COMPARATIVE ANALYSIS OF STRATEGIC CYBER SECURITY FOCUS AREAS – UNITED KINGDOM, ESTONIA, ROMANIA

Cristian CONDRUȚ*

Abstract:

Given the fact that cyber-security has a significant impact on many socio-economic sectors and it is dependent on the national context, it is important to analyse the strategic perspective at a national level. Still, by considering that cyber-security strategic topics are being more and more addressed in an international context, it is also relevant to tailor any cyber-security strategy analysis to well-recognized international documents. In this article, we aim to analyse the strategic areas of cyber-security, as they are defined by the International Telecommunication Union, in the manner that those are reflected in the national cyber-security strategies of the United Kingdom, Estonia and Romania. We will highlight some of the common and different elements found in those strategies and will focus more on the Romanian strategy, by making tailored recommendations for each strategic area, based on the International Telecommunication Union Guide.

Keywords: *cyber security, strategy, ITU, UK, Estonia, Romania*.

Introduction

The premise from which we started this research is that cyber-security affects a wide range of sectors of socio-economic development and is influenced by factors dependent on the national context. Thus, the emergence of cyber-security in various sectors of social and economic activity has acquired strategic relevance for states and has led them to adopt national cyber-security strategies. These are the most important

* Teaching assistant, PhD Student in Intelligence and National Security Doctoral School, within National Intelligence Academy "Mihai Viteazul". Email: condrut.cristian@animv.eu

planning document for strategic cyber-security activities and synthesize a particular state's vision of the role it assumes, both for the development of the field at the national level and for the way in which it is related or influences international debates and initiatives (ITU et. al., 2021, p. 34).

The strategic development of the field of cyber-security has been expanded since 2008, when complex state-sponsored cyber-attacks were deployed, with major negative consequences on other states (Shafqat & Masood, 2016, pp. 129-131). Between 2007 and 2010, a series of major cyber-attacks were carried out: the 2007 cyber-attacks in Estonia[1], the 2008 attacks in Georgia and the use of the Stuxnet *worm* in 2010 to disrupt Iran's nuclear infrastructure. These cyber-attacks influenced the adoption of strategic decisions at national and international levels. Most countries with a high level of development in the field of cyber-security adopted their first cyber-security strategy after 2008 (Shafqat & Masood, 2016, p. 131).

An important moment for the development of cyber-security strategies is the year 2018, when *the International Telecommunication Union* (ITU), the specialized organization of the UN, made the first edition of *the Guide to Developing a National Cybersecurity Strategy*. Subsequently, in 2021, the ITU proposed the second edition of the guide, the purpose of which is to provide support for national decision-makers for the development of their cyber-security strategies (ITU et. alii., 2021, p. 8). The ITU approach is of high relevance at the international level, as the ITU guide is the first public document assumed by the UN, which standardizes the good practices of designing and drafting a cyber-security strategy. Section 5 of the ITU Guide is important for our research because it indicates and details how seven strategic focus areas specific to the field of cyber-security should be captured in national cyber-security strategies.

The objective of our research is to carry out a comparative analysis of how the seven strategic focus areas are reflected in three European cyber-security strategies, in order to highlight the common

[1] The time of 22 of days (i.e. between 27 April and 18 May 2007), Infrastructure cybernetics Estonian from Sectors governmental, financial-banking, media online and from the Suppliers of Services Digital at former Target some Attacks cybernetics de tip Distributed Denial of Service.

elements and the differences in the strategic perception of the field of cyber-security in the level of these states. The scope of this research is to assess if any of these countries must undertake any significant efforts in order to better comply with the ITU's Guide recommendations. Thus, this paper could be an instrument for shaping future national cyber-security national strategic policy for any of the three studied nations.

In the next sections, we will present the research methodology, the analysis of the seven strategic focus areas by referring to the strategies and a series of conclusions.

Methodologies

The focus areas of interest in the ITU Guide are: 1) governance; 2) risk management in national cybersecurity; 3) preparedness and resilience; 4) critical infrastructures and essential services; 5) capability and capacity building and awareness raising; 6) legislation and regulation; 7) international cooperation (ITU et. alii., 2021, pp. 34-73). In our approach, these-strategic focus areas will serve as a benchmarking framework for the cyber-security strategies of the states retained for analysis – the United Kingdom, Estonia and Romania. The analysis will be descriptive and explanatory, given that, on the one hand, we will present elements from the national cyber-security strategies, and on the other hand, we will make comparisons between them each related to the strategic focus areas.

We will limit our research to 3 national cyber-security strategies because we are particularly interested in the differences between Romania's strategy and those of the United Kingdom and Estonia, the arguments for choosing each state being:

- *National Cyber Strategy 2022 (NCS UK)* – the choice is based on the fact that the UK is a global cyber power, ranked second globally and first in Europe in the *Global Cybersecurity Index 2020* (ITU Development Sector, 2021, p. 25). The state is at its fourth cyber-security strategy, with the first two being published in 2009 and 2011 (Shafqat & Masood, 2016, p. 131), the third in 2016 (HM Government, 2017) and the fourth in 2022 (HM Government, 2022a), having a rich experience in strategic management of cyber-security.

- *Cybersecurity Strategy 2019-2022* (CS EE) – as mentioned in the introductory section, the choice of Estonia is motivated by the fact that the 2007 cyber-attacks to which it was subjected represent one of the critical points of the field of cyber-security. Those cyber-attacks fundamentally changed the traction that the domain has begun to receive at the strategic level. Moreover, the Estonian Ministry of Economic Affairs and Communications (MAEC Estonia) mentions at the beginning of the document the events of 2007, classifying them as the only ones that have affected the Estonian informational society (MAEC Estonia, 2019, p. 11). For this reason, Estonia represents a European model in terms of digital transformation of public services, ranking first in this category in the *Digital Economy and Society Index*[2] (European Commission, 2022), which justifies the inclusion of the strategy in the present research.
- *Romania's cybersecurity strategy for the period 2022-2027* (SSCR RO) – the main argument is that our most important interest is in the situation of the strategic perception of cyber-security at the national level of Romania and how it can be compared to those presented in the strategies of the United Kingdom and Estonia. The secondary argument is that the present research will be part of a broader doctoral research that will be carried out in relation to the national cyber-security context and will address the topic of cyber-security education.

