Cybersecurity in the Era of Digital Transformation: The case of Greece

Leandros Maglaras
Cyber Technology Institute
De Montfort University, Leicester, UK
& National Cyber Security Authority of Greece, Athens
leandros.maglaras@dmu.ac.uk

George Drivas
Department of Digital Systems
University of Piraeus, Peiraeus, Greece
& National Cyber Security Authority of Greece, Athens
george.drivas@unipi.gr

Nestoras Chouliaras
Dept. of Informatics & Computer Eng.
University of West of Attica, Greece
& National Cyber Security Authority of Greece, Athens
nchouliaras@uniwa.gr

Eerke Boiten
Cyber Technology Institute
De Montfort University, Leicester, UK
eerke.boiten@dmu.ac.uk

Costas Lambrinoudakis
Department of Digital Systems
University of Piraeus, Peiraeus, Greece
clam@unipi.gr

Sotiris Ioannidis
School of Electrical & Computer Eng.
Technical University of Crete &
Foundation for Research and
Technology Hellas
Sotiris@ece.tuc.gr

***Abstract*—This article presents the cyber security progress in Greece since the creation of the Greek National Cyber Security Authority as a nation-wide cybersecurity coordination and policy making unit. During this period, Greece issued a Ministerial Decree that established the National Cyber Security Authority, issued the National Cybersecurity strategy, transposed the NIS Directive to National Law and issued a Ministerial Decree that helped establish a cybersecurity framework for the public sector and the critical infrastructures that reside in Greece. This structured effort led to the achievement of gaining the 1st position in the prestigious NCSI index for Greece, amongst 160 countries.**

Keywords—cybersecurity, policy, maturity framework

I. Introduction

Cybersecurity is a very important aspect of the digital development that every country around the globe aims to achieve [1]. In order to offer new online applications and remote services to citizens, these must be secured and robust to several attacks. Recently several critical incidents have targeted service providers of National Critical Infrastructures (NCIs). In September 2018, following the "Cyber Europe" exercise that tested European reaction and cooperation against a cyber-attack to the aviation sector, information screens in Bristol airport were taken offline by a "ransomware" type attack [2].

As Critical National Infrastructures are becoming more vulnerable to cyber-attacks, their protection becomes a significant issue for Countries [3]. Over the past few years, the European Union (EU) has proposed a wide range of measures to enhance the protection of its citizens and businesses against cyber-attacks and to equip Europe with the tools necessary to deal with ever-changing cyber threats. In addition to the Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) of July 2016, the European Commission adopted a cybersecurity package in September 2017 with proposals to further strengthen EU's resilience and response to cyber-attacks, along with the Cybersecurity Blueprint to respond effectively to large scale cybersecurity incidents [4]. These initiatives were recently strengthened by the Cybersecurity Act, which has reformed the European Union Agency for Cybersecurity (ENISA) and enshrined in law EU cybersecurity certification frameworks; the NIS Toolkit to implement the NIS Directive; and the proposed European Cybersecurity Industrial, Technology and Research and Competence Centre to build and promote stronger cyber awareness and hygiene, skills base, and research and innovation actions [5].

Following these directives and measures, each member state has taken further actions for enhancing cyber security which range from policies and laws to specific security measures. In this article we present the progress and the steps that Greece has followed starting from the establishment of the National Cyber Security Authority of Greece till achieving to be ranked first among 160 countries in the prestigious NCSI index.

It is important to mention here the role of the European Union Agency for Cybersecurity (ENISA). ENISA has a common vision of achieving a high common level of cybersecurity across Europe. It is the EU Agency for network and Information System Security (ISS) and a designated network and information systems professional hub for Member States, the private sector and the people of EU [6].

II. NIS Directive : The Greek Posture

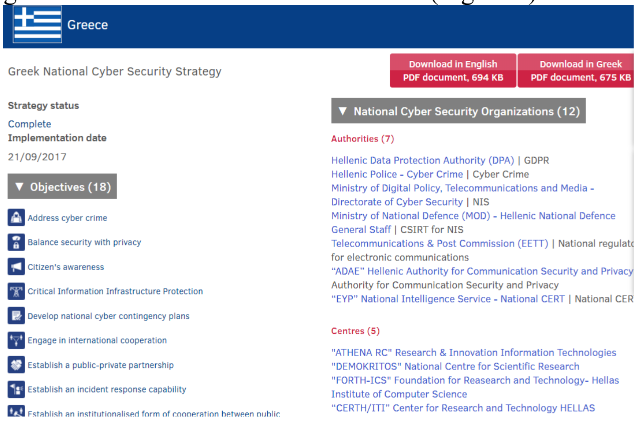
As the EU continues to implement the 2017 Cybersecurity Package, it gets ready for the new EU Security Union Strategy adopted on 24 July 2020 for the period 2020 to 2025 and prepares for the review of the NIS Directive (NISD). In the context of the review of the NIS Directive, a public consultation has been announced, and responses are expected until October 2020.

