establishing a series of definitions applicable throughout the country. Thus, national critical infrastructure means (translated into English) "an element, a system or a component thereof, located on the national territory, which is essential for maintaining the vital functions of society, health, safety, security, social or economic well-being of individuals and whose disruption or destruction would have a significant impact at the national level as a result of the inability to maintain the respective functions, as well as the project of a strategic objective of national interest whose construction is imperative to safeguard the national interest" (Government of Romania, 2019).

By comparison, we can see that all definitions include the idea that national critical infrastructures are of general use, important for various types of human activities, especially economic activities, but also for activities necessary to protect national security and health. Although today, all components of a critical infrastructure are based on ICT networks and services, not all are equally vulnerable to cyber attacks. For example, hospitals and communication systems, energy, banking etc., all rely on cyber components making them targets for an attacker. Conversely, road infrastructure is not so attractive as a target for a cyber-only attack without physical destruction vectors.

Therefore, we consider that attacks on a national critical infrastructure can be classified according to the mode of execution into merely cyber attacks and physical attacks with a cyber component, and according to the effects they produce into attacks resulting in only material damages, material and functional damages and in merely functional damages (see Table 1).

We describe the six possible combinations of means of attack and the expected results in the following table:

Table 1: *Types of potential attacks on national critical infrastructure*

Damage / Attack means	1. Merely material	2. Material and functional	3. Merely functional
A. Physical and cyber	A1	A2	A3
B. Merely cyber	B1	B2	B3

Regarding the damage caused by an attack we can distinguish the following effects: Merely material (1), Material and functional (2) and Merely functional (3). In our classification, when the attack is Merely functional (3), the damage effects are only on information and there is no direct material damage. For the Material and functional attack class (2), the effects are accumulated by evaluating the degree of damage to those critical infrastructure

components that can be removed in different time values. And in an attack with Merely material effects (1), the targets attacked may be material elements of the critical infrastructure as well as the personnel and staff.

In order to effect the modelling of physical destruction, there are numerous research projects and studies from the institutes and centers for the protection and security of citizens, which clearly show the importance of increasing the resistance of material structures against various types of explosions, especially after studying the effects of a terrorist attack on Twin Towers (WTC-USA, 2001). Regarding the study of the effects of cyber attacks on critical infrastructures, there are some specialist studies that address the physical and cyber components together by analyzing the methods of attack on the security and control systems necessary for critical infrastructure operation. As for the information attack in the cyberspace related to a critical infrastructure, the studies approach this issue in two distinct directions: information as an environment in which only communication techniques are used and information as an element (measurable in bits) in which formulas based on the general theory of information transmission rates are the most important (Shannon's Law).

From an ethical point of view and based on the law of armed conflicts applicable to cyber warfare, a quite controversial criterion in the legal function as a measure that legitimizes a military response depending on the severity of the cyber attack, all these issues become extremely complicated. This approach is aimed at reacting to an attack that leads to the physical destruction of a single server and not the incapacitation of critical infrastructure. According to this criterion, a cyber operation counts as a physical attack if „restoring functionality requires the replacement of physical components" (Schmitt, 2013: 108).

The classification of attacks according to the effects produced on a critical infrastructure, by measuring them against the previously presented cyber security values, aims to optimize the identification of vulnerabilities and establish specific risk management procedures, in order to increase the global security of a national critical infrastructure (Bucovețchi et al., 2018). We believe that an attack on cyberspace can be Merely cyber (eg, a virus or trojan) or Physical and cyber (eg, E-bomb, a Stuxnet malware etc.). We ignore a purely physical attack, even if it causes major material damage, because it does not belong to the domain of cyber defence. For example, destroying a bridge for a road or rail infrastructure, destroying a cargo ship or chemically contaminating a water tank are not cyber attacks.

We consider that the Physical and cyber attack class (1) includes those that produce only material damages (A1), such as the Ukrainian drone attack on the Novoshakhtinsk refinery (22.06.2022), of the Material and functional type (A2) as sabotaging the Nord pipelines Stream 1 and 2 (26.09.2022) and Merely functional (A3) as the irresponsible decision to limit fuel consumption leading to national blackout in Pakistan (23.01.2023). Obviously, the example chosen for the A3 model is not a physical attack by definition, but the overall effect is to disable the functions of several critical national infrastructures without the need to replace any cyber components.