Analysis of strategic focus areas of cyber-security

In *Table 0* we present the strategic focus areas of cyber-security and the specific areas of each. We will comparatively analyse the strategic focus areas of cyber-security and will lay out in *Tables 1 – 7*, our assessment of the way that ITU recommendations are implemented for each specific area in the case of NCS UK, CS EE and SSCR RO.

[2] Index Measured the Level States member EU that Measured Level of Digitization, through reporting the Parameters as capital human, integrate a Technologies Digital and Services Public Digital.

Table 0[3]: Correspondence between strategic focus areas and specific areas recommended to be captured in a national cyber-security strategy. Data retrieved *from the Guide to Developing a National Cybersecurity Strategy* (ITU et. alii., 2021).

Strategic focus areas	Specific areas
1. Governance	• Ensure the highest level of support; • Establish a competent cybersecurity authority; • Ensure intra-governmental cooperation; • Ensure inter-sectorial cooperation; • Allocate dedicated budget and resources; • Develop an implementation plan.
2. Risk management in national cybersecurity	• Conduct cyber threat assessment to align policies with the ever-expanding cyber threat landscape; • Define a risk-management approach; • Identify a common methodology for managing cybersecurity risk; • Develop sectorial cybersecurity risk profiles; • Establish cybersecurity policies.
3. Preparedness and resilience	• Establish cyber-incident response capabilities; • Establish contingency plans for cybersecurity crisis management and disaster recovery; • Promote information-sharing; • Conduct cybersecurity exercises; • Establish impact and severity assessment of cybersecurity incidents.
4. Critical infrastructures and essential services	• Establish a risk-management approach to identifying and protecting critical infrastructures and essential services; • Adopt a governance model with clear responsibilities; • Define minimum cybersecurity baselines; • Utilise a wide range of market levers; • Establish public-private partnerships.
5. Capability and capacity building and awareness raising	• Strategically plan capability and capacity building and awareness raising; • Develop cybersecurity curricula; • Stimulate capacity development and workforce training;

[3] The table was also presented within the Doctoral Research Project, elaborated as a part of the doctoral research program of the author.

	• Implement a coordinated cybersecurity awareness-raising programme; • Foster cybersecurity innovation and R&D • Tailored programmes for vulnerable sectors and groups.
6. Legislation and regulation	• Establish a domestic legal framework for cybersecurity; • Establish a domestic legal framework for cybercrime and electronic evidence; • Recognise and safeguard human rights and liberties; • Create compliance mechanisms • Promote capacity-building for law enforcement; • Establish inter-organizational processes; • Support international cooperation to combat cyber threats and cybercrime.
7. International cooperation	• Recognise cybersecurity as a component of foreign policy and align domestic and international efforts; • Engage in international discussions and commit to implementation. • Promote formal and informal cooperation in cyberspace; • Promote capacity building for international cooperation.

Governance. The designation of a competent authority and the assurance of inter-sectorial cooperation are the only elements satisfied in all strategies. The unitary nature of this common dimension is explained by the existence of Directive 2016/1148 of the European Parliament and of the Council on improving the level of cyber-security of network and information systems at the EU level (i.e. the NIS Directive), the EU Member States being obliged to designate such an authority (European Union, 2016, p. 6). With regard to cross-sectorial cooperation, all strategies refer to the public-private partnership. One of the most significant differences is captured in the dimension of ensuring the highest level of support, given that SSCR RO is not assumed by a high representative of the state, as it happens in the case of NSC UK. In order to be in line with the ITU Guide, Romania should include in the future cyber-security strategy the declaration of support of a high representative of the state, present more extensively the mechanisms of

intra-governmental cooperation and allocate estimated resources for the field of cyber-security.

Table 1: Summary representation of the strategic *governance area*. Source: author

Governance	Highest level of support	Competent authority	Intra-governmental cooperation	Inter-sectorial cooperation	Budget and resource allocation	Implementation plan
NCS UK	Present	Present	Present	Present	Present	Present
CS EE	Unidentified	Present	Present	Present	Partially	Partially
SSCR RO	Unidentified	Present	Partially	Present	Partially	Present

NCS UK – The document defines how public institutions at the UK level will apply the strategy's provisions. On the one hand is being mentioned the control body over the implementation of the strategy's action plan – *The National Security Council* – and on the other hand, the public entities that have clear roles and responsibilities for implementation (HM Government, 2022a, p. 112). The most important governmental actor involved is the *National Cyber Security Centre*, defined as the technical authority for cyber threats (HM Government, 2022a, p. 128). For *intra* and *inter*-governmental cooperation, the document promotes *the whole-of-society* vision, which involves defining roles and responsibilities throughout British society and capitalizing on partnerships between relevant actors (HM Government, 2022a, p. 50). Regarding the financial resources allocated to the domain, the document provides for the sum of 2.6 billion pounds for the development of the IT and cyber-security sectors (HM Government, 2022a, p. 115). Although the UK strategy does not include a separate action plan, the implementation section presents the related strategic targets and objectives with deadlines for implementation (HM Government, 2022a, pp. 46 – 97).

CS EE – The document clearly defines the responsibilities of each Estonian government institution, as well as the links between the national cyber-security strategy and other government strategies (e.g., Estonia's Digital Agenda 2020, Lifelong Learning Strategy 2014-2020) (MAEC Estonia, 2019, pp. 29-32). The competent authority for the implementation of the provisions of the cyber-security strategy is MAEC Estonia and the strategic coordination is ensured by the Cyber Security Council of the Governmental Security Council (MAEC Estonia, 2019, p. 33). For intra-governmental cooperation, MAEC Estonia organizes these actions at the national level, including the exchange of information between responsible officials (MAEC Estonia, 2019, p. 36). Beyond the role of guiding and structuring the strategic steps associated with the field of cyber-security, the Estonian strategy was also created as a means of communication to improve public-private partnerships (MAEC Estonia, 2019, p. 8), support and promote cyber-security research and development (R&D) (MAEC Estonia, 2019, p. 52) and develop public and private sector talent. The strategy does not provide for the allocation of a fixed amount of budget but plans to adopt one based on the activities carried out in 2020 (MAEC Estonia, 2019, p. 32). It also does not provide for a specific implementation plan, with the responsibility being delegated to competent authorities (MAEC Estonia, 2019, p. 32).