The NISD offers the theoretical framework for necessary measures to be put in place by local stakeholders [7], considering the fact that integration at corporate and legislative level would be accomplished by its proper transposition into national laws. The European Commission has also issued a Communication in September 2017 to support Member States in the consistent application of the NISD throughout the EU. The NISD offers essential criteria on establishing operators of essential services (OES) and describing Digital Service Providers (DSP) and emerging technology service goods and terminology for maintaining a mutual understanding between Member States and EU stakeholders, for the purposes of developing a cohesive Europe-wide strategy [8].

Having to cope with the obligations of the NIS directive and to meet strict deadlines, Greece has taken some steps forward and with the Presidential Degree of 82/2017 a National Cyber Security Authority (NCSA) was established, along with a Single Point of Contact, both of which currently operate at the Ministry of Digital Governance [9]. This first step was very important because the newly established NCSA was given the overall coordinator role for the cybersecurity policy in Greece. NCSA was responsible for coordinating the public sector and the operators of essential services of Greece, in order to take all necessary steps towards a secure Greek Cyberspace. Its main objective is to shield the Nation from external threats and to provide a secure digital environment for all Greek citizens.

III. Greek National Cybersecurity Strategy

Shortly after the Presidential Decree, in March 2018, Greece issued the National Cyber Security Strategy. The establishment of the National Cyber Security Strategy determined the main principles for the creation of a safe online environment in Greece and set the strategic objectives and the action framework through which these could be achieved [10]. The Greek National Cybersecurity Strategy was created in order to bridge the organizational and coordinative gap among relevant stakeholders and to give the coordination role to the NCSA (Figure 1).



Greece

Greek National Cyber Security Strategy

Download in English PDF document, 694 KB | Download in Greek PDF document, 675 KB

Strategy status
Complete
Implementation date
21/09/2017

▼ Objectives (18)

- Address cyber crime
- Balance security with privacy
- Citizen's awareness
- Critical Information Infrastructure Protection
- Develop national cyber contingency plans
- Engage in international cooperation
- Establish a public-private partnership
- Establish an incident response capability
- Establish an institutionalised form of cooperation between public

▼ National Cyber Security Organizations (12)

Authorities (7)

Hellenic Data Protection Authority (DPA) | GDPR
Hellenic Police - Cyber Crime | Cyber Crime
Ministry of Digital Policy, Telecommunications and Media - Directorate of Cyber Security | NIS
Ministry of National Defence (MOD) - Hellenic National Defence General Staff | CSIRT for NIS
Telecommunications & Post Commission (EETT) | National regulatc for electronic communications
"ADAE" Hellenic Authority for Communication Security and Privacy Authority for Communication Security and Privacy
"EYP" National Intelligence Service - National CERT | National CER

Centres (5)

"ATHENA RC" Research & Innovation Information Technologies
"DEMOKRITOS" National Centre for Scientific Research
"FORTH-ICS" Foundation for Reasearch and Technology- Hellas Institute of Computer Science
"CERTH/ITI" Center for Research and Technology HELLAS

Fig. 1. Greek National Cybersecurity Strategy as it appears on ENISA interactive map website

The main objectives of the Greek strategy were:

- Define stakeholders
- Define Critical Infrastructures
- National Risk Assessment
- National Cyberspace Contingency Plan
- Determine basic security requirements
- Cyber security incident handling
- National preparedness exercises
- User-citizen awareness
- Reliable information exchange mechanisms
- Record and improve the existing institutional framework
- Support of research and development programmes and academic educational programmes
- Cooperation at international level
- Evaluation and revision of the National Strategy

Most of these objectives were put forward immediately from the NCSA with the cooperation of the stakeholders. Using the strategy as guide, NCSA issued the Greek National Law 4577/2018 that transposed the NISD into the Greek legal framework, determined the main threats and vulnerabilities of the public sector through structured questionnaires, identified the operators of essential services (National Critical Infrastructures), defined a minimum set of security requirements, and developed a novel cybersecurity assessment model among others. All these actions that were accompanied by the initial development of an incident notification platform with the cooperation of the competent CSIRT for OESs, helped build the cybersecurity framework that later gave Greece the 1st place in the NCSI index [11].

IV. Identification of Threats and Risks in the Public Sector

To map the national cybersecurity posture, NCSA has decided to follow a Plan-Do-Check-Act (PDCA) approach with strong cooperation of all relevant stakeholders for securing service providers of NCIs. In order to achieve a high level of security, a blend of processes, technologies and properly trained people is needed. Moreover, the competent authorities of each member state (National Cyber Security Authorities, DPAs, CSIRTs, etc.) must have a general overview of the current situation in terms of hardware, software and security procedures that public sector and service providers of NCIs are using. To achieve this, a creation of an IT inventory along with a security inventory of all service providers of NCIs that reside inside Greece, along with all critical operational centers of the public sector and governmental clouds was needed. For that reason an initial questionnaire was sent to relevant stakeholders, aiming in capturing the level of security of central ICT infrastructures of the public sector [12].

