STRENGTHENING THE SECURITY CULTURE IN ROMANIA

Bianca-Elena STAN (PREDOANĂ)[*]
Ana-Rodica STĂICULESCU[*]
Marius-Răzvan PREDOANĂ[*]

Abstract:
The current security context requires proper and consolidated solutions in order to lower the number of risks posed by the ongoing national security threats. Strengthening the security culture is one of these solutions, as it can ensure the engendering of desirable attitudes towards existing security risks. Shortly, security culture is a combination of knowledge and attitudes toward the security issues of the state. In Romania, since 2010, the consolidation of security culture is an assumed objective within the National Defence Strategies. Over time, different Romanian institutions have taken several steps to achieve this goal, but a main actor is represented by the Romanian Intelligence Service, as it took multiple measures in order to have a better-informed population and better trained authorities. In addition, the National Cyber Security Directorate has been actively involved in strengthening the cybersecurity culture, an extremely important branch of the security culture. Taking into consideration that every human activity is more and more connected to the cyber space, people have to face many risks coming from this direction.

In this article you will find information about some measures taken in Romania in order to strengthen the security culture. The main objective of this article is to emphasize the importance of creating a common security culture, but also to spot the limits of such a process. For accomplishing this objective, it was used "literature review" as a research method.

Keywords: *security culture, strategy, risks, defence, training.*

Introduction

What is security culture? Why is it important? What are the benefits brought to the state and to its citizens? What are the tools of

[*] PhD Student, University of Bucharest, email: bianca-elena.stan@s.unibuc.ro
[*] Professor "Ovidius" University of Constanta, email: ana.staiculescu@unibuc.ro
[*] PhD Student, University of Bucharest, email: marius-razvan.predoana@s.unibuc.ro

Romanian authorities for strengthening the security culture? All these questions represent the main objectives of this article, along with the desire to make a topic that lacks public attention more visible, even though it is of a great importance: security culture. The research method used was "literature review" by integrating multiple data from different findings and perspectives.

Security culture is a new concept that incorporates various meanings from a micro environment to the state or interstate level. This can be considered a branch of national and universal culture, but it becomes more than that, as it is a vital dimension for the strategic leadership. Security culture refers to a set of knowledge and attitudes towards the security issues that a state face. So, the purpose of the security culture is to help the citizens of a society to be aware of the potential dangers and to encourage them to participate in the process of achieving national interests. The security culture is rather an ongoing process, because the knowledge fund needs to be constantly updated and connected to the dynamics of the regional and global security environment.

Snyder (Ustun, 2010) defines security culture as a set of ideas, emotional answers and patterns of behaviour that members of the national strategic community acquired through training, imitation or exchange of knowledge on strategies. So, Snyder focuses his definition on security culture at a managerial level. This level is essential, preliminary, in the process of consolidating security culture among population.

More recently, Chiru (2016, p. 65) defines security culture as an "interrelated set of information, values, attitudes about security, which shapes security behaviours of social individuals, including perceptions of security risks."

Why is security culture important?

The post-Cold War era brought a significant shift in the use of power, from the hard power (military) type, to the soft one, which focuses more on the economic level. This shift has also led to considerable changes in the "war" meanings. Today, "war" has a new content and several forms of manifestation. Decreasing trust in the state institutions, declining social cohesion and denying national values can be

new forms of an unseen war, a slow one, whose battlefield has become invisible. Unfortunately, the changes brought by the end of the Cold War cannot be stopped, diminished or excluded. Also, the forms of manifestation of future threats cannot be anticipated, but preventive measures can be taken in order to ensure the continuity of the state, even if society faces black swan scenarios.

In this security context, raising the security culture among population (and especially among the leading factor) might be a useful prevention measure. The security culture must provide the individual with a complex ability of understanding a large spectrum of security issues – from how their own computer can be used by another person thousands of miles away to carry out a cyber-attack, to the advantages and disadvantages of using shale gas (Munteanu, 2013). The security culture is an absolutely necessary pillar, also because of the fact that it determines favourable attitudes and behaviours that lead to individual and state security.

Security culture meets the following specific goals and needs followed by the leading factors that have responsibilities in the security field (Piwowarski, 2017):

a) effective control of high-risk and high-impact threats;
b) recovery of security in case of imbalances generated by different events;
c) optimizing the different levels of security understanding;
d) increasing individual and social awareness of the need for trichotomous development (mental/social/material).