SSCR RO – Although the strategy is adopted with a decision of the Romanian Government, it is not assumed by a high governmental representative. At the strategic level, the coordination of cyber security approaches in Romania is ensured by the Cyber Security Operational Council (COSC), subordinated to the Supreme Council of National Defence (Romanian Government, 2022, p. 19). The effective implementation of the actions provided for in the strategy is achieved through the involvement of several governmental institutions, the central role in this regard is ensured by the National Directorate of Cyber Security (DNSC) (Romanian Government, 2022, p. 20). Although the development of intra-governmental cooperation is one of the responsibilities of the DNSC, the COSC is the "inter-institutional cooperation mechanism" (Romanian Government, 2022, p. 19). The inter-sectorial cooperation component is addressed by establishing measures aimed at strengthening the public-private partnership

(Romanian Government, 2022, pp. 21-23). The Romanian Government encourages the allocation of budget and resources to a wide range of actors in society, without providing clear information in this regard (e.g., an estimated budget or certain fiscal policies). The strategy also contains an implementation plan, in which the strategic objectives are correlated with the measures and actions necessary to be implemented while establishing the participant and responsible entities and the deadlines for the implementation (Romanian Government, 2022, pp. 30-48).

Risk management in national cybersecurity

Establishing cyber-security policies is the only specific area that is fulfilled in all 3 strategies and we argue that it is correlated to the NIS Directive, transposed into the national legislation of all 3 states. It provides for the implementation of minimum cybersecurity baselines for operators of essential services and digital service providers. The comparative analysis of the 3 strategies shows that the risk management situation is different at the level of each state, given that the UK has fulfilled most of the recommendations in the ITU Guide: 4 out of 5; Estonia – 3 out of 5; Romania – 1 out of 5. For a future cyber-security strategy of Romania, it is necessary to present and promote approaches and methodologies of risk management, as well as to establish cyber-security risk profiles for citizens, and public and private entities.

Table 2: Summary representation of the *risk management in national cyber-security area*.
(Source: author's view)

Risk management	Cyber threat assess-ment	Risk manage-ment approach	Methodology for risk management	Risk profiles	Cyber-security policies
NCS UK	Partially	Present	Present	Present	Present
CS EE	Present	Partially	Present	Uniden-tified	Present
SSCR RO	Partially	Uniden-tified	Unidentified	Uniden-tified	Present

NCS UK – The document presents a brief strategic assessment of the cyber threat, based on the premise that cyber-space is an environment created and influenced by human behaviour (HM Government, 2022a, p. 17). Thus, one of the objectives assumed by the UK Government is to improve the understanding of cyber risks in order to carry out actions to strengthen cyber-security and resilience (HM Government, 2022a, p. 68). The strategy presents previous efforts to understand cybersecurity threats, including large-scale adoption of a conceptual framework (CAF – Cyber Assessment Framework) for assessing existing risks at the level of critical cyber infrastructures (HM Government, 2022a, p. 68). The UK has transposed into national legislation the NIS Directive, which defines technical and organizational measures for sectors providing essential services to the population (i.e., energy, transport, health and drinking water) and sectors that make digital services available (i.e., *cloud computing* services, search engines, online marketplaces). The document presents cyber-security policies, an example being the optimization of the government's vulnerability reporting programme – *Vulnerability Reporting Service*.

CS EE – Estonia's strategy begins by conducting a cyber-security national assessment, structured on three subchapters: 1) trends affecting the state of cyber-security (e.g., emerging technologies, development of cybercrime-as-a-service phenomenon, complicated geopolitical and security situation); 2) Estonia's strengths (e.g., efficiency and flexibility of a small state, Estonia's international influence) and 3) challenges to cyber-security of Estonia (e.g. lack of integrated *leadership*, insufficient understanding of the interdependencies between cyber threats; lack of specialists and training of new specialists) (MAEC Estonia, 2019, pp. 19-28). The methodological framework of risk management is provided by the *Law on Crisis Management*[4] and the *Law on Cyber-Security*[5], the need for improvement on this component is

[4] Estonian Law on Crisis Management available in English at https://www.riigiteataja.ee/en/eli/525062014011/consolide, accessed on 07.02.2023.

[5] Estonian Law on Cyber-Security is the national law transposing the EU Directive 2016/1148 on measures for a high common level of security of network and information systems in the Union (NIS Directive) and EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the

generated by the implementation in practice of the two normative acts (MAEC Estonia, 2019, p. 45). For cyber-security policies, MAEC Estonia mentions a number of programs, such as the ITC sector development one or *Targalt Internetis.*[6]

SSCR RO – It is presented a cyber-threat assessment structured according to the activities carried out by state actors, cyber-crime groups and ideologically or politically motivated hacker groups (Romanian Government, 2022, p. 7). However, the assessment is not carried out by highlighting risks to critical infrastructures as recommended in the ITU Guide, nor does it identify these infrastructures (ITU et. alii., 2021, p. 37). The Romanian Government does not present a risk management approach but includes in the action plan measures aimed at developing and implementing future methodologies for assessing the level of cyber-security (Romanian Government, 2022, pp. 30-31). The Romanian Government encourages the creation and implementation of a minimum set of cyber-security policies and disaster recovery plans (Romanian Government, 2022, p. 16).

Preparedness and resilience

Promoting information exchange and conducting cyber-security exercises are the only areas common to the 3 analysed strategies. The promotion of information exchange is a natural consequence of public-private partnership and the involvement of different types of actors in strengthening national cyber resilience. The cyber security exercises are carried out through the direct involvement of all 3 states, which have either the role of organizer or participant. The only area not addressed within SSCR RO is assessing the impact and severity of cyber-security incidents, being necessary to encourage this practice in the future cyber-security strategy, by reference to how critical goods, services, infrastructure and citizens are affected (ITU et. alii., 2021, p. 41).

