Radu Antonio Serrano 2025 "National Cybersecurity: Global and Regional Descriptive Snapshots through the Analysis of 161 Countries"
Halduskultuur. The Estonian Journal of Administrative Culture and Digital Governance 23(1-2), 83-105

National Cybersecurity: Global and Regional Descriptive Snapshots through the Analysis of 161 Countries

RADU ANTONIO SERRANO IOVA, RAGNAR NURKSE DEPARTMENT OF INNOVATION AND GOVERNANCE, TALLINN UNIVERSITY OF TECHNOLOGY

Abstract

National cybersecurity includes so many topics and considerations that a global overview of trends is a quite complex endeavor. Previous studies either focus on individual countries or multiple ones while considering only a specific subtopic or point of interest of national cyber security. The purpose of this article is to present the regional cybersecurity trends of 161 nations, as of late January 2023, through the use of the National Cyber Security Index (NCSI). With the help of the NCSI, its methodology and publicly available database, we will provide both global and regional snapshots of what countries have been focusing on and doing in reference to their national cybersecurity. This will allow the discovery of similarities, best practices, and more importantly, underdeveloped topics that should be improved upon to guarantee a more robust approach to national cybersecurity. Globally, the national approaches seem to be reactionary, with very little focus on proactive measures, but regionally some differences start to appear. Future research will be able to build upon this research by either individual case studies or comparative studies among multiple countries.

Keywords: Cybersecurity, global, cybercrime, cyberoperations

Introduction

Information and communication technologies (ICT) and digital technologies have become so ubiquitous around all of us, that cyber security is no longer a topic that is undertaken by only handful of highly specialized individuals. Because of this, whole countries nowadays must endeavor to create complex strategies and policies to protect their cyber security, and mitigate, and recover from, attacks and threats. As Shackelford and Kastelic (2014, 1) have posited in their opening statement "*nations bear increasing responsibility for enhancing cybersecurity.*"

The definition of the term cybersecurity or cyber security it is still under discussion in multiple academic and non-academic circles (Bay 2016; Craigen et al. 2014; ENISA 2015). The debate turns even more complex when you consider the different languages throughout the world that are discussing this universal topic (Carlini 2016; Guranda 2021; K. Newmeyer et al. 2015; Pohlmann 2019), the multiple national interpretations that are given to the term(s) and the

difference in approaches in academia and the non-academic worlds. For this article, we will refer to the definition of the European Union Agency for Cybersecurity (ENISA):

> *"Cybersecurity comprises all activities necessary to protect cyberspace1, its users, and impacted persons from cyber threats… Cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security)." (ENISA 2017, 6)*

National cybersecurity refers to all these efforts at the state level, by the government in charge and relevant stakeholders. Although national cybersecurity has been the focus of academic research before (K. P. Newmeyer 2015; Carlini 2016), this article attempts to answer the following questions:

- How is national cybersecurity undertaken throughout the world?
- What similarities and differences exist in national cybersecurity efforts, at the regional and global level?
- From which countries can future best practices be adopted for specific national cybersecurity efforts?

A comparative analysis of 161 national cybersecurity efforts, grouped into regions, allows us to answer these questions. This comparison is constructed according to the national cyber security framework, which forms the basis of the similarly named National Cyber Security Index (NCSI). Given the almost global nature of the sample size, the M49 Standard of the Statistics Division of the United Nations Secretariat has been used.

The purpose of this article is both theoretical and practical. Theoretical, providing a holistic snapshot of national cybersecurity focus globally, and fostering further research through bilateral/multilateral regional comparative studies or individual case studies. Practical, so that countries can use this information as a benchmark and see what they are missing or can improve upon, and/or further endeavor to publicize their efforts so that other nations may benefit from the knowledge and best practices.

National Cybersecurity Research: From the Sporadic to the Specific

Previous research has been focused either on individual case studies or multiple country comparative studies, with the focus on a single theme (e.g., cybercrime, critical infrastructure protection, governance, etc.) or a single sector (e.g., health, defense, industry, etc.). For example, Berthelet (2020) analyses the topic of the fight against cybercrime within the context of the European Union as a whole, exploring how the different member states act together

1 Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information. (ENISA 2017, 6)

to fight this transnational phenomenon (Berthelet 2020). Bada et al. (2019) analyze national cybersecurity awareness in six African countries. Their paper presents recommendations for the implementation of national awareness campaigns and how to identify and prioritize relevant activities (Bada et al. 2019). Le Barreau and Longeon (2016), on the other hand, present a study case of Saudi Arabia. Their analysis centers on "*the integration of cybersecurity into national security*" and additional implications between the stakeholders (Le Barreau and Longeon 2016, 155). Loiseau et al. (2013) study Canada and how its national cybersecurity has evolved throughout the years. Dewar et al. (2018) and Shackelford and Kastelic (2014) focus on national cyber security strategies and policies. The former also delve into cyber defense of France, Finland, Germany, and the United Kingdom. However, the latter presents the analysis of multiple countries. On the other hand, there are also compilations of individual studies, such as Stevens (2018) and Romaniuk and Manjikian (2021). However, the former is a special edition of a journal, whose individual articles deal with specific cybersecurity themes, while the latter, a book, presents chapters and is "*the most comprehensive and up-to-date comparative overview of the cyber-security strategies and doctrines of the major states and actors in Europe, North America, South America, Africa, and Asia*" (page i). In this book, once again we see that each chapter is an individual study, and focus is on the "major states and actors" (bypassing countries that might be worthy of study), without any regional or global analysis that might uncover similarities or differences between the chosen countries.

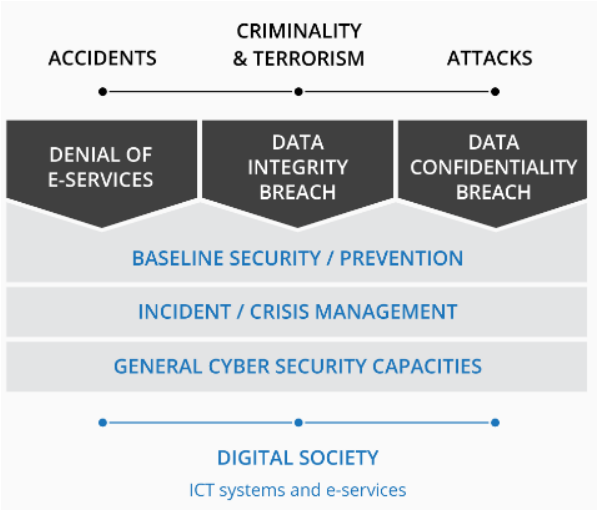
A singular, almost similar, global endeavor is the Global Cybersecurity Index (GCI). The GCI is compiled by ITU-D, the Telecommunication Development Sector of the International Telecommunication Union. In short, an Expert Group sends out a GCI Questionnaire to focal points in the Member States, who then respond and return such answers to the Expert Group for analysis (ITU-D n.d.). While the tools and methodology are publicly available, the responses and weighting process are not. Therefore, we posit that the GCI is not academic in nature, due to its replicability factor being affected by its partially obscure methodological process.

This article focuses on expanding the lack of academic studies on the overarching cybersecurity field with an almost global analysis, information extracted in late January 2023, and inductive regional similarities and differences.