According to Ioan Deac (2018), the security culture defines the group identity of a community/society and it ensures social solidarity around common goals that inspire devotion, loyalty, cohesion, sense of belonging and patriotism. Therefore, the security culture provides the implementation of a well-structured set of values, both within a social group and, also, at the individual level. This is utterly important, as values will directly influence the adoption of certain future attitudes. The attitudes will guide the individual's behaviour towards action/active involvement and in this way, society will finally have responsible citizens that take part into the national security ongoing process.

In a more theoretical approach, we can say that security culture brings its contribution through the functions that it possesses (Onișor, n. d.), which are often related to stability, integration and continuous progress.

The informative function ensures the population's general information regarding the security system structure, the political actions of its components, the national and common/collective security values (Onișor, n. d.). This function builds knowledge about the institutions responsible for national security, the inter-institutional cooperation, as well as the actions taken by them in order to ensure a safe environment. Moreover, the informative function creates a framework of the values and norms concerning individual and state security, which can influence desirable behaviours. This function develops in two directions, from the power factor to the population, but also from the population to the ruling class. This way, all the involved actors benefit from knowledge. First of all, the citizens are aware of the decisions taken by the rulers, as well as the basis on which they were developed. Next, the rulers are informed about citizens' choices, interests and grievances and about the ways their messages and actions are perceived. This set of data is extremely relevant as it could anticipate attitudes and behaviours on social, security and political issues.

The axiological function of the security culture points out how security values are perceived in connection with international politico-military phenomenon and, also, the concrete ways of establishing values in a national system (Onișor, n.d.). Through this function, a set of opinions, beliefs and ideas about security values are formed. These can generate acceptance, attachment and involvement or, on the contrary, indifference and rejection. Furthermore, these approaches lead to certain attitudes towards political and the security events that take place inside and outside a state, attitudes that can facilitate or hinder the governing process. Therefore, the security culture is an indispensable factor for the state stability, due to the fact that it creates a strong link between society and the ruling class.

The normative function refers to the way security values become norms, procedures, rules, techniques and security standards meant to give stability to the state and to ensure the state's contribution of the

international security (Onișor, n.d.). Besides these norms, the attitudes of the citizens are of great importance, but especially the attitudes of the institutional apparatus that must guide the citizens through own example. If the rules are not followed by those who drafted them, it will generate disobedience and indignation. It is essential that the rules and regulations governing internal and international security be accepted by a clear majority of the population, not only by a small community.

Thus, the security culture, through these three functions, provides a framework for the driving factor, but also an effective guidance to the citizens, as it offers a set of relevant information, attitudes and behaviours towards the state security.

Security culture – a strategic objective

The perception of risk is correlated with cultural factors, because the cultural models are those that establish a system of interpretation of facts and the attribution of emotions. In order for a whole population to have favourable, coherent and predictable perceptions and responses to a threat, it is absolutely necessary to create a common culture of security. One relevant and primary step towards this aim is represented by communication, especially, public communication on risks. An important channel is represented by official documents that stipulate current risks (for instance, the National Defence Strategy or other related documents).

The Guide of National Defence Strategy for 2015-2019 is an essential document that defines the steps which should be done for consolidating the security culture in Romania, both at the institutional and societal level. According to this document, the process involves a joint effort of society and institutions with responsibilities in the field of national security. The role of institutions is to ensure that the rights and freedoms of every citizen are respected, while the role of society is to inform and to provide institutions with relevant directions concerning all identified issues. The Guide mentions the definition of security culture in accordance with this approach: "a concept related to the need to learn generating security, both as a citizen or as a state" (Presidential Administration, 2015, p. 14).

The Guide promotes a public communication between citizens, organizations and institutions in the field of national security. As this

communication can only be shaped throughout a solid security culture, there were identified several steps for its consolidation (Presidential Administration, 2015):

- encouraging citizens to develop a security culture with the help of media products and other various related ways;
- introducing security culture in the education field through courses, conferences and so on;
- creating and promoting different informative materials;
- training security experts;
- continuous collaboration with national and international organisations that aim to strengthen the security culture.

For a proper communication it is imperative to be productive in the following three dimensions (Sandman, 1988): 1. Experts and society; 2. Experts and decision makers; 3. Decision-makers and society. It is, also, important how communication is carried out. Its content must be clear and concise, in order to be correctly received by the interlocutor. Possible distortions, generated by own interpretations of the content, can alter the message and, consequently, change the perception and attitude of those who receive it.