Understanding the patterns of Merely cyber attacks is much easier because they are related to the cyber tools with which they are executed. Thus, for the B1 model the best example is Stuxnet, the malware that targeted Siemens software and operated in Iran's uranium enrichment facility (2010), specifically on the industrial control system for the enrichment centrifuges. The software was created to physically damage nuclear power plant cooling turbines. Model B2 encompasses attacks that disrupt the information infrastructure and cause damage. The most dangerous attack of this type was carried out with the Triton malware (2017). It allowed hackers to take control of the safety systems of a petrochemical plant in Saudi Arabia, allowing the physical destruction of the infrastructure and the release of toxic gas into the atmosphere. The initial attack method was spear phishing also benefiting from the identification of a vulnerability in the cyber security system, i.e. a misconfigured firewall.

B3 attacks target information without causing physical damage. This includes the most publicized examples of cyber attacks, from DDoS attacks to bots and AI in social networks. One such example is the attack on Taiwan's CPC Corp (2020), a company responsible for the delivery of petroleum products and the import of liquefied natural gas. Although production remained undamaged, the attack targeted the payment system, rendering payment apps useless and customers unable to use VIP payment cards, generating chaos.

We observe that a global critical infrastructure such as the Internet network can, at a certain moment, be the support of an attack that causes physical or functional damage. Material damage is the effect of hitting one or more hardware or software components. A network can be vulnerable to physical and cyber attacks, or only cyber attacks. Thus servers, antennas or other network elements can be hit. The global effect is measurable by the impacts produced on the population, i.e. blocking access and connectivity to the Internet, reducing, slowing down traffic or generating errors.

Currently, the analysis of the typology of cyber attacks is extremely important due to the number and complexity of vulnerabilities that can appear at the level of a critical infrastructure. The typology develops through the CIs expanding their digitalization of processes and digitization of data and implementing artificial intelligence with various destinations for the collection and analysis of information, for the development of Internet-of-things applications, through 5G implementation, because of the lack of specialized personnel on the labor market etc. Physical and functional isolation of components is not a solution. Only a development of cyber security capabilities and a good training of key personnel and general staff can constitute solutions to limit vulnerabilities and improve the ability to defend critical infrastructures. This requires adequate time and funds, allocated to both scientific research and public education programs. Improving preventative measures is a compromise strategy in a short timeframe, that can solve the maintenance issues of national cyber security, until the appearance of other technologies that, even if they would ensure a certain level of social comfort, would produce new vulnerabilities at the level of critical infrastructures and, implicitly, require new research to identify solutions to neutralize them. On the other hand, the persistence of the conflict state between technology and the ethical values of cyber security will lead to compromises in the economic development policy of the state even if, in the short or medium term, there will be mainly social inconveniences such as the loss of jobs, the need for professional reconversion, for workforce migration etc. It is clear that the introduction of artificial intelligence-based technologies at the level of national critical infrastructures will generate additional social and economic value. At the same time, hacking tools will be developed, which will produce new types of cyber attaks.

For example, the use of self-driving drones in delivery services will develop the systems and trade service in that area. However, a drone under terrorist control can represent an effective vector strike against which there is no legal system to analyze and frame the act. Such a hacked drone can hit a hospital, a person with an important position in the political-administrative system, a public square or any local critical infrastructure. Another hypothetical example is that of human trafficking recognition and monitoring systems, extremely necessary tools to fight against crime and terrorism. Who is to stop us from thinking that they couldn't also be used in deepfake applications, with the overall effect of producing misinformation and diversions in social networks and maintaining disorder in an area of interest?

CONCLUSIONS

Cyber technology is a core component of national critical infrastructures. This has a dual role. It can be used both defensively and offensively by exploiting the vulnerabilities it generates. Implementation of AI technology is extremely important in cyber defense applications such as spam filters, malware detectors, facial recognition technologies

and other applications useful in criminal investigations and the fight against terrorism. This can generate conflicts between the presented values as: security vs. confidentiality, non-discrimination vs. national security, cyber security vs. network security etc.

Hackers are not the only ones responsible for cyber problems. Often abuses and excessive servility (human characteristic), based on lack of education and a minimal cybersecurity culture, can produce vulnerabilities in critical infrastructures.

Regardless of the objectives, the democratic values of a society must not be affected. As is known, AI can be used to identify physiological and behavioral patterns of people, but the intelligence methods and databases must respect all the rules of confidentiality and data protection.