---

free movement of such data (GDPR Regulation). Available in English at https://www.riigiteataja.ee/en/eli/523052018003/consolide, accessed on 07.02.2023.

[6] The project whose mission is to develop the skills of children and parents for the use of the Internet. The information is available on https://www.targaltinternetis.ee/en/about-the-project/ and was accessed on 07.02.2023.

Table 3: Summary representation of the *preparedness and resilience area*. (Source: author's view)

Preparedness and resilience	Cyber-security incident response capabilities	Contingency plans and crisis management	Promote sharing of information	Cyber-security exercises	Assessment of the impact and severity of cyber-security incidents
NCS UK	Present	Present	Present	Present	Present
CS EE	Partially	Partially	Present	Present	Partially
SSCR RO	Present	Partially	Present	Present	Unidentified

NCS UK – The UK strategy addresses the cyber resilience component in an exhaustive manner, given that one of the major strategic dimensions is of developing a digital, prosperous and resilient UK. UK's vision is segregated into three major areas: understanding the risks; acting to secure information systems and networks; developing cyber resilience to minimise the impact of cyber incidents and improve recovery capacity (HM Government , 2022a, p. 65). The UK Government defines objectives and proposes measures to strengthen cyber resilience through cyber-security incident response capabilities – both through teams and technical authorities, as well as through law enforcement organisations – by adopting contingency plans (i.e., *cyber incident response schemes*), by exchanging *intra* and *cross*-sectorial information, by conducting cyber-security exercises (i.e. *Cyber Incident Exercising service*) (HM Government, 2022a, pp. 64 – 77) and by assessing the impact and severity of cyber-security incidents (HM Government, 2022a, p. 125).

CS EE – The Estonian strategy makes only one reference to the existence of an institution that has responsibilities for responding to cyber-security incidents – *the Computer Emergency Response Team* (CERT). Although within the ITU Guide (ITU et. alii., 2021, p. 39) it is recommended that such an institution also has responsibilities in terms of vulnerability management, situational awareness or educational services, CERT-EE has responsibilities only in terms of cyber security

incident management (Information System Authority, n.d.). The strategy states that crisis management activities, integration of cyber-security with defence planning and crisis management preparedness are carried out through joint cybersecurity exercises (MAEC Estonia, 2019, p. 47). The promotion of information exchange is seen in direct connection with the mitigation of cyber-security risks (MAEC Estonia, 2019, p. 46), with the bilateral cooperation dimension being accentuated through activities aimed at carrying out joint analyses, exchanges of good practices and technical information (MAEC Estonia, 2019, p. 59). One of Estonia's main strategic directions is cyber-security exercises, given the rich history of hosting and involvement in such activities, an important example in the context being *the NATO Locked Shields* exercise, organized CCDCOE (CCDCOE, n.d.). There is no particular reference to cyber-security assessments based on the impact on essential goods, services, infrastructures and citizens, as recommended by the ITU Guide (ITU et. alii., 2021, p. 41). However, the Estonian Police and the Estonian Internal Security Service (i.e., KAPO) are responsible for carrying out integrated assessments of the state of cyber-security at the national level (MAEC Estonia, 2019, p. 35).

SSCR RO – Within the strategy is mentioned the measure of creating CERTs and Security Operational Centres (SOCs) by sectors of activity (Romanian Government, 2022, pp. 23-24), as a part of the objective of developing cyber resilience at a national level, thus being satisfied the recommendation from the ITU Guide on encouraging the development of capabilities for responding to cyber-security incidents (ITU et. alii., 2021, p. 39). With regards to the adoption of contingency plans, this practice is encouraged in the strategy, without any reference to the crisis management component (Romanian Government, 2022, p. 16). Furthermore, the action plan requires the exchange of information between certain public institutions and private entities on a permanent basis (Romanian Government, 2022, p. 32). Cyber-security exercises are presented as a good opportunity to test resilience and response capabilities and cooperation mechanisms (Romanian Government, 2022, p. 24).

Critical infrastructures and essential services

None of the specific areas of this strategic focus area is fulfilled in all three strategies, however there are three areas for which NCS UK and

CS EE meet the recommendations of the ITU. Romania's approach on this dimension is too general, given that the SSCR RO does not refer to any risk management approach or any governance model and it is not detailed how the state will capitalize on public-private partnerships. Although there are references to all these areas by correlation with other strategic focus areas (e.g., governance, risk management), none of them is customized in the context of operators of essential services or digital service providers. It is necessary for Romania's future cyber-security strategy to pay more attention to this dimension, considering, on the one hand, the regional security context – the use of cyber tools in the Russian-Ukrainian War – and on the other hand the adoption at EU level of the NIS 2 Directive[7] at the end of 2022.

Table 4: Summary representation of the *critical infrastructures and key services area*. (Source: author's view)

Critical infra-structures and essential services	Risk management approach	Governance model	Minimum cyber-security baselines	Wide range of market levers	Public-private partnerships
NCS UK	Present	Present	Present	Present	Present
CS EE	Present	Unidentified	Present	Present	Partially
SSCR RO	Unidentified	Unidentified	Partially	Partially	Unidentified

NCS UK – Government's UK institutions must lead by example other national entities in understanding cyber-security risks. The UK government aims to adopt CAF on a large scale, to gain a better understanding of how critical infrastructures depend on supply *chains*, to improve partnerships with managers and operators of critical infrastructure, and to obtain a better understanding of the risks posed by

[7] It is the update of the NIS Directive and directly introduces the rule on the threshold by size, without leaving this to the discretion of the Member States. Information available at https://www.consilium.europa.eu/ro/press/press-releases/2022/11/28/ eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/ on 23.02.2023.

accelerated digitalisation (HM Government, 2022a, p. 68). The UK's governance model appoints the authorities responsible for coordinating the implementation of cyber-security measures for critical infrastructures at national level (HM Government, 2022a, p. 124). The UK's Government encourages the fulfilment of the minimum cybersecurity baselines set by the competent authorities for operators of essential services defined in the national legislation transposing the NIS Directive (HM Government, 2022a, p. 71). The public-private partnership is reflected in the UK's strategy by adopting special laws to create facilities for organisations that pose a high cyber-security risk. In addition, cooperation and dialogue with influential economic actors (e.g., investors, financial institutions or auditors) will encourage the large-scale adoption of cybersecurity best practices for the UK's economy (HM Government, 2022a, p. 72).