Consolidating the security culture in Romania

The Romanian strategic documents establish that security culture needs a joint effort made by both civilian and military institutions and also a continuous effort for raising awareness among population. The intelligence services are also responsible for promoting a security culture among population, because such a concept would ease their dialogue with citizens and other institutions of the state. No human being is born with a set of clearly printed instructions, so it is necessary to promote precise rules, regulations and values throughout effective informing channels and a better transparency of the institutions responsible for national security.

The Romanian Intelligence Service attaches great importance to strengthening the security culture, using various training methods, such as: meetings with civil society representatives, debates, conferences or various partnerships with academic or research institutions (Calangea, 2017).

The opening of Security Culture Information Centre (RIS, 2003) was an important step in fulfilling the mission of the Romanian Intelligence Service within the National Plan for Romania's Accession to NATO, Chap. IV, regarding the creation of a security education. This centre has led to increasing public communication and much more effective training of the citizens in relation to the security environment.

The Security Culture Information Centre was inaugurated on September 30, 2003 and it provides an organized framework for debating security environment issues. The "Security Culture" pilot program is addressed to students, researchers, the academic world, journalists and all those interested in the promotion of security culture and Euro-Atlantic values. Through this program, it is created a database consisting of studies, researches and reports of national and international organizations. This database must be available to the public and the debate groups that operate within the Centre.

Other relevant actions taken by the Romanian Intelligence Service in order to promote the security culture are (Calangea, 2017):

1. The campaign „Terorismul de lângă noi" ("The terrorism near us"). It took place between 2004 and 2010 and its purpose was to raise awareness among pupils, high school students and, last but not least, representatives of public authorities about the terrorist threat and its implications. The campaign was really useful in consolidating relevant knowledge in this field.

2. The international conference „Tu poţi preveni terorismul" ("You can prevent the terrorism", 2007). It took place at Cluj Napoca County Library and aimed to present the steps taken by the Romanian Intelligence Service to prevent and combat terrorism.

3. The round table conference „Societate, Democraţie, Intelligence" ("Society, Democracy, Intelligence", 2008). Its purpose was to identify the perceptions of population towards the Romanian Intelligence Service actions, but also to assess the need to strengthen the public relations regarding the area of intelligence.

4. „SRI în 50 de minute" ("SRI in 50 minutes", 2013) was a 50 minutes informative session that provided data on the security environment, as well as data about the proper ways to manage the security risks.

5. The debate „Evoluţii social media: o privire spre viitor" ("Social media evolutions: a look to the future", 2015) which focused on the new risks determined by the growing influence of social media on the public relations.

6. The master's degree program „Studii de Securitate – Analiza Informaţiilor" ("Security Studies – Information Analysis") offered by the Faculty of Sociology and Social Work of the University of Bucharest. It aims developing analytical skills among master students, as well as creating a strong security culture.

7. The international conference *Intelligence in the Knowledge Society* – organized annually by the "Mihai Viteazul" National Intelligence Academy in order to exchange experiences and good practices in the intelligence area among doctoral and postdoctoral students from Romania and abroad.

8. The student scientific communication session ANISTUD – organised, also, by "Mihai Viteazul" National Intelligence Academy for both civilian and military students. It promotes the share of knowledge and opinions through debates on various topics in the area of national security and beyond.

9. The journals – *Intelligence*, as well as Romanian Intelligence Studies Review are, also, important steps in consolidating security culture among society, as they provide essential knowledge in the field of national security and generate transparency of Romanian Intelligence Service and its activities.

10. The Romanian Intelligence Service online activity is, perhaps, the most powerful tool for increasing the security culture, because everyone is connected to the digital environment, so this way it is created a direct communication channel with people. The Romanian Intelligence Service has developed friendly web design websites, such as: sri.ro, animv.ro, intelligencestudies.ro or intelligence.sri.ro. Also, the Romanian Intelligence Service has an active presence on social platforms, including: Facebook, Instagram, Twitter and YouTube. Open-Source Intelligence (OSINT) plays an essential role in creating the security culture, as it constantly identifies the needs for change and adjustment of the Service's approaches in accordance to technological and social developments.