Framework and Methodology

The NCSI (http://www.ncsi.ega.ee/) was created by the e-Governance Academy (eGA) as a live global index, and as a cybersecurity reference, assessment, and capacity-building tool (eGA 2022, 12). It does so through 46 indicators (presented in Annex 1). These indicators were developed through the national cyber security framework (eGA n.d.-b) which in turn alludes to the CIA (Confidentiality, Integrity, and Availability) triad. The CIA triad refers to "*the fundamental elements of security controls in information systems*" (Samonas and Coss 2014, 22), which in turn has been "*a popular definition of cybersecurity*" (Ham 2021, 18:1). However, this has not been the case of the aforementioned framework, and as Ham (2021, 18:1) posits, more focus has been "*on the activity and associated risks for cybersecurity.*" The national cyber security framework (see Figure 1) assessed the fundamental threats to the CIA triad of the national ICT systems and services. "*In order to manage these cyber threats, a country must have appropriate capacities for baseline cyber security, incident management, and general cyber security development.*" (eGA n.d.-b)

Figure 1: National Cyber Security Framework (eGA n.d.-b).

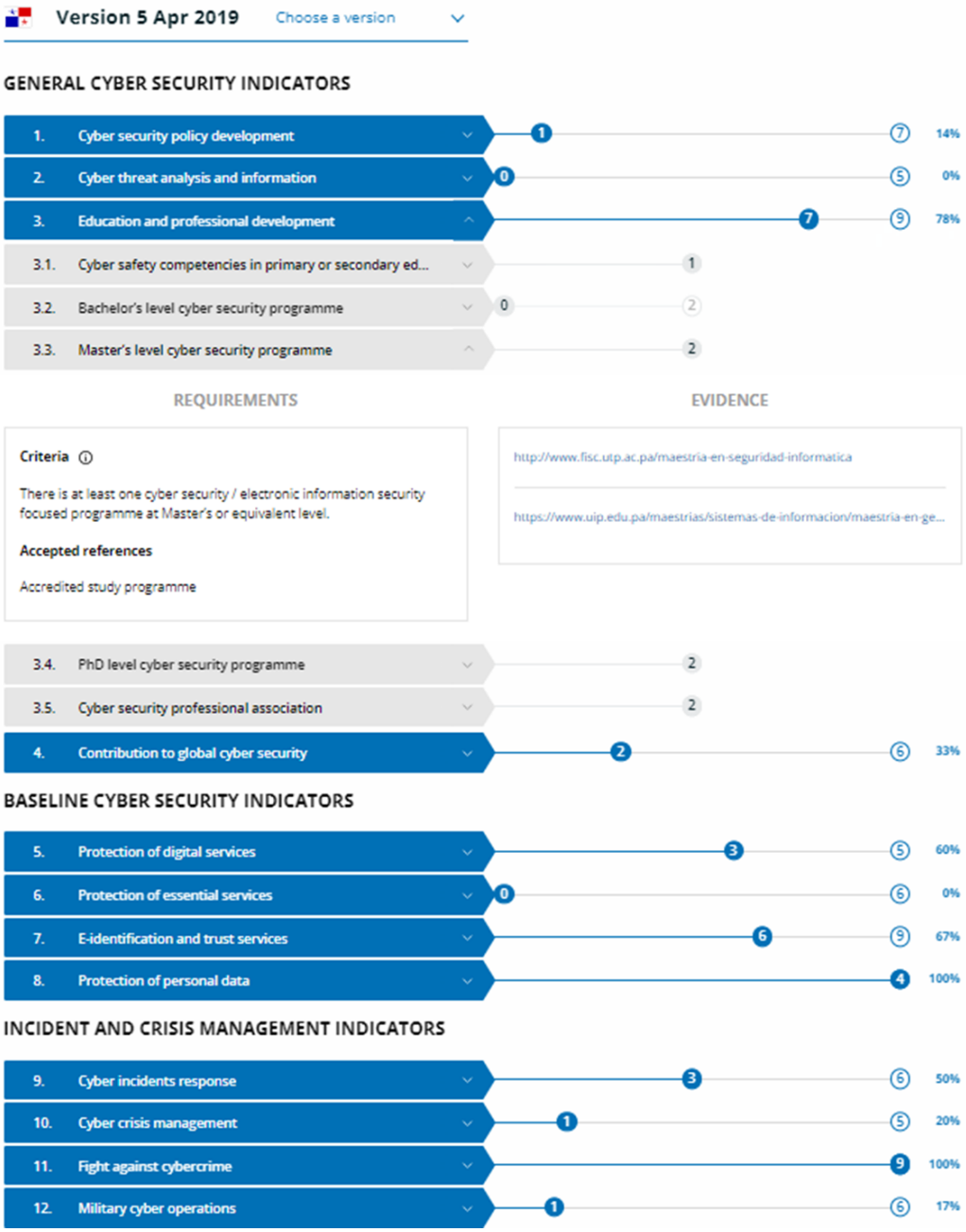


Once the threats were identified, measures and capacities followed, with the selection of important and measurable aspects. This led to the development of the 46 indicators, which in turn are grouped into 12 capacities (seen in Figure 2):

1. Cyber security policy development
2. Cyber threat analysis and information
3. Education and professional development
4. Contribution to global cyber security
5. Protection of digital services
6. Protection of essential services
7. E-identification and trust services
8. Protection of personal data
9. Cyber incidents response
10. Cyber crisis management
11. Fight against cybercrime
12. Military cyber operations

(eGA n.d.-b, 2020)

Figure 2: Partial screenshot of a Country Page (Panama) with the third capacity expanded and Indicator 3.3 expanded as well.



Each measurable indicator is attributed either 0 points (for no evidence) or a specific number of predetermined points (for existing evidence). A country must publicly provide proof of fulfillment of a specific indicator's criteria in order to gain those points. Therefore, to fulfill a specific capacity, a country should provide proof of fulfillment of that capacity's indicators (see Annex 1 for a full overview of the capacities, the indicators, and their respective weights). For example, capacity 1 (i.e., cyber security policy development) contains four indicators (i.e., 1.1, 1.2, 1.3, and 1.4). Each indicator in turn has been assigned a number of points and is subjected to the "all-or-nothing" approach regarding evidence. Then, the points of indicators

with evidence can be divided by the total of points possible in a capacity to indicate the completion rate of that capacity. Following the previous example, if Country A only has evidence for indicator 1.1, it presents a completion rate of 43% for capacity 1; if Country B has evidence for indicators 1.3 and 1.4, it presents a completion rate of 28% for capacity 1; if country C has evidence for all indicators, it presents a completion rate of 100% for capacity 1.

All evidence is collected by the NCSI team, or by country contributors,[2] and is submitted via the back-end platform and verified by experts,[3] who either accept or reject it for the specific indicator that they have been presented. The verification process is not public, but if a piece of evidence is rejected, the experts can leave an explanation for the submitter. Accepted evidence is published in the corresponding country page and visible to any visitor of the website.