In addition, the monitoring and classification of social groups based on social patterns must be extremely carefully used without causing discrimination and compromises. AI must be used with great care.

Education is extremely important. In the background of the decline of interest of youth in reading, an excessive and long-term use of AI applications in educational programs may lead to the dissolution of the school as an institution. In order to prevent such a trend, a professional retraining of the personnel must be carried out. Undoubtedly, the lack of such programs for teachers and professors will lead to the staff dequalification, which will produce an acute lack of specialists for the labor market.

Creating an adequate law system is an emergency for any state. Especially through the prism of the lessons learned from the Ukraine war, the appearance of the premises of a new arms race in the cyber environment must be acknowledged. In a global cyber warfare all actors involved will lose.

Thus, without responsible behavior in cyberspace, where AI is only a functional extension of the population, all technological developments will lead to the collapse of high-tech society. We will go back to the industrial age without understanding why. That is why we insist on the creation and, to some extent, the imposition of educational and continuous learning programs by the Ministry of Education, in various forms, by educational goals according to ages and according to professional training categories. These can take place in various forms such as: games, courses, media debates, thematic competitions with attractive prizes etc.

It is obvious that cyber adversaries will become quite efficient as well. But this situation must become a stimulus for performance and for the establishment of fair rules in cyberspace, their non-compliance leading both to coercive measures and to a lack of attractiveness to the policies and ideologies promoted by them.

In this paper, we proposed that through a philosophical approach to ethical values and the establishment of a cyber attacks analysis matrix, we would add value to the way of establishing a cyber security strategy for a national cyber infrastructure. It is observed that an increased connection of digital technologies with non-digital ones allows the identification of new solutions that raise awareness of the increased need for education and professional reconversion, adapted to the requirements determined by cyberspace and the implementation of artificial intelligence technologies. And all this through the permanent pursuit of adapting and maintaining an adequate legal framework aimed at strengthening information security, defending digital resources against all kinds of attacks, software and hardware confidentiality etc., all representing essential conditions of an increased national cyber security.

REFERENCE LIST

Alexandru, A., Vevera, A. V. & Ciupercă, E. M. (2019) National security and critical infrastructure protection. *International Conference Knowledge-Based Organization*. 25(1), 8-13. doi: 10.2478/kbo-2019-0001.

Bucovețchi, O., Georgescu, A., Lazăr, M. & Cîrnu, C. E. (2018) A critical space infrastructure perspective on Romanian national security. *Romanian Journal of Information Technology and Automatic Control [Revista Română de Informatică şi Automatică]*. 28(3), 31-40.

Ciupercă, E. M., Vevera, V. & Cîrnu, C. E. (2019) Social variables of cyber security educational programmes. In: *The 15th International Scientific Conference „eLearning and Software for Education", 11-12 April 2019, Bucharest.* pp. 190-194.

Dinu, M. Ș. (2022) The cyber domain - aspects with impact in the assessment of the security state of the states [Domeniul cibernetic - aspecte cu impact in evaluarea stării de securitate a statelor]. *Journal of Military Science [Revista de Ştiinţe Militare].* 68(3), 102-110. Romanian Academy of Scientists Publishing House.

Government of Romania. (2010) *GEO no. 98/2010 regarding the identification, designation and the protection of critical infrastructures, with amendments and additions, The Official Monitor no. 757 from 12th November 2010 [OUG no. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, cu modificări și completări, Monitorul Oficial nr. 757 din 12 noiembrie 2010].*

Government of Romania. (2019) *GEO no. 61/2019 for the amendment and completion of the GEO no. 98/2010 regarding the identification, designation and protection of critical infrastructures, approved with amendments by Law no. 71/2021 Monitorul Oficial nr. 717 from 30th August 2019 [OUG no.61/2019 pentru modificarea și completarea OUG nr.98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 71/2021, Monitorul Oficial nr. 717 din 30 august 2019].*

Nl#times (3 January 2017) *Dutch servers used to hack U.S. Democratic Party.* https://nltimes.nl/2017/01/03/dutch-servers-used-hack-us-democratic-party [Accesed 09 February 2023].

Presidential Administration. (2020) *National Defence Strategy 2020-2024 [Strategia națională pentru apărare a țării pentru perioada 2020-2024].* https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.

Schmitt, M. N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge, Cambridge University Press.