11. The Romanian Intelligence Service runs an awareness program, designed to raise awareness of risks, vulnerabilities and threats among employees of companies of strategic importance, but also among civil servants. Through this program, the Romanian Intelligence Service aims highlighting the main risks generated by the access to certain data; training these professional categories in order to adopt a counter-informative behaviour; emphasizing the importance of self-protection (Romanian Intelligence Service, 2017).

12. The Romanian Intelligence Service has carried out a campaign among high school and college teachers in order to help them identify possible cases of radicalization among young people. Once identified, teachers can report those behaviours or even help treating them. Strengthening the security culture among teachers represents an important measure, as teachers can pass on the knowledge to students and create security education among them.

In order to consolidate the security culture at the experts' level, there were also promoted many prevention and intervention programs for the representatives of the Romanian institutions (Romanian Intelligence Service, 2016):

- RAN (Radicalization Awareness Network) – it was developed in 2011 at the European Union level, with the participation of experts in the field of radicalization, among NGOs, academics or police and intelligence services.
- CoPPRa (Community Policing Preventing Radicalization) – it was created in 2010 within the European Union to train police officers in detecting radicalized persons. Personnel from the Romanian Intelligence Service, the Ministry of Internal Affairs and the Ministry of Justice also took part in this program.
- CLEAN-IT ("Fighting the illegal use of the internet with public-private partnerships from the perspective of counter terrorism") – it is a program developed by the European Commission in 2011 and our country is part of it. It is aimed to develop a set of rules and good practices that would stop the use of the Internet in carrying out terrorist activities.
- PLIR ("First Line Against Radicalization") – it is a program developed in 2014 by the Romanian Intelligence Service along

with the Ministry of Internal Affairs, being an extension of the CoPPRa program at the national level. Its purpose is also to train police officers to identify radicalized people.

Besides, the Romanian Intelligence Service pays close attention to the cybersecurity culture, as it became one of the most important parts of the security culture. According to the Service official website, any person is exposed to cyber risks, but the main targets are represented by the Romanian state institutions (SRI, 2018). However, even when it comes to institutions, the main vulnerability is represented by people, because nowadays everyone manages IT&C systems. Therefore, the representatives of the Romanian Intelligence Service argue that every citizen must be aware and understand the need to secure and protect their own computer systems. In order to raise cybersecurity culture among the citizens, the Romanian Intelligence Service has carried out the next measures:

A. Cybersecurity Good Practice Guidelines – taking into consideration increased exposure to cyber risks determined by the society's constant connection to cyberspace, the Romanian Intelligence Service has issued a cybersecurity guide. It is addressed to every citizen and can be found on the official website of the Service.

The guide is an important source for strengthening the cybersecurity culture, as it gathers many aspects of cybersecurity (SRI, 2018):

- rules for safe Internet browsing;
- securing the Internet connection;
- multiple anti-malware protection;
- using a firewall program;
- rules for the protection of personal data;
- securing the use of e-mail address;
- tips for choosing a solid password;
- the need to periodically update the software;
- the periodic backup;
- tips for securing access to the Wi-Fi network;
- rules for the protection of personal data during travels;
- recommendations regarding the use of social platforms.

In addition to these data, the guide includes useful tips for developing a cybersecurity culture within organizations (data about implementing an information security policy, defining responsibilities and properly integrating information security principles).

B. *Cyberint Bulletin* – since 2018, the Romanian Intelligence Service has published the *Cyberint Bulletin*, a biannual publication that aims to inform citizens about the trends in the field of cyber security. Its role is to summarize and present data about cyber-attacks, viruses, actors involved, good practices and so on.

C. Glossary of cybersecurity terms – the Romanian Intelligence Service (2019) has published a glossary of the most used terms in the field of cyber security. The glossary includes both basic and complex terms, explained through short definitions that can be understood by any citizen. Thus, it represents a good measure for increasing the knowledge field.

D. Carrying out the Awareness Program – as we mentioned earlier, the Romanian Intelligence Service has developed an extensive awareness program dedicated to relevant (national security related) entities from our country. The program aims to raise the level of awareness even in the cyber security field. Through this program, there are emphasised topics such as cyber-attacks, actors and defending methods (RIS, n. d.).