CS EE – The risk management approach in Estonia is presented as being in relation to the implementation in practice of the Cybersecurity Law and the Crisis Management Law. Since the Cybersecurity Act transposes the NIS Directive into the national regulatory framework and because it also refers to operators of essential services, it can be concluded that Estonia presents in the strategy a risk management approach for critical infrastructures and essential services. Estonia's minimum cybersecurity baselines are based on one of Germany's policies in the field: *the BSI IT-Grundschutz* (MAEC Estonia, 2019, p. 42), which is the minimum standard of cyber-security measures for computer systems and networks (Information System Authority, 2022). However, ISKE (i.e., the Estonian adaptation of the German standard) has raised many issues for public authorities in Estonia, strategy proposing systematization of criteria and the centralized provision of cyber-security services for implementation at the level of government institutions, private companies, NGOs and citizens (MAEC Estonia, 2019, p. 42). Given the wide range of entities covered by minimum cybersecurity standards, the strategy also refers to the policy-making component to encourage organisations and individuals to strengthen their cyber-security. While no direct reference is made to the development of the public-private partnership to ensure the cyber-security of critical infrastructures and essential services, the very establishment of minimum cybersecurity

standards across Estonian society can facilitate development on this component.

SSCR RO – Romania's strategy encourages the practice of adopting a minimum set of cyber security baselines at the level of each entity that operates information systems or networks (Romanian Government, 2022, p. 16). However, no reference is made to the adoption of such measures for operators of essential services or digital service providers. The Romanian Government encourages the creation of a unified regulatory framework in the field of cyber-security measures and policies and the provision of training formats for cyber-security experts (Romanian Government, 2022, p. 16), without customizing on the context of operators of essential services and digital service providers.

Capability and capacity building and awareness raising

The only two areas that comply with the recommendations of the ITU Guide in all 3 strategies are strategic planning and the implementation of a coordinated programme to raise awareness. Roles and responsibilities for the implementation of measures aimed at developing capabilities, capacities and awareness are clearly defined in all three strategies. Coordinated *awareness* programmes at the population level are supported by concrete elements or projects in all three strategies. However, the creation of curricular frameworks, the development of training formats for the workforce or the development of research, innovation and development are areas that require increased attention for future cyber-security strategies, especially from Romanian side. We found that SSCR RO generally encourages the development of measures for these areas, but without promoting existing or planned projects to be carried out, compared to NCS UK and CS EE, which present concrete initiatives.

Table 5: Summary representation of the *capability and capacity building and awareness raising area*. (Source: author's view)

Capability and capacity building and awareness raising	Strategic planning	Curricular frameworks	Workforce training	Coordinated awareness programme	Research, innovation and development in cyber-security	Tailored programmes for vulnerable groups and sectors
NCS UK	Present	Partially	Present	Present	Present	Unidentified
CS EE	Present	Present	Partially	Present	Present	Partially
SSCR RO	Present	Partially	Partially	Present	Partially	Unidentified

NCS UK – UK runs a number of projects, predominantly managed by *the National Cyber Security Centre* (NCSC) or the *National Crime Agency* (NCA), such as *NCA Cyber Choices* and *NCSC Cyber Aware*, although there is no authority specifically designated in the strategy to implement the capability, capacity and awareness development programmes. Cyber-security education is predominantly treated in relation to the specialization and diversification of the workforce in the field, the UK Government's approach being *a whole-of-society* one, which implies the involvement of all actors from the British society in the training of future specialists in cyber-security and in which public institutions, private companies and the academic environment subsequently benefit from their training. In addition, the UK Government is paying close attention to academia, stating that at national level are 19 centres of academic excellence in cyber-security, whose curricula will be aligned with cyber-security industry standards by 2030 (HM Government, 2022a, p. 52). In the UK there are 19 centres of academic excellence and 4 research institutes on cyber-security issues (HM Government, 2022a, p. 21). The UK Government's vision of RDI is captured within the strategic objective of improving the ability to anticipate, evaluate and act on advances in science and technology, vital to maintaining the UK's *status quo* of cyber power (HM Government, 2022a, p. 81). The UK Government aims to better analyse technological and scientific advances in cyber-security to better understand the

strategic implications they entail (HM Government, 2022a, p. 81). In order to improve and sustain its own and allied technological advantage, the UK Government encourages academia to better cooperate with the private cyber-security industry to promote and operationalise research results (HM Government, 2022a, p. 83). Another objective of the UK Government is to encourage communities made up of actors from multiple sectors of society to develop technological standards in priority areas that safeguards democracy principles and improve the level of cyber-security (HM Government, 2022a, p. 88).

CS EE – Strategic planning of capability development and awareness raising is well articulated in the Estonian strategy. *State Information System Authority* (RIA) has responsibilities to develop technological resilience, to raise awareness of general population and to coordinate research and development in cyber-security and the Ministry of Education and Research deals with the harmonisation of the objectives of this strategy with the Lifelong Learning Strategy 2014-2020. Relating to curricular frameworks, Estonia deals exhaustively with the subject in relation with different educational stages. However, at least three aspects are assumed by MACE Estonia as problematic in terms of curricular frameworks in the field of cyber-security: 1) lack of conceptual links between private sector needs and the cyber-security competence framework (MAEC Estonia, 2019, p. 70); 2) lack of unitary practices in the continuous professional training of specialists in the public sector (MAEC Estonia, 2019, p. 89); 3) limited existence of tools to measure cyber-security knowledge and skills (MAEC Estonia, 2019, pp. 67-68). For awareness programmes in the field of cyber-security, MACE Estonia aims to carry out projects adapted for different social groups: the general public, students and teachers, government institutions and local public institutions and high-level officials of the Estonian state (MAEC Estonia, 2019, pp. 66-69). One of the major strategic objectives is the industry development and cyber-security research. The achievement of this objective depends on capitalising on cooperation between organisations in the public, private and academic sectors, on the realisation of a national R&D plan in the field of cyber-security, on the provision of state support for innovation and on ensuring a beneficial environment for the development of *start-ups* (MAEC Estonia, 2019, pp. 52-54). The only

vulnerable group to cyberattacks, which often lacks the capacity to ensure an adequate level of cyber-security are the small companies, RIA Estonia Providing support in the event of the materialization of cyber-security incidents (MAEC Estonia, 2019, p. 66).