The NCSI has been utilized extensively across recent academic debates (Andrade et al. 2021; Calderaro and Craig 2020; Maglaras et al. 2020). Jazri and Jat (2017, 1) mention the NCSI in their road toward *"proposing a simplified and quick framework of measuring cyber security risks profile for critical organizations."* Yarovenko (2020, 195) used the NCSI in her *"assessment of the level of threat to national information security."* Farahbod et al. (2020, 63) uses information from the NCSI and other international indices to *"explore the relationship between cyberattacks and the factors that can possibly be used to predict the impact of such attacks within supply chain domains."* Kruhlov et al. (2020, 1) make use of NCSI country data in their attempt to *"analyze the possibility of providing cybersecurity through the use of public-private partnership (PPP) mechanisms."* Most recently, Urbanovics (2022, 79) utilized NCSI country data for the quantitative analysis of an overarching *"comparative analysis of the strategy development processes in six Latin American countries including Argentina, Brazil, Chile, Colombia, Mexico and Peru."*

The following analysis and discussion sections include the data of all 161 countries that were available in the NCSI in late January 2023 (NCSI 2022; 2023). The data was valid as of its extraction date; however, it was made up from country datasets last updated between 2020 and 2023.[4] Given the large number of the studied sample size, the national results are presented at the level of continents and regions, using the country groupings of the M49 Standard of the Statistics Division of the United Nations Secretariat. It categorizes countries purely by geography and has been used in papers touching upon global matters, albeit mostly in nature research (e.g., De la Fuente et al. 2020, Amon et al. 2022). The M49 Standard was chosen since there exists no other alternative to group such a large sample of countries without running into inherent definition issues due to lack of consensus on the classification terminology (e.g., small, main, developing countries, etc.), there exist no similar papers dealing with such a large sample in the field and the NCSI presents information about U.N. members and allows to visualize them by said standard. Additionally, it is a classification system that helps "*to circumvent several concerns levied against national comparisons*" (Field et al. 2021, 1800).

2 The NCSI core team has varied among the years, containing between two to five individuals, (eGA n.d.-a) while the country contributors themselves have also fluctuated as well, stabilizing at around 60% of the number of countries in the index.

3 As to ensure bias is as low as possible during the verification process, the evidence is checked by at least two different individuals who are considered cybersecurity experts and have previously collaborated in this area with eGA. To guarantee the impartiality of their decisions, their identifiable information is not made public by neither the system nor the NCSI team.

4 Being a live index, the countries are updated constantly and continuously as information is made available by the NCSI team or the different country contributors. As of late January 2023, there were only 161 countries in the NCSI and all of them were last updated between 2020 and 2023. All available countries in the NCSI were used for this publication (see Annex 2 for the comprehensive list), no countries in the NCSI were excluded.

Each country is presented in one region only, and these geographic regions are based on continental regions (United Nations 2021) (see Annex 2 for a full overview of the regions and the countries in them). For a better presentation of the results, the data has been arranged into radar charts (Figures 3 through 8), with each of the spokes (not illustrated for the purpose of simplicity) representing an NCSI capacity (as indicated in each of the vertices), with values corresponding to the completion rate (the center point representing a 0% completion rate, and each vertex, 100% completion rate). The regional average completion rate values for all capacities have been connected to one another through the use of colored lines, thus becoming the global and corresponding regional snapshots. While Figure 3 presents the global and regional snapshots, Figures 4 through 8 also present the best-performing countries for each capacity. This latter group of Figures, in addition to presenting the global and regional snapshots, includes the top two completion rate values for each specific capacity and any country that achieved such value. Said countries have been noted using the ISO 3166-1 alpha-2 country codes,[5] and placed in a random order around the corresponding point that represents the value of the completion rate. If more than eight countries at a time scored the same completion rate, the placeholder "M#C" (i.e., multiple number of countries) has been used in the figures to replace such a large group of countries that cannot be orderly presented in the figure.

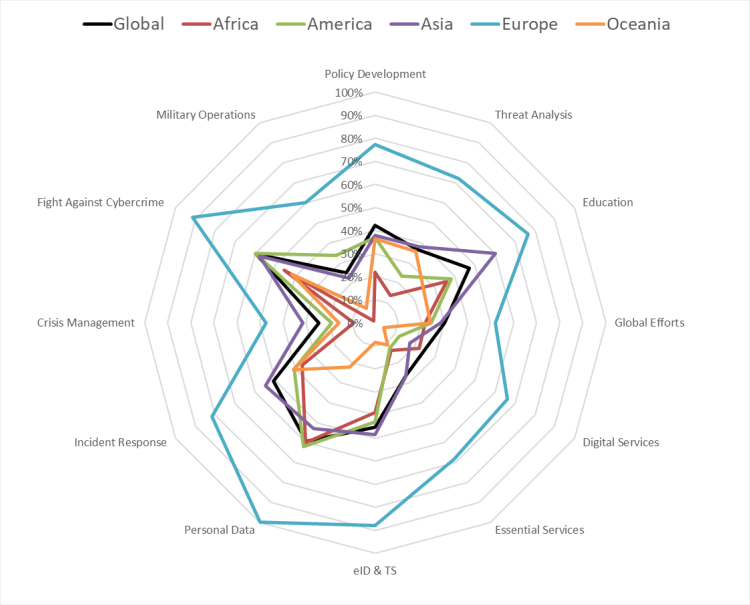
Global and Regional Findings

Globally, personal data protection and fight against cybercrime capacities represent the top focus of countries. Africa, the Americas, Asia, and Europe present more than 50% completion for the former capacity, while only America, Asia, and Europe do so for the latter. Incident response is slightly above halfway its completion rate; however, this is due to Europe and Asia's completion rates balancing out the lower ones from the rest of the regions.

The protection of digital services and crisis management capacities have been underdeveloped globally. All regions, except for Europe, present less than 25% completion in relation to digital service protection. Crisis management is Europe's lowest completion rate (47%), which is still higher than the rest of the regions. Throughout the world, the other lagging capacities are cyber military operations and the protection of essential services. The rest of the capacities have more mid-range completion values, however, variations among individual regions. Based on the collected data, the cyber security trends as of late January 2023 have been as shown in Figure 3.

5 The ISO 3166 standard can be found at: https://www.iso.org/iso-3166-country-codes.html.

Figure 3: Global cybersecurity focus in each of the individual regions.