The National Cyber Security Directorate (NCSD – former CERT-RO) is also an active institution that fights for strengthening the cybersecurity culture among the Romanian society. The NCSD's publications, as well as the constantly organized events, contribute both to the education of the citizens and to the improvement of the employees with attributions in the cyber field. There have been identified the following NCSD activities:

I. Cybersecurity Weekly News and Cyber Risk Alerts – every week, on the NCSD website (www.dnsc.ro) are published the news in the cyber security field. The information is clear and summarized in order to offer to the readers the possibility to get informed quickly and correctly and, of course, to create over time a solid cybersecurity culture. In addition, NCSD has created a special section on the website, called THREATS, meant to warn the general public on the recent risks in the cyberspace.

II. Awareness campaigns – NCSD has conducted several cyber threat awareness campaigns over time. These focused on the following topics:

- malware on mobile devices;
- prevention of cybercrime among young people;
- fraud with false technical support.

III. Conferences – the annual conference "New global challenges in cybersecurity" was organised from 2011 up to 2020. It started with a small focus group of cybersecurity experts and later became the largest conference in the country, bringing together both public and private decision-makers on cybersecurity. In addition, the conference gained a global perspective, as speakers and participants from around the world were taking part. The themes focused on the new global challenges in the field of cyber security.

Another example is the international conference "Preventing and Combating Cybercrime" – organized in 2016 by the Faculty of Law of "Babeș Bolyai" University in partnership with NCSD and other organisations. The conference was attended by prestigious guests from 8 European countries, including the United States. The debates focused on the following topics: electronic harassment, cybercrime and prevention, property rights in cyberspace and so on (NCSD, 2016).

IV. Workshops for experts from public and private sector – NCSD in partnership with private institutions and companies has conducted over time multiple workshops dedicated to cybersecurity experts and to representatives of public institutions or private sector:

- workshop dedicated to a next-gen endpoint protection product (NCSD, 2017);
- workshop dedicated to SSL solution – "visibility and Data leak prevention (DLP) Network Monitor" (NCSD, 2017);
- workshop dedicated to server security and cyber threats prevention (NCSD, 2017);
- workshop dedicated to proper managing of WANNACRY attacks (NCSD, 2017);
- workshop dedicated to "Smart WIFI and Cloud Managed LAN & WLAN" (NCSD, 2017);

- workshop dedicated to protection of industrial control systems (NCSD, 2017);
- online workshop dedicated to the Connecting Europe Facility (CEF) Telecom program (NCSD, 2020).

V. Target group training sessions – NCSD organized a cyber-security course for Agerpres journalists (NCSD, 2016). The purpose of this program was to bring awareness about cyber-attacks, actors, as well as useful data about safety rules. The journalists took part into a practical demonstration in order to measure their awareness of cyber threats. For a better understanding of the cyber risks, NCSD simulated a cyber-attack.

NCSD specialists took part into the "European Judicial Cooperation in the field of combating cybercrime" project (NCSD, 2016). They carried out a training program for the judges and prosecutors (Romanians and Bulgarians) in the field of cybercrime. The program focused on cooperation in the fight against cybercrime at the European level.

All these steps taken by the Romanian Intelligence Service and NCSD are a proof that security culture represents an important pillar both at the societal and the institutional level. Besides these, the desire for transparency and the constant public communication are also relevant steps for the process of consolidated security culture, because it leads to a closer relationship between society and the state institutions and create a better understanding of the needs of population.

Limits of the security culture shaping process

The process of consolidating security culture among society is as useful as it is costly and difficult to achieve. Thus, we must consider the main limitations in the process of shaping the security culture.

First of all, an efficient communication from leaders to population requires the use of a very large accumulation of financial, material, human and time resources. Top-down communication from government to society must be a continuous and transparent process, which is utterly difficult to achieve. It is well known that this type of communication can often lead to distortions or filtered information, caused either by internal factors, related to the individual, or by external ones such as press or public relevant actors. Media can generate own interpretations or even create conspiracy theories in order to attract the citizens to a certain

part. It must be taken into consideration that disinformation can be created not only into our country borders, but also outside of them and the limits in stopping such messages are a lot. The right to free speech, as well as the inability to cover permanently such a wide range of information are worth mentioning.

Secondly, strengthening the security culture requires a very well organized and explicit framework of security values, norms and rules. It is true that all these are mentioned in the official strategic documents, but the way they have been transposed, as well as the low visibility in the public area, made these efforts unknown to the ordinary citizen.