SSCR RO – Strategic planning is ensured by adopting the action plan of the cyber-security strategy. Although the Romanian Government encourages the development of cyber-security educational programmes in all educational stage – "since the primary school" (Romanian Government, 2022, pp. 21-22) – it does not propose the adoption of curricular frameworks for cyber-security. In terms of training formats for the labour market, the strategy encourages the strengthening of the level of technical knowledge and the development of behaviours for mitigating cyber-security risks (Romanian Government, 2022, p. 22). However, the recommendations made in the ITU Guide are being followed to a small extent, as the definition of career trajectories or schemes for the training of cyber-security specialists are not encouraged (ITU et. alii., 2021, p. 45). With regards to cyber threat awareness, multiple activities are state in the action plan (Romanian Government, 2022, pp. 38-39). The strategy provides for a series of measures for the development of the field of cyber-security research and innovation, the Romanian Government supporting the cooperation with the private and academic environment, the involvement of the research community in European networks in the field or the additional allocation of governmental financial resources. However, the strategy does not encourage access to research grants or the development of research programmes and the dissemination of research results, as recommended in the ITU Guide (ITU et. alii., 2021, p. 46).

Legislation and regulation

The creation of compliance mechanisms is the only area for which the recommendations of the ITU Guide are followed in all 3 strategies, given that the NIS Directive has been transposed into the national legislation of all 3 states. However, all 3 states have gaps in the establishment of a national legal framework for cyber-security, since none of the 3 strategies refer to a law in force regulating institutional roles and responsibilities in the field. The field of cybercrime is not

presented in the SSCR RO in terms of legislative, cooperation or capability building, unlike NCS UK or CS EE, which encourages the amendment of criminal legislation, defines institutional responsibilities and presents concrete cases of international cooperation to combat cybercrime. With regards to Romania's strategy, cybercrime field is not being sufficiently addressed, being necessary to approach and detail this dimension in the future cyber-security strategy of Romania.

Table 6: Summary representation of the *legislation and regulation area*. (Source: author's view)

Legislation and regulation	Domestic legal framework	Domestic legal framework in the field of cybercrime and digital evidence	Recognition and protection of human rights and liberties	Creation of compliance mechanisms	Capacity building for law enforcement	Establishment of inter-organizational processes	Supporting international cooperation to fight cyber threats and cybercrime
NCS UK	Partially	Partially	Present	Present	Present	Present	Present
CS EE	Partially	Partially	Partially	Present	Present	Present	Partially
SSCR RO	Partially	Unidentified	Partially	Present	Unidentified	Partially	Unidentified

NCS UK – The legal framework in the field of cyber-security is composed of the national law transposing the NIS Directive and the one transposing the European GDPR Regulation (HM Government , 2022a, p. 65). With regards to the legal framework in the field of cybercrime and electronic evidence, it is stipulated that the *Counter State Threats Bill* – which is part of the UK's national security package (HM Government, 2022b) – must be amended to cover national security threats from cyberspace. In order to optimise the roles and responsibilities of law enforcement institutions for cyber-security offences, the UK's Government is promoting the need to amend the *Proceeds of Crime Act 2002* (HM Government, 2022a, p. 104). The UK's government recognises the importance of fundamental human rights and freedoms in the context of countering digital authoritarian movements and abusive state

control (HM Government, 2022a, p. 34). Enforcement of compliance mechanisms is ensured by the competent authorities for the coordination and application of the legislation transposing the NIS Directive (HM Government, 2022a, p. 122). The promotion of the development of law enforcement capabilities is captured in one of the most consistent chapters of the strategy, which is about countering threats. New investments are foreseen here to provide law enforcement agencies with the capabilities they need to conduct investigations and maintain their technological advancement compared to adversaries (HM Government, 2022a, p. 100). Given that the UK's strategy is created by adopting the *whole-of-society* vision, the component of inter-organisational processes is approached in relation to this principle. Beyond the wide range of already existing public enforcement institutions, such as the NCSC, NCA, Government Communications Headquarters (GCHQ) or Ministry of Defence (MoD), in 2020 the National Cyber Force (NCF) was created whose responsibility is to operate *in* and *through* cyberspace to counter, disrupt, degrade and challenge entities with hostile intentions against the UK. The NCF conducts operations to influence individuals or groups, to disrupt online communication systems or to degrade physical systems, all of which are defined in the strategy as *cyber offensive* (HM Government, 2022a, pp. 41-42). The importance of the international cooperation dimension in countering cyber threats and cybercrime is recognised and encouraged in the UK strategy and integrated into British government's endeavours (HM Government, 2022a, p. 104).

CS EE – The main elements of cyber-security regulatory framework in Estonia are the Cybersecurity Law and the Crisis Management Law. The legislative framework on cybercrime is represented by the Estonian Criminal Code, which defines the offences such as obtaining illegal access to information systems (Estonian Parliament, 2015). One of the four principles on which the Estonian strategy is based refers to the equal importance of protecting and promoting fundamental rights and freedoms, both in physical and cyberspace. However, during the course of the strategy, the subject is not elaborated. The subject of compliance mechanisms is extensively addressed within the strategic objective aimed at affirming Estonia as a

sustainable digital state, the standard of minimum cybersecurity baselines, ISKE (a topic also addressed in the critical *infrastructures and essential services* section) being adopted (MAEC Estonia, 2019, p. 42). The development of the capabilities and capacities of the law enforcement institutions is carried out through the Internal Security Development Plan 2021 – 2030, which includes activities such as promoting the capabilities of detection and investigation of cybercrime activities, promoting cooperation at national and international level or analysing and reducing the risks to *the e-Residency*[8] systems and digital identity[9] (MAEC Estonia, 2019, p. 30). The organizational processes related to the fight against cybercrime are detailed in the strategy, the main institutions responsible for this component being the Ministry of Justice, the Office of the Prosecutor General's, the Data Protection Inspectorate, the Estonian Forensic Science Institute or the Centre of Registers and Information Systems (MAEC Estonia, 2019, p. 34). With regards to international cooperation in the field of cybercrime, certain elements (e.g., cooperation formats, international treaties in the field) are not particularly articulated, but it is proposed to create a framework for cooperation and information exchange through which capabilities will be strengthened.