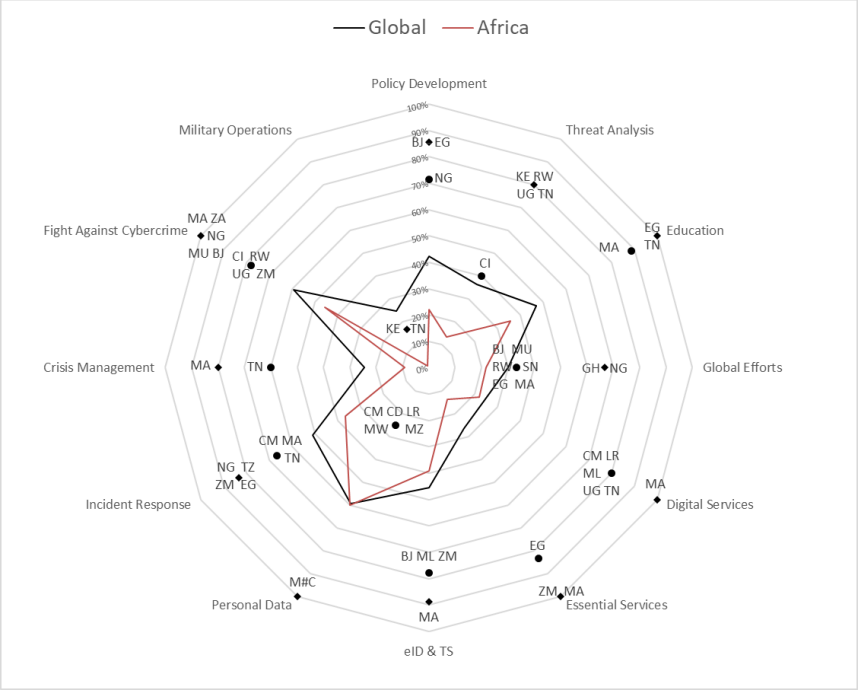
The next sub-sections will delve into the different regions, in alphabetical order, and their findings, followed by the "Discussion and Recommendations" section which will present inductive trends and patterns.

Africa

The African region excels at personal data protection (in relation to the rest of the capacities), with mid-range scores in the fight against cybercrime, incident response, and electronic identification and trust services. They are underdeveloped in military operations and cyber crisis management, with more work needed regarding the protection of essential services and cyber threat analysis. Morocco and Tunisia score the highest, with high completion percentages in nine and seven of the capacities, respectively (Figure 4).

In this region, 46% of the countries have no policy development capacity at all. As of 2023, only Benin and Egypt lead the capacity, followed by Nigeria. Similarly, threat analysis is among the capacities that contain the lowest completion in Africa. Nevertheless, four countries present the highest (80%) completion rate. Egypt and Tunisia lead in the next capacity related to education and professional development, while Nigeria and Ghana lead with a 67% completion rate in global efforts (Figure 4).

Figure 4: Cybersecurity focus in Africa and top scorers for each capacity.



Morocco is at the forefront with a 100% completion rate in the protection of digital services capacity, closely followed by Cameroon, Liberia, Malawi, Tunisia, and Uganda. Zambia, Morocco, and Egypt return with completion rates of 100%, 100%, and 83%, respectively, for the protection of essential services. Regarding electronic identification and trust services, Benin, Mali, and Zambia have a 78% completion rate, following Morocco's 100% completion rate (Figure 4).

Data protection is the capacity in which 21 out of the 37 African countries in the NCSI have achieved a 100% completion rate, with Cameroon, the Democratic Republic of Congo, Liberia, Malawi, and Mozambique following with 25%. The incident response capacity has four leading countries (Egypt, Nigeria, Tanzania, and Zambia) all with an 83% completion rate. However, cyber crisis management is underdeveloped in Africa (and led by Morocco and Tunisia with an 80% and 60% completion rate, respectively). In the fight against cybercrime, Benin, Mauritius, Morocco, Nigeria, and South Africa lead with a 100% completion rate. Finally, in the military operations capacity, Kenya and Tunisia lead with a 17% completion rate because of their participation in international military exercises with cyber components (Figure 4).

Americas

The American region's average overall trends are under the global average, except for the Military Cyber Operations, Fight Against Cybercrime, and Personal Data Protection capacities. The countries should work hard to improve the protection of digital and essential services, crisis management, and threat analysis. The Dominican Republic has eight capacities with high completion percentages, while Canada, Paraguay, and the United States follow with high completion percentages in seven capacities. Nevertheless, other countries also score at the top in individual capacities (Figure 5).

Figure 5: Cybersecurity focus in the Americas and top scorers for each capacity.

Regarding policy development, a 100% completion rate exists in the United States, Ecuador, Paraguay, Dominican Republic, and Chile. However, threat analysis and global effort capacities are very underdeveloped in the region, with only a handful of countries leading them (Figure 5).

The education capacity is headed by Canada and the United States, with 100% and 89% completion rates, respectively. Slightly more than one third of the region maintains some level of protection of digital services, with Cuba and Peru leading with 100% and 80% completion rates (Figure 5).

Regarding the essential services protection capacity, Paraguay and Uruguay are both at 50%, and Peru at 67% completion rate, with almost half of the countries not having any protective elements whatsoever. Electronic ID and trust services in the region are spearheaded by Paraguay 100% and Uruguay 89%. In the region, almost 70% have passed some sort of data protection legislation, but evidence has found that only 21 of them have established a corresponding authority.

Cyber incident response is led by Peru 100%, followed by Bolivia, Costa Rica, the Dominican Republic, Ecuador, Trinidad and Tobago, Paraguay, Uruguay, and Canada, with an 83% completion rate. Crisis management is the third most underdeveloped capacity of the region, spearheaded by the United States with 80% and Panama, Argentina, Paraguay, and the Dominican Republic's 40% completion rates (Figure 5).

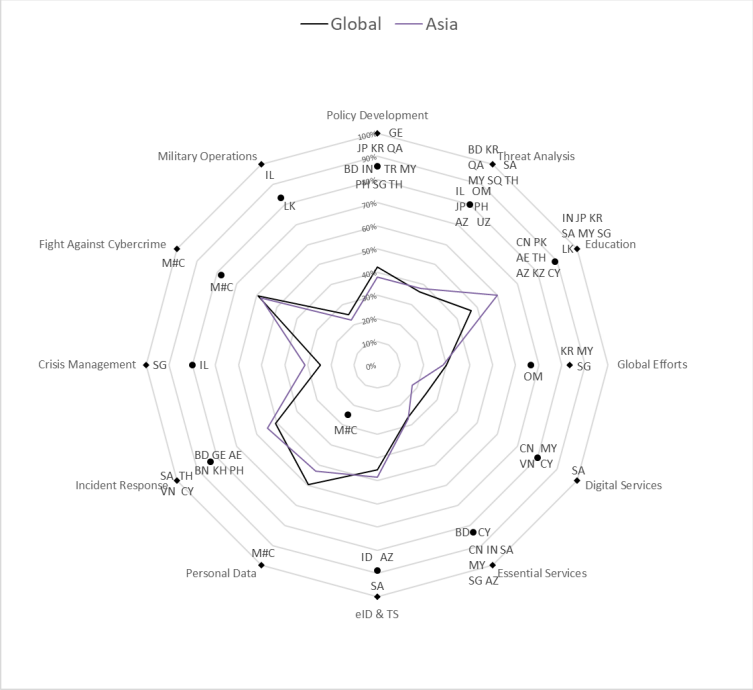
The fight against cybercrime capacity is the closest capacity to the global average, however, above it (Chile, Colombia, Costa Rica, the Dominican Republic, Panama, Peru, Canada, the U.S., Argentina, and Paraguay lead with a 100% completion rate, with followed by other countries' 78% rate). Finally, the region's military cyber operations capacity exceeds the global average, and is spearheaded by four Latin American countries, Canada, and the United States (Figure 5).

Asia

Asia's highest-scoring capacity revolves around education, followed by the fight against cybercrime. Their lowest scores are evidenced in the protection of digital services, followed by cyber military operations and the protection of essential services. Saudi Arabia, Singapore, and Malaysia score the highest, with high completion percentages in eight of the capacities, respectively, followed by South Korea and Cyprus, in six of them.