Third, the security culture involves a constant "look" at the ruling factor. As long as the leader is not a role model that respects and promotes the security norms and values, its credibility and legitimacy in front of population may be automatically lost. Not only that the leader won't be considered a trustworthy man, but his actions will be challenged and his decisions will be outrageous. Once a system has lost its credibility, it will certainly be ineffective in the process of strengthening a common security culture. Formed beliefs will always have an impact on the attitudes and behaviours of the majority, no matter how complex are the attempts of changing people's perceptions.

Last but not least, another factor that could hinder the process of shaping security culture is represented by the level of education among society. In order to base knowledge on security values and norms, it is essential to have a consolidated image on the country's general situation: inside situation and outside situation as a member of the international community. Having in mind these circumstances which can lead to an understanding of the need for values/norms and therefore to the adoption of certain decisions and behaviours.

Conclusions

Starting from the questions posed in the introduction of this article, we can conclude the following:

1. The security culture is a set of knowledge about the security risks, vulnerabilities and threats, as well as a set of desirable attitudes and behaviours for individual and state defence.

2. The security culture is an important pillar for the national security ensuring process, because it shapes the perception of reality (the perception of risk and safety), but also the attitudes of citizens. We can also assert that security culture is important, because it determines a more efficient communication between citizens and the responsible institutions in the field of national security.

3. In terms of benefits brought to the state and its citizens, security culture provides relevant benefits for the current security context.

First of all, the average citizen has a useful framework on the proper behaviours required for his own defence. For instance, a person with a strong security culture will know that using the same password for all the online accounts can generate major security risks in case of a cyber-attack.

As for the state, the security culture ensures a better cooperation with the citizens, which can be an extremely useful tool. A person with a strong security culture will understand much faster the security risks and will be more aware of the help they should provide to the responsible authorities. For example, if a regular citizen has information about what radicalisation means, in case he/she identifies any signs, it will certain that he will communicate those signs to the responsible authorities.

4. Even though the Romanian authorities have used numerous tools for strengthening the security culture, many of these have remained unknown to citizens. As we mentioned in this article, the security culture is a strategic objective for Romania, so the efforts to this direction must be considerable. Our country has included the consolidation of security culture in the strategic documents since 2010. Up until now, several steps have been taken in order to connect the population and the Romanian institutions to the ongoing security risks.

The Romanian Intelligence Service is one of the most involved institutions in this process. Over time, the RIS representatives held several events to increase awareness among the population (conferences, debates, presentations, informative sessions, student scientific communication sessions, journals editing, master's degree, awareness program, informative materials and so on). NCSD has also been actively involved in providing the population with useful information about cybersecurity, which has led to the strengthening of

cybersecurity culture (cybersecurity news, awareness campaigns, conferences, workshops, training sessions and so on). Both institutions have, also shown interest in training certain professional categories (their own staff, public servants, magistrates, journalists, and police officers).

Even if all these measures meant strengthening the security culture were not really in the public eye, they were important steps in achieving the strategic goal. Strengthening the security culture is not a simple process that is why there should be a constant awareness of the limits of such a process: distorted communication by various internal or external factors, a bad framework of security rules and regulations, a low level of education among population and so on.

References:

1. Buluc, R., Deac, I. & Lungu, C. (2018). *Promovarea Culturii de Securitate*. Bucureşti: Asociaţia ProSCOP.

2. Calangea, C.D. (2017). „Cultura de securitate. Surse şi resurse". *Revista Intelligence*. Accessed on 30.05.2022 from www.intelligence.sri.ro/cultura-de-securitate-surse-si-resurse/

3. Chiru, I. (2016). „Percepţia socială asupra riscurilor de securitate naţională: un ingredient (lipsă) al culturii de securitate". *Revista Cultură de securitate şi diplomaţie publică*, 16, 59-72.

4. Presidential Administration. (2015). *Ghidul Strategiei Naţionale de Apărare a Ţării pentru perioada 2015-2019*. Accessed on 15.06.2022 from http://old.presidency.ro/static/Ghid%20SNApT_2015-2019_AP.pdf

5. Romanian Intelligence Service. (2003). *Serviciul Român de Informaţii a inaugurat Centrul de Informare pentru Cultura de Securitate*. Accessed on 15.06.2022 from https://sri.ro/articole/serviciul-roman-de-informatii-a-inaugurat-centrul-de-informare-pentru-cultura-de-securitate

6. Romanian Intelligence Service. (2016). *Calendar Contraterorist*. Accessed on 30.05.2022 from https://www.sri.ro/assets/files/publicatii/CALENDAR_CT_2016_RO.pdf