SSCR RO – Given the fact that SSCR RO was adopted in December 2021, it is not mentioned the fact that Romania has recently adopted a national law concerning cyber-security and cyber-defence – Law 58/2023[10]. This law regulates responsibilities regarding information networks and systems that are used, organised, administered or possessed by public and private entities, including citizens. It also regulates the strategic and operational cyber-security framework in

[8] Digital system through which any person can obtain a digital business identity registered in the records of the Estonian state, online and in about 15 minutes. Information available at https://www.e-resident.gov.ee/, on 10.02.2023.

[9] Digital system through which any Estonian citizen can obtain a digital personal identity that he can use for digital signing, online voting or access to personal medical and tax data. Information available at https://e-estonia.com/solutions/e-identity/id-card/, on 10.02.2023.

[10] Law concerning cyber-security and cyber-defence was adopted on March 14, 2023 and is available in Romanian language at https://monitoruloficial.ro/Monitorul-Oficial--PI--214--2023.html. It was accessed on March 16, 2023.

Romania, regarding cyber-incident response, cyber resilience, national and international cooperation, research and development, cyber-education, crisis management, but also enforces penalties for entities that do not comply with the law (Romanian Parliament, 2023). Another important legislative element is 2018 the Law 362/2018 on ensuring a high common level of security of network and information systems, which transposes the provisions of the NIS Directive, was adopted (DNSC, n.d.). Within the Romanian strategy there are no references to elements of normative framework in the field of cybercrime, although Romania is a signatory state of the Budapest Convention (Council of Europe, n.d.) and that the Law 286/2009 (i.e., the Criminal Code) provides for a series of "crimes against the safety and integrity of information systems" (Romanian Parliament, 2009). Although the adoption of a cyber-security regulatory framework that falls within the limits of the international legislation on human rights and fundamental freedoms is encouraged, the existing recommendation in the ITU Guide on accentuating contextual differences between cyber-security (i.e., understood in a technical way) and cybercrime (i.e., understood as a process of applying criminal legislation) (ITU et. alii., 2021, p. 48) is not respected. The creation of compliance mechanisms is encouraged for all network operators and information systems, and in particular for entities designated under the legislation transposing the NIS Directive (Romanian Government, 2022, p. 16). With regards to the inter-organisational processes, multiple actors are designated in the implementation plan of the strategy to participate in the implementation of the measures assumed in the document. However, some elements recommended in the ITU Guide, such as judicial cooperation and compliance with national and international legislation in the field of cybercrime (ITU et. alii., 2021, pp. 49-50), are not defined or addressed in the Romanian strategy.

International cooperation

International cooperation is a well-represented strategic area in all of the 3 strategies. Each of the three states recognizes that cyber-security is an integral part of foreign policy and promotes the need to engage in international discussions. In Romania’s case, it is necessary to

present punctual initiatives and projects to promote formal and informal cooperation, but also to develop the capacity for international cooperation.

Table 7: Summary representation of the *international cooperation* strategic *area*. (Source: author's view)

International cooperation	Recognizing cyber-security as a component of foreign policy	Engagement in international discussions and commitment to implementation	Promoting formal and informal cooperation in cyberspace	Promoting capacity building for international cooperation
NCS UK	Present	Present	Present	Present
CS EE	Present	Present	Present	Present
SSCR RO	Present	Present	Partially	Partially

NCS UK – Cyber-security is perceived by the UK's Government as a central component of the foreign policy conducted by the state, given that each of the proposed strategic objectives requires international involvement (HM Government, 2022a, p. 36). Involvement in international discussions on cyber-security issues is based on the UK's cybersecurity status, one of the strategic objectives being to influence global governance to promote a safe, open and free cyber-space (HM Government, 2022a, p. 94). The UK is involved in cooperation formats (e.g., *Five Eyes*, G7) or is an important part of organisations such as the UN, the EU or the World Bank (HM Government, 2022a, p. 93). The UK's involvement in international cooperation activities is illustrated both by activities aimed at strengthening cyber capabilities for states in Eastern Europe, Africa and the Indo-Pacific (HM Government, 2022a, p. 92), as well as by the use of all available cooperation channels – foreign policy or law enforcement organisations (HM Government, 2022a, p. 93). The UK Government promotes the development of the capacity for international cooperation by recognising the importance of diplomatic measures on cyber-security and by harnessing the external influence of the state (HM Government, 2022a, p. 91).

CS EE - One of the most articulated components of the Estonian strategy is the recognition of cyber-security as an integrated part of the state's foreign policy. There are many initiatives carried out by the Estonian authorities, such as the inclusion of the cyber-security field in the Foreign Policy Development Plan 2030 and in the Development Plan for Cooperation and Humanitarian Aid 2016-2020 (MAEC Estonia, 2019, p. 31); hosting the NATO CCDCOE in Tallinn (MAEC Estonia, 2019, p. 72); Estonia's participation in regional and international cooperation formats, within organizations such as NATO, the EU or the OSCE (MAEC Estonia, 2019, pp. 58-61). Estonia encourages formal and informal cooperation in the field of cyber-security as a measure to achieve all the objectives proposed in the strategy, addressing dimensions such as public-private partnership, cooperation by law enforcement institutions or cooperation with strategic partners from other states or international organisations. Given that the dimension of international cooperation is found in all the strategic objectives assumed by the Estonian State, measures to develop the capacity for international cooperation, such as the inclusion of cyber-security experts in organisations with responsibilities outside Estonian territory, are also promoted in the strategy (MAEC Estonia, 2019, p. 59).