In Asia, the policy development capacity's average is below the global average. Only 17 nations (41% of the countries in the sample) have reached a completion rate of more than 50%. Out of these, Georgia, Japan, South Korea, and Qatar have achieved a 100% completion rate in the policy development capacity (Figure 6).

Figure 6: Cybersecurity focus in Asia and top scorers for each capacity.



Regionally speaking, the threat analysis capacity is barely higher than the global average, with Bangladesh, Malaysia, Qatar, Saudi Arabia, Singapore, South Korea, and Thailand having achieved a 100% completion rate. The education capacity in the region is better than the global average, with 61% of the sample countries achieving more than 50% of completion rate. However, in global efforts, the Asian region scores lower than the global average, with South Korea, Singapore, and Malaysia spearheading efforts (Figure 6).

As previously mentioned, the digital services protection trend in Asia is below the global average. Only Saudi Arabia reaches a 100% completion rate, while China, Cyprus, Malaysia, and Vietnam score 80%. Essential service protection, from a regional perspective, is tied to the global trend. The top scorers of this capacity include Azerbaijan, China, India, Malaysia, Saudi Arabia, and Singapore. eID and trust services are spearheaded by Saudi Arabia (100%) and Indonesia and Kazakhstan (89% completion rates) (Figure 6).

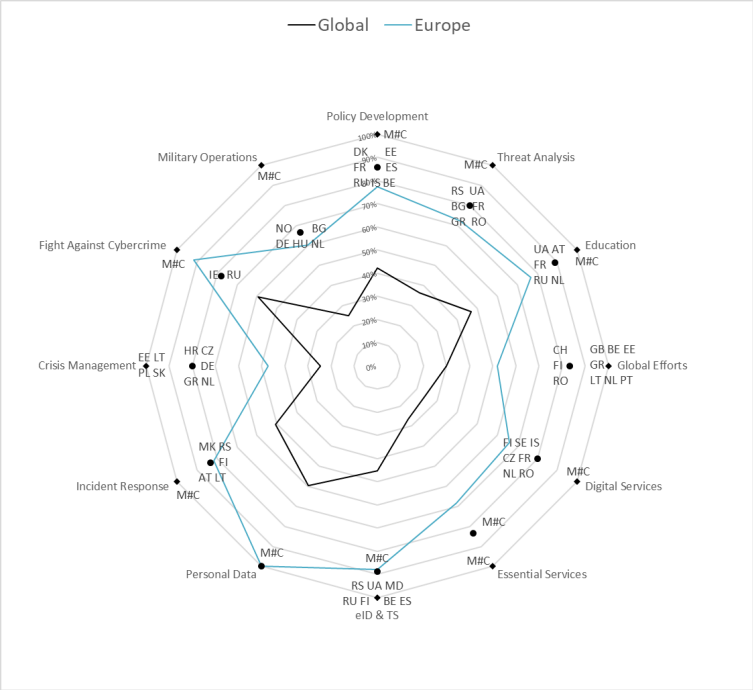
Data protection has been legislated in 30 countries, but the corresponding authority has only been found in 19 of them. Regional incident response capacity is slightly better than the global mean. Cyprus, Saudi Arabia, Thailand, and Vietnam, lead with a 100% completion rate (Figure 6).

Crisis management is the fifth lowest capacity in the region, but it is still better than the global average. Singapore leads with a 100% completion rate, followed by Israel, with 80%. In the fight against cybercrime, the region scores slightly below the global average. Of the sample, 32 nations have evidence of some form of unit designated to tackle cybercrime and 19 have a governmental digital forensics unit. Finally, in the military operations capacity, Israel presents a 100% completion rate, followed by Sri Lanka at 83% (Figure 6).

Europe

Europe's capacities exceed the global average, and they are top performers in personal data protection. Their lower scores are focused on crisis management, global efforts, and military operations capacities. Greece, Belgium, Czech Republic, Germany, and Lithuania are the top scorers with high completion rates; however, they are not the only ones (Figure 7).

Figure 7: Cybersecurity focus in Europe and top scorers for each capacity.



Out of the 39 countries of the region, 30 have established a cyber security policy unit, and have indicated a policy coordination format (but not necessarily the same countries). Only 36 nations have published a national cybersecurity strategy, and of those only 25 have a corresponding implementation plan. Regionally, the cyber threat capacity is regionally at a high level: 34 of the countries maintain a cyber safety and security website, 28 of them have established a cyberthreat analysis unit, and 23 regularly publish their cyber threat reports.

The educational capacity is also well developed in the region. Master's degrees in cybersecurity topics are the most common educational level with 34 countries having some form of program, and PhD level programs are the least available in 24 countries. Global efforts are also quite spread out in the region. The United Kingdom, Belgium, Estonia, Greece, Lithuania, the Netherlands, and Portugal lead in this capacity with a 100% completion rate (Figure 7). The Budapest convention on cybercrime has been signed by 36 nations and all the countries in the region maintain representation in international cyber security cooperation formats.

Approximately 92% of the region has undertaken efforts to protect digital service providers, of which 28 nations have established cyber security responsibilities for digital service providers, while 26 countries have done so for the public sector as well. The essential services capacity is also widespread, 34 of the countries have identified their corresponding operators of essential services while 31 of those have legally required them to follow those minimum cybersecurity standards for their protection and 27 have established at least one competent corresponding supervisory authority.

The basis for eID and trust services has been well cemented in the region and cyber incident response is similarly almost universal (i.e., a regional average completion rate value that is equal to the second top completion rate value, and close to 100%, for each capacity). However, the cyber crisis management capacity is the least developed in the region. Even though 32 countries have participated in international cyber crisis exercises and 20 have executed their own national-level drills, only 12 nations have made public any kind of cyber crisis management plan and only 8 have legislated operational support from volunteers during cyber crises.

Finally, combating cybercrime is also a highly scored regional endeavor, while almost 85% of the region's countries present evidence of military cyber operation capacities.

Oceania

Oceania's strengths surface relative to incident response, policy development, and the fight against cybercrime. Its threat analysis capacity almost equals the global average trend; however, there is still a lot of work to be done in all the rest of the capacities since they are below the global average, and more specifically in terms of digital service protection, electronic ID and trust services and military operations. Australia and New Zealand spearhead the region, with high completion rates in 12 and 10 of the capacities, respectively (Figure 8).

Figure 8: Cybersecurity focus in Oceania and top scorers for each capacity.

The policy development capacity in the region is led by Australia with a full completion rate, closely followed by Vanuatu with 71%. Threat analysis capacities in the region are led by Australia and New Zealand with a 100% completion rate followed up by Tonga with an 80% completion rate. Regarding education, only three countries register any completion rate, Australia, and New Zealand at 100% and Papua New Guinea at 22% (Figure 8).

Australia and Tonga are the only countries that have signed the Convention on Cybercrime, and Australia and New Zealand have endeavored in cyber security capacity-building activities for other countries and personal data protection. Nevertheless, all countries in the region maintain representation in international cooperation formats.