7. Romanian Intelligence Service. (2017). *Awareness*. Accessed from https://www.sri.ro/awareness

8. Romanian Intelligence Service. (2018). *Ghid de bune practici pentru securitatea cibernetică*. Accessed on 16.06.2022 from https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

9. Romanian Intelligence Service. (2019). *Glosar de termeni pentru domeniul securității cibernetice*. Accessed on 15.06.2022 from https://www.sri.ro/assets/files/publicatii/GLOSAR-TERMENI-CYBER-12-09-2019.pdf

10. Romanian Intelligence Service. (n.d.). *Cyberintelligence*. Accessed on 30.05.2022 from https://www.sri.ro/cyberint

11. Romanian Intelligence Service. (n.d.). *Awareness*. Accessed on 15.06.2022 from https://www.sri.ro/awareness

12. Munteanu, R. (2013). *Importanța culturii de securitate în mediul dinamic al globalizării*. Accessed on 16.06.2022 from https://adevarul.ro/international/in-lume/importanta-culturii-securitate-mediul-dinamic-alglobalizarii-1_517e5993053c7dd83f5a0cd2/index.html

13. NCSD. (2016). *Conferința Internațională "Preventing and Combating Cybercrime" (20-21 Mai 2016).* Accessed on 30.05.2022 from https://dnsc.ro/citeste/preventing-and-combating-cybercrime-2016

14. NCSD. (2016). *Curs de securitate cibernetică la AGERPRES*. Accessed on 26.06.2022 from https://dnsc.ro/citeste/curs-de-securitate-cibernetica-la-agerpres

15. NCSD. (2016). *CERT-RO sprijină pregătirea magistraților pentru combaterea criminalității informatice*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/cert-ro-sprijina-pregatirea-magistratilor

16. NCSD. (2017). *Workshop de prezentare a unei tehnologii de tip next generation endpoint protection.* Accessed on 30. 05.2022 from https://dnsc.ro/citeste/workshop-bitdefender-gravity-zone-elite

17. NCSD. (2017). *Workshop de prezentare a soluției SSL – visibility and Data leak prevention (DLP) Network Monitor.* Accessed on 16.06.2022 from https://dnsc.ro/citeste/workshop-combridge

18. NCSD. (2017). *Workshop de prezentare cu privire la securitatea serverelor și prevenirea atacurilor cibernetice*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/workshop-anssi.

19. NCSD. (2017). *Workshop pe tema bune practici în gestionarea atacurilor de tip WANNACRY*. Accessed on 30.05.2022 from https://dnsc.ro/citeste/workshop-pe-tema-bune-practici-in-gestionarea-atacurilor-de-tip-wannacry

20. NCSD. (2017). *Workshop CERT-RO – Combridge: soluții de securitate pentru Smart WIFI și Cloud Managed LAN & WLAN*. Accessed on 17.06.2022 from https://dnsc.ro/citeste/workshop-cert-ro-combridge-

21. NCSD. (2017). Workshop on *Protejarea sistemelor de control industrial*. Accessed on 30.05.2022 from https://dnsc.ro/citeste/workshop-pe-tema-protejarea-sistemelor-de-control-industrial-

22. NCSD. (2020). *CERT-RO organizează un workshop online de prezentare a programului Connecting Europe Facility (CEF) Telecom*. Accessed on 15.06.2022 from https://dnsc.ro/citeste/cert-ro-organizeaz-un-workshop-online-de-prezentare-a-programului-connecting-europe-facility-cef-telecom

23. Onișor, C. (n.d.). *Contribuții Teoretico-Metodologice privind Cultura de Securitate.* Suport de curs înregistrat în Biblioteca Centrală Universitară a ANIMV, București.

24. Piwowarski, J. (2017). "Three Pillars of Security Culture". *Security Dimensions International and National Studies,* 22, 16-27. Accessed on 16.06.2022 from https://www.researchgate.net/profile/Juliusz_Piwowarski2/publication/323243164_Three_Pillars_of_Security_Culture/links/5a883550458515b8af91b64f/Three-Pillars-of-Security-Culture.pdf?origin=publication_detail.

25. Sandman, P.M. (1988). "Risk Communication: Facing Public Outrage". *Revista Academică Management Communication Quarterly*, 2, 235-238.

26. Ustun, C. (2010). *Turkey and the European Security Defence Policy*. New York: Tauris Publisher.