SSCR RO - Although it is not mentioned in the Romanian strategy that cyber-security must represent a part of the state's foreign policy, as recommended in the ITU Guide (ITU et. alii., 2021, p. 51), the Romanian Government assumes that the country will become a relevant actor in the international cooperation architecture (Romanian Government, 2022, p. 24). According to the Romanian Government, this objective can be achieved by strengthening Romania's role at global and regional level, in bilateral relations and by strengthening *cyber-diplomacy* (Romanian Government, 2022, pp. 23-27). Thus, it is supported the continuation of Romania's participation in international formats that stimulate cyber-security debates (e.g., within organizations such as the UN, OSCE, NATO or EU). However, the component of formal and informal cooperation is presented too generally, given that the exchange of information between the public and private sectors is encouraged in order to mitigate cyber risks (ITU et. alii., 2021, p. 32), but that no mechanism or format of operational cooperation at the national level is presented. The only

element aimed at promoting the capacity for international cooperation refers exclusively to Romania's foreign policy in the field of cyber-security but excludes other areas of interest for such formats, such as arms control, trade or data protection, aspects desirable to be addressed, as specified in the ITU Guide (ITU et. alii., 2021, p. 53).

Results and Discussions

The numerical situation of the total, partial or non-fulfilment of the ITU recommendations can be found in Table 8.

Table 8: Summary representation of the fulfilment of the ITU recommendations, depending on the number of specific areas. (Source: author's view)

	Totally fulfilled recommendations (i.e., *present*)	Partially fulfilled recommendations (i.e., *partially*)	Not fulfilled recommendations (i.e., *unidentified*)
NCS UK	33	4	1
CS EE	22	13	3
SSCR RO	12	14	12

By exclusively referencing the ITU Guide and the 3 cyber-security strategies that were analysed, it can be concluded that NCS UK is the best correlated strategic document with the recommendations formulated by the ITU, and the SSCR RO the least. One of the possible explanations for this result lies in the number of cyber-security strategies adopted by each state until the present. The UK has so far issued 4 cyber-security strategies, Estonia 3 such documents (MAEC Estonia, 2019, p. 7), and Romania 2 (Romanian Government, 2022, p. 5).

Although the strategic vision assumed and adopted by the decision-makers at the level of a state is dependent to a large extent on the national context, the field of cyber-security is, on the one hand, multidisciplinary, and on the other hand in close connection with the events and debates carried out at regional and international level. For all 3 states, there are still a number of elements that are not satisfied or are partially satisfied in relation to the ITU Guide. However, our research has

highlighted that the United Kingdom and Estonia generally aim for strategic objectives for which there are already ongoing projects at the national level, while Romania encourages the development of such projects, but without presenting the existence of those already in progress or those planned. It is necessary for the future edition of Romania's cyber-security strategy to concretely capture existing projects and initiatives at the national level, meant to contribute to the achievement of the strategic objectives assumed.

Conclusion

The aim of this research was to highlight the common elements and the differences in the strategic perception of the field of cyber-security in the level of the United Kingdom, Estonia and Romania. Given that we have undertaken a descriptive and explanatory comparative analysis, by using ITU recommendations as an analytical grid, we have fulfilled the research objective. Although we have chosen the United Kingdom, Estonia and Romania for comparison, any other combination of three would have brought some relevant aspects for a national cyber-security comparative analysis. For future research, we believe that it could be useful to assess by comparison cyber-security strategies or polices form different international organisations or from much culturally diverse nations than the ones we chose.

References:

1. CCDCOE. (n. d.). Locked Shields. Retrieved February 8, 2022, from https://ccdcoe.org/exercises/locked-shields/

2. Council of Europe. (n. d.). *The Budapest Convention* (ETS No. 185) and its Protocols. Retrieved February 13, 2023, from https://www.coe.int/en/web/cybercrime/the-budapest-convention

3. DNSC. (n. d.). *Informatii generale despre NIS* (Legea 362/2018). Retrieved February 13, 2023, from https://dnsc.ro/pagini/informatii-generale-despre-nis

4. Estonian Parliament. (2015, January 22). *Penal Code*. Retrieved February 10, 2023, from https://www.riigiteataja.ee/en/eli/522012015002/consolide

5. European Commission. (2022, September 16). *The Digital Economy and Society Index – Countries' performance in digitisation.* Retrieved February 21, 2023, from European Commission: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

6. European Union. (2016, July 6). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. Retrieved February 6, 2023, from EUR-Lex: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016L1148&from=RO

7. HM Government. (2022a). *National Cyber Strategy 2022*. Retrieved March 16, 2023, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

8. HM Government. (2017, September 11). *National Cyber Security Strategy 2016 to 2021*. Retrieved February 21, 2023, from GOV.UK: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

9. HM Government. (2022b, July 12). *Legislation to counter state threats*. Retrieved February 2, 2023, from https://www.gov.uk/government/consultations/legislation-to-counter-state-threats

10. Information System Authority. (2022, November 17). *IT baseline security system ISKE*. Retrieved February 8, 2023, from https://www.ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske

11. Information System Authority. (n.d.). *Monitoring cyberspace and impeding incidents*. Retrieved February 8, 2023, from https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

12. ITU Development Sector. (2021). *Global Cybersecurity Index 2020*. Retrieved December 7, 2022, from ITUPublications: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

13. ITU et. al. (2021). *Guide to Developing a National Cybersecurity Strategy.* Retrieved March 16, 2023, from United Nations: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

14. MAEC Estonia. (2019). *Cybersecurity Strategy. Republic of Estonia*. Retrieved March 16, 2023, from https://www.mkm.ee/media/703/download

15. Romanian Government. (2022, January 3). *E-monitor.* Retrieved February 12, 2023, from Monitorul Oficial: https://monitoruloficial.ro/Monitorul-Oficial--PI--2Bis--2022.html

16. Romanian Parliament. (2009, July 24). *Codul penal din 17 iulie 2009*. Retrieved February 13, 2023, from Portal Legislativ: https://legislatie.just.ro/Public/DetaliiDocumentAfis/223635

17. Romanian Parliament. (2023, March 15). *Monitorul Oficial*. Retrieved March 15, 2023, from https://monitoruloficial.ro/Monitorul-Oficial--PI--214--2023.html

18. Shafqat, N., & Masood, A. (2016). *Comparative Analysis of Various National Cyber Security Strategies*. International Journal of Computer Science and Information Security, 129-136.