The protection of digital services is the most underdeveloped capacity in the region (with Australia and New Zealand's 20% completion rate) and the protection of essential services is led by a 17% completion rate by multiple countries. Cyber incident response has also been undertaken by two thirds of the nations and is spearheaded by New Zealand. Personal data protection is led once again by Australia and New Zealand with full completion rates, having passed personal data protection acts and established the corresponding authority. No other country in the region has advanced in terms of this capacity (Figure 8).

Cyber incident response has also been undertaken by two thirds of the nations, led the capacity by Papa New Guinea and Vanuatu with an 83% completion rate, while the rest of the countries follow at 50%. The crisis management capacity only shows endeavors in three countries Australia 80%, New Zealand 40%, followed by Tonga. In relation to the fight against cybercrime, there has been much more activity in the region. Seven nations criminalize cybercrimes while Australia and New Zealand contain both cybercrime and digital forensics units. Finally, in relation to the military cyber operations capacity only Australia has a cyber operations unit and has participated in international military cyber exercises (Figure 8).

Discussion and Recommendations

Globally, the snapshot provided in this study appears to demonstrate countries focusing on reactionary measures rather than proactive endeavors. This is exhibited by the high scores in the fight against cybercrime and incident response capacities and the low scores in digital and essential services protection, cyber crisis management, and threat analysis. Countries must implement and/or improve upon their proactive activities, in addition to being prepared to react to incidents and threats. With ever-increasing levels of electronic and trust services throughout the world, all stakeholders should realize that cyber security is a concern for everyone. In that line of thought, global efforts (from those within the same region and to those across regional boundaries) must be redoubled and increased so that different capacities may be developed by those countries that need them. The shared data also shows that best practices can be implemented no matter the characteristics of the country or the type of government that it might have.

Africa's high score in personal data protection might have been the result of the adoption of the African Union Convention on Cyber Security and Personal Data Protection, since 2014, which states that the signatories would commit to establishing a legal framework relative to personal data protection. This brings up considerations that regional agreements and treaties might help push national cybersecurity toward improvement. It would be worth exploring if such a commitment for any of the other capacities would make a positive difference in the region. Given the region's young population, we advocate for less efforts into the military cyber operations capacity and more development of educational opportunities, coupled with the creation of the protective frameworks through crisis management mechanisms and the protection of the digital and essential services. Similarly, threat analysis and policy development seem to be lagging behind, both of which are necessary components for a robust level of national cybersecurity.

Generally speaking, government regulation of the private sector is not well seen in the Americas region. While this might not be the main or only reason behind the low scores in the digital and essential services protection, we believe that it is still an important component. When talking about national cybersecurity, multiple stakeholders have responsibilities in this context. The government must work with the private sectors and all other relevant parties to establish a baseline of minimum cyber security requirements and to ensure their application. An interesting phenomenon was identified in the Caribbean subregion, where island nations had scored for the protection of essential services. Closer inspection revealed that they had identified their essential services prior to the advent of modern ICT (identified by the dates of enactment of the legislation relative to natural disasters and essential services). These countries can work with the existing legislation so that in addition to natural phenomena crises, they are also covered in case of cyber incidents. Next to Oceania and Africa, this region has also the lowest average score in regard to the education capacity; future efforts must focus on these components. With the ongoing development of the region, threat analysis and cyber crisis management must also become strategic priorities, especially for those countries lacking a national armed force.

Second to Europe, Asia's focus on the education capacity is a step in the right direction for the future of the region. Nevertheless, efforts must not shun away from the protection of digital and essential services. With better scores in response crisis management and threat analysis

than the global average, intra-regional efforts and cooperation should allow individual countries to reach a more homogeneous level. Policy development electronic identification trust services and personal data protection must also receive a boost.

Europe's all-around high-leveled capacities could be attributed to the regional standards and common legislative instruments[6] that have pushed the issue of cybersecurity to the forefront. Nevertheless, the cyber crisis management capacity is still a bit lacking in this respect and further endeavors must be geared toward developing these components. The high scores of the education capacity should further be reflected into global efforts and cooperation. We believe the main risk to the region to be complacency and the maintenance of the status quo, which must never be the norm around always progressing cyber capacity building and technological advancements.

The sample of countries from Oceania is limited due to the lack of available infrastructure and hardware necessary for the maintenance of cyberspace in such remote nations. Similarly, to the Caribbean nations (in the American region), most of the countries have identified their essential services due to legislation dealing with emergency situations, caused specifically by natural phenomena. While not specifically related to the cybersecurity topic, the identification of such services gives them an advantage since they can now build upon it with the corresponding cyber security legislation. Nevertheless, they must make sure that in the context of cyberspace, they have identified all the necessary essential services for them to be fully protected. The military cyber operations capacity will be hard to improve within the remote island nations due to their inherent lack of armed forces. Rather, those efforts must be redirected into the protection of digital and essential services and the development of a cyber crisis management system.

Limitations and Future Research

The NCSI itself presents a couple of biases. The first one is that it was created within the context of the European Union and its understanding of cybersecurity, by an Estonian team. As such, some of the indicators were modeled after studying the best practices of the European region. Since the indicators are the components of the capacities and the "all-or-nothing" approach is followed regarding the allotment of points in the event of evidence, this has an impact on the completion rate for the countries. Nevertheless, even if such indicators might provide a region with any apparent advantage, they are still some of the best practices in national cybersecurity that have been implemented and exist around the world. Any similar metrics, with a different degree of strictness, would still yield the same inductive trends (i.e., similarities and differences), and any different metrics are outside the scope of this paper, but a good starting point for future research. The second bias is the fact that the index only accepts publicly available evidence. In some countries, cybersecurity is intricately connected with the concept of national security and as such, evidence might not be disclosed to the public. In such cases, it is not possible to award the points if there is no publicly available evidence that can be shared. Nevertheless, the creators and administrators of the index believe that

6 At first glance, inductively, more European Union (EU) countries have an increased number of 100% completion rates in multiple capacities, than non-EU countries. However, the M49 Standard of the Statistics Division of the United Nations Secretariat does not group all EU countries in the same region. Additionally, under this grouping, the term "non-EU countries" includes the Russian Federation, Switzerland, and the United Kingdom, which are all showcased in the region for their performance. Future research is recommended on supranational unions, specific subregions, and/or categories.

having a multinational index based on publicly available official information outweighs any downgrade in position that a country might suffer due to lack of transparency.

The article has presented how national cybersecurity is being undertaken throughout the world. Regional trends (i.e., similarities and differences) exist (as presented in the previous section), but globally, reactionary measures are being preferred rather than proactive ones. The paper also presents a number of countries from which best practices can be adopted for specific topics (as presented in the regional subsections of the "Global and Regional Findings" section). As previously stated, this article serves as a global and regional snapshot and point of reference for any future single case or comparative studies of national cybersecurity. Since national cybersecurity includes so many individual components and since this article explores 161 countries in an overarching way, we believe that there will never not be a lack of future research topics stemming from this document in this field. With this article, we also wanted to showcase countries and regions that have arguably been underrepresented across academic literature and policy debates and give visibility to their efforts, i.e., non-major states and actors. Future case studies could start focusing on these countries through the whole 12 capacities lens or more in-depth with some of the specific indicators. Similar comparative studies may be proposed among specific subregions and subcategories (i.e. developing, small, island, etc.) of nations, or supranational unions (i.e. African Union, European Union, Caribbean Community, etc.). Since the NCSI is publicly available, such possibilities will remain on the table.

Disclaimers

The NCSI was originally developed through the "Development of a National Cyber Security Index" project, funded by the Ministry of Foreign Affairs of Estonia and managed by the e-Governance Academy. The author of this article has acquired and managed the country data for the NCSI and this article through the following projects: 2018-2020 "Shaping of Trusted Information Societies in Developing Countries"; 2020-2022 "Advancing Cybersecurity Capacities for Digital Transformation"; all funded by the Ministry of Foreign Affairs of Estonia and managed by the e-Governance Academy. The NCSI updated its methodology in November 2023. Nevertheless, all data from the previous methodology (i.e., that was used for this article) was saved for historical purposes and is publicly available.

Acknowledgments

I would like to extend my thanks and appreciation to my colleagues at the e-Governance Academy's Cybersecurity Competence Center (Ms. Merle Maigre, Ms. Epp Maaten, Ms. Kadri Kaska, and Mr. Hauke Schulz) and to all the national contributors who have helped to keep the NCSI up to date throughout the years.

Annex 1

NCSI Capacities and their Indicators	% Value of Corresponding Capacity
1. Cyber security policy development	100
1.1. Cyber security policy unit	43
1.2. Cyber security policy coordination format	29
1.3. Cyber security strategy	14
1.4. Cyber security strategy implementation plan	14
2. Cyber threat analysis and information	100
2.1. Cyber threats analysis unit	60
2.2. Public cyber threat reports are published annually	20
2.3. Cyber safety and security website	20
3. Education and professional development	100
3.1. Cyber safety competencies in primary or secondary education	11
3.2. Bachelor's level cyber security programme	22
3.3. Master's level cyber security programme	22
3.4. PhD level cyber security programme	22
3.5. Cyber security professional association	22
4. Contribution to global cyber security	100
4.1. Convention on Cybercrime	17
4.2. Representation in international cooperation formats	17
4.3. International cyber security organisation hosted by the country	50
4.4. Cyber security capacity building for other countries	17
5. Protection of digital services	100
5.1. Cyber security responsibility for digital service providers	20
5.2. Cyber security standard for the public sector	20
5.3. Competent supervisory authority	60
6. Protection of essential services	100
6.1. Operators of essential services are identified	17
6.2. Cyber security requirements for operators of essential services	17
6.3. Competent supervisory authority	50
6.4. Regular monitoring of security measures	17
7. E-identification and trust services	100
7.1. Unique persistent identifier	11
7.2. Requirements for cryptosystems	11
7.3. Electronic identification	11
7.4. Electronic signature	11
7.5. Timestamping	11
7.6. Electronic registered delivery service	11
7.7. Competent supervisory authority	33

NCSI Capacities and their Indicators	% Value of Corresponding Capacity
8. Protection of personal data	100
8.1. Personal data protection legislation	25
8.2. Personal data protection authority	75
9. Cyber incidents response	100
9.1. Cyber incidents response unit	50
9.2. Reporting responsibility	17
9.3. Single point of contact for international coordination	33
10. Cyber crisis management	100
10.1. Cyber crisis management plan	20
10.2. National-level cyber crisis management exercise	40
10.3. Participation in international cyber crisis exercises	20
10.4. Operational support of volunteers in cyber crises	20
11. Fight against cybercrime	100
11.1. Cybercrimes are criminalised	11
11.2. Cybercrime unit	33
11.3. Digital forensics unit	33
11.4. 24/7 contact point for international cybercrime	22
12. Military cyber operations	100
12.1. Cyber operations unit	50
12.2. Cyber operations exercise	33
12.3. Participation in international cyber exercises	17

Annex 2

The 161 countries in NCSI and analyzed in this paper are as follows: 37 countries from Africa, 35 from America, 41 from Asia, 39 from Europe, and 9 from Oceania.

Africa	America	Asia	Europe	Oceania
Angola	Antigua and Barbuda	Afghanistan	Albania	Australia
Algeria	Argentina	Armenia	Austria	Kiribati
Benin	Bahamas	Azerbaijan	Belarus	New Zealand
Botswana	Barbados	Bahrain	Belgium	Papua New Guinea
Burundi	Belize	Bangladesh	Bosnia and Herzegovina	Samoa
Cameroon	Bolivia	Bhutan	Bulgaria	Solomon Islands
Chad	Brazil	Brunei Darussalam	Croatia	Tonga
Congo (Democratic Republic of the)	Canada	Cambodia	Czech Republic	Tuvalu
Côte d'Ivoire	Chile	China	Denmark	Vanuatu
Egypt	Colombia	Cyprus	Estonia	
Ethiopia	Costa Rica	Georgia	Finland	
Ghana	Cuba	India	France	
Kenya	Dominica	Indonesia	Germany	
Liberia	Dominican Republic	Iran (Islamic Republic of)	Greece	
Libya	Ecuador	Israel	Hungary	
Madagascar	El Salvador	Japan	Iceland	
Malawi	Grenada	Jordan	Ireland	
Mali	Guatemala	Kazakhstan	Italy	
Mauritania	Guyana	Korea (Republic of)	Latvia	
Mauritius	Haiti	Kyrgyzstan	Lithuania	
Morocco	Honduras	Lao PDR	Luxembourg	
Mozambique	Jamaica	Malaysia	Malta	
Namibia	Mexico	Mongolia	Moldova (Republic of)	
Nigeria	Nicaragua	Myanmar	Montenegro	
Rwanda	Panama	Nepal	Netherlands	
Senegal	Paraguay	Oman	North Macedonia	
Seychelles	Peru	Pakistan	Norway	

Africa	America	Asia	Europe
Sierra Leone	Saint Kitts and Nevis	Philippines	Poland
Somalia	Saint Lucia	Qatar	Portugal
South Africa	Saint Vincent and the Grenadines	Saudi Arabia	Romania
South Sudan	Suriname	Singapore	Russian Federation
Sudan	Trinidad and Tobago	Sri Lanka	Serbia
Zambia	United States	Syrian Arab Republic	Slovakia
Zimbabwe	Uruguay	Tajikistan	Slovenia
Tanzania, United Republic of	Venezuela	Thailand	Spain
Tunisia		Turkey	Sweden
Uganda		Turkmenistan	Switzerland
		United Arab Emirates	Ukraine
		Uzbekistan	United Kingdom
		Vietnam	
		Yemen	

References

Amon, D. J. et al. 2022. "My Deep Sea, My Backyard: A Pilot Study to Build Capacity for Global Deep-Ocean Exploration and Research." *Philosophical Transactions of the Royal Society B* 377(1854), 20210121. doi: http://doi.org/10.1098/rstb.2021.0121

Andrade, R. O. et al. 2021. "A Comprehensive Study About Cybersecurity Incident Response Capabilities in Ecuador." *Advances in Intelligent Systems and Computing* 1277, 281-292. doi: https://doi.org/10.1007/978-3-030-60467-7_24

Bada, M., B. Von Solms and I. Agrafiotis. 2019. "Reviewing National Cybersecurity Awareness for Users and Executives in Africa." *International Journal On Advances in Security* 12(1&2), 108-118. doi: https://doi.org/10.48550/arXiv.1910.01005

Bay, M. 2016. "What is Cybersecurity? In search of an encompassing definition for the post-Snowden era." *French Journal for Media Research* 6, 1-28.

Berthelet, P. 2020. «La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels.» *Revue Québécoise de Droit International* Special Issue, 25-39. doi: https://doi.org/10.7202/1067257ar

Calderaro, A. and A. J. S.Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." *Third World Quarterly* 41(6), 917-938. doi: https://doi.org/10.1080/01436597.2020.1729729

Carlini, A. 2016. "Ciberseguridad: un nuevo desafío para la comunidad internacional." *Bie3: Boletín IEEE* (2) 950-966.

Craigen, D., N. Diakun-Thibault and R. Purse. 2014. "Defining Cybersecurity." *Technology Innovation Management Review* 4(10), 13-21. doi: https://doi.org/10.22215/timreview835

De la Fuente, B. et al. 2020. "Built-Up Areas Within and Around Protected Areas: Global Patterns and 40-Year Trends." *Global Ecology and Conservation* 24, e01291. doi: https://doi.org/10.1016/j.gecco.2020.e01291

Dewar, R. S. et al. 2018. *National Cybersecurity and Cyberdefense Policy Snapshots*. ETH Zurich, Switzerland. doi: https://doi.org/10.3929/ethz-b-000314596

eGA. n.d.-a. *National Cyber Security Index*. https://ncsi.ega.ee/. Last accessed January 2023.

eGA. n.d.-b. *NCSI - Methodology*. https://ncsi.ega.ee/methodology/. Last accessed October 2022.

eGA. 2020. *National Cyber Security in Practice*. https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

eGA. 2022. *Upgrading National Cyber Resilience: National Cybersecurity in Practice 2*. https://ega.ee/wp-content/uploads/2021/05/NCSI-Cyber-Resilience-Digi_F.pdf

ENISA - European Union Agency for Network and Information Security. 2015. *Definition of Cybersecurity - Gaps and Overlaps in Standardisation*. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf

ENISA - European Union Agency for Network and Information Security. 2017. *ENISA Overview of Cybersecurity and Related Terminology*. https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf

Farahbod, K., C. Shayo and J. Varzandeh. 2020. "Cybersecurity Indices and Cybercrime Annual Loss and Economic Impacts." *Journal of Business and Behavioral Sciences 30*(1), 63-71. http://asbbs.org/files/2020/JBBS_32.1_Spring_2020.pdf

Field, J. G. et al. 2021. "More alike than different? A Comparison of Variance Explained by Cross-Cultural Models." *Journal of International Business Studies* 52, 1797-1816. doi: https://doi.org/10.1057/s41267-021-00428-z

Guranda, V. 2021. La Cyber-sécurité. *Technical-Scientific Conference of Undergraduate, Master and Phd Students* 1, 383-385. https://ibn.idsi.md/ro/vizualizare_articol/134005/datacite

Ham, J. Van Der. 2021. "Toward a Better Understanding of 'Cybersecurity'." *Digital Threats: Research and Practice* 2(3), 1-3. doi: https://doi.org/10.1145/3442445

ITU-D. n.d. ITU-D Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model (Methodology). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf. Last accessed January 2023.

Jazri, H. and D. S. Jat. 2017. A quick cybersecurity wellness evaluation framework for critical organizations. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. doi: https://doi.org/10.1109/ICTBIG.2016.7892725

Kruhlov, V. et al. 2020. Public-private partnership in cybersecurity. *CEUR Workshop Proceedings* 2654. https://ceur-ws.org/Vol-2654/paper48.pdf

Le Barreau, L. and E. Longeon. 2016. «Les enjeux de cybersécurité en Arabie saoudite: Variables culturalistes et conceptualisation d'une stratégie nationale.» *Études Internationales* 47(2-3), 155-175. doi: https://doi.org/10.7202/1039541ar

Loiseau, H. et al. 2013. «La stratégie du Canada en matière de cybersécurité : de la parole aux actes?» *Canadian Foreign Policy Journal* 19(2), 144-157. doi: https://doi.org/10.1080/11926422.2013.805151

Maglaras, L. et al. 2020. "Cybersecurity in the Era of Digital Transformation: The Case of Greece." *2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020*. doi: https://doi.org/10.1109/ITIA50152.2020.9312297

Newmeyer, K., E. Cubeiro and M. Sánchez. 2015. "Ciberespacio, Ciberseguridad Y Ciberguerra." *II Simposio Internacional de Seguridad y Defensa: Perú 2015*, 76-95.

Newmeyer, K. P. 2015. "Elements of National Cybersecurity Strategy for Developing Nations." *National Cybersecurity Institute Journal* 1(3), 9-19.

NCSI. 2022. Happy New Year 2023!. In *News*. https://ncsi.ega.ee/88/happy-new-year-2023/

NCSI. 2023. Updated Countries January 2023. In *News*. https://ncsi.ega.ee/89/updated-countries-january-2023/

Pohlmann, N. 2019. Cyber-Sicherheit. In *Cyber-Sicherheit*. Springer Fachmedien Wiesbaden GmbH. Wiesbaden, Germany. doi: https://doi.org/10.1007/978-3-658-25398-1

Romaniuk, S. and M. Manjikian. 2021. *Routledge Companion to Global Cyber-Security Strategy.* 1st ed. Milton: Taylor and Francis.

Samonas, S. and D. Coss. 2014. "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security." *Journal of Information System Security* 10(3), 21-45.

Shackelford, S. and A. Kastelic. 2014. "Toward a State-Centric Cyber Peace? Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity." *SSRN Electronic Journal* 18, 895-984. doi: https://doi.org/10.2139/ssrn.2531733

Stevens, T. 2018. "Global Cybersecurity: New Directions in Theory and Methods." *Politics and Governance* 6(2), 1-4. doi: https://doi.org/10.17645/pag.i92

United Nations. 2021. *Standard country or area codes for statistical use (M49): Geographic Regions*. Series M, No. 49. https://unstats.un.org/unsd/methodology/m49/. Last accessed January 2023.

Urbanovics, A. 2022. "Cybersecurity Policy-Related Developments in Latin America." *Academic and Applied Research in Military and Public Management Science* 21(1), 79-94. doi: 10.32565/aarms.2022.1.6

Yarovenko, H. 2020. "Evaluating the Threat to National Information Security." *Problems and Perspectives in Management* 18(3), 195-210. doi: https://doi.org/10.21511/ppm.18(3).2020.17

Radu Antonio Serrano Iova works as an Expert at the e-Governance Academy. His responsibilities include managing and updating the National Cyber Security Index database, in addition to assisting with other international projects in the fields of cybersecurity, e-governance, and digital transformation. Radu holds a Doctorate degree in Public Administration with a Specialization in Technology Governance, from Tallinn University of Technology. His academic research and multiple publications have been focused on topics of cybersecurity, internet voting, foreign direct investment, and the Panamanian economy. Email: raduserrano@hotmail.com