In order to achieve its objectives, the questionnaire was designed in order to:

1. Build an initial network of security officers
2. Identify major threats especially for central infrastructures
3. Record and analyze capacity building priorities
4. Record procedures, security measures and policies in place
5. Determine any existing incident response plans
6. Capture training and education plans

By analysing the information collected from the questionnaire, NCSA managed to meet all of the aforementioned objectives. Therefore, NCSA decided to introduce a horizontal security policy along with a set of baseline security requirements for OESs and DSPs with a Ministerial Decree (MD 1027/2019). Moreover, based on these findings, NCSA decided to develop a novel

Cybersecurity Maturity Assessment Model, containing different levels of maturity against each of the different security requirements [13].

According to a study in the health sector in the UK, it was found that 92,5% of security incidents reported have their origin in human errors [14]. In consistency with these findings a further analysis of the questionnaire's results revealed strong relationship of security posture and education and awareness activities. First, education activities, even if they are not carried out in a systematic way, help organisations understand their cyber security needs in terms of establishing necessary incident reporting and incident handling mechanisms. Secondly, organisations that do not yet understand the importance of cyber security do not educate their personnel properly and do not establish procedures that might help them manage and recover after a cyber security incident [15]. Based on these findings NCSA successfully hosted or co-organized a series of awareness events with ENISA, OWASP, OSCE and other cybersecurity related organisations in order to raise awareness among Greek citizens.

V. Identification of the Operators of Essential Services

As stated in the NISD, the OESs or DSPs which meet relevant assigned thresholds of their sector, or are appointed by competent authorities, are required to comply with the requirements of the NISD. Among these requirements is the incident notification and monitoring by the OES or DSP, of each sector (i.e. energy, transport, banking, etc.) and the proper dissemination to competent authorities. A structured approach for engaging with designated operators is required for effective monitoring, and competent authorities should consider developing a compliance mechanism to track the implementation of these requirements.

The Greek NCSA specified the methodology for identifying OESs for each sector. This methodology was issued with the Ministerial Decree 1027/2019. According to it, an institution in order to meet the criteria and to be characterized as an OES, must belong to a sector or sub-sector as determined in national law 4577/2018, offer an essential service (according to a predefined list) that is based on digital systems and meet at least one of the proposed thresholds per service. The National Cyber Security Authority, according to these criteria, has compiled the registry of OESs, which can be updated every two years. Moreover, the Ministerial Decree stated that any Organization that meets the criteria, can apply for inclusion in the registry of OESs.

VI. A Novel Maturity Assessment Framework

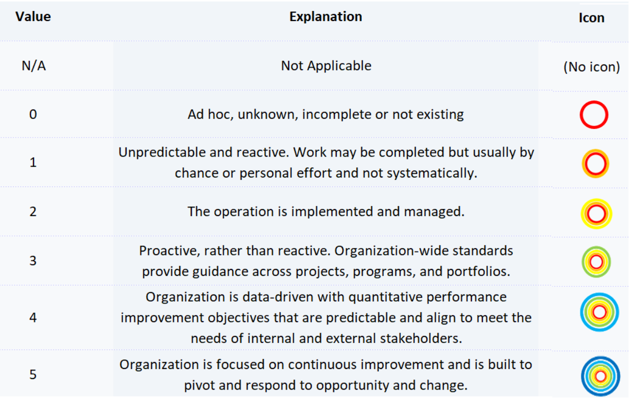
The minimum security requirements that OESs and DSPs have to comply with, were also specified with the Ministerial Decree 1027/2019. These security requirements cover several areas from Risk Management, to Physical and Environmental Controls and form a high-level general guide that can help organizations formulate their cybersecurity policies and controls.

As there was a need to elaborate and enrich the security guidelines to formulate a maturity assessment framework for all organizations, NCSA proceeded to develop such a framework that is also compliant with the NISD [13]. Through this process, which includes a set of methods and semi-automated tools for the collection, processing and evaluation of relevant data, NCSA would be able to draw comparable results on the security posture of assessed organizations and categorize them according to a 6-level model in order to create a classification matrix (Figure 2). The proposed framework consists of 20 distinct security requirements and six maturity levels. It can be used both as a self-assessment as well as an audit tool, thus facilitating companies to perform regular gap analyses and evaluate their security posture.

The objectives of the maturity assessment framework can be summarized as follows:

1. Standardization of the collected feedback
2. Assignment of a specific level of security, based on the implemented controls per category
3. Analysis of the outputs and extraction of relevant statistical information regarding the level achieved per industry, category, and service
4. Implementation of comparisons between subsequent assessments, in order to monitor progress
5. Extraction of possible correlations or contrasts between the information security postures among stakeholders
6. Conduction of further analysis and identification of best practices

This framework can be used as basis to develop a semi-automated software tool to check against all relevant cybersecurity requirements applicable to different sectors (e.g., energy, aviation, healthcare, public administrations, etc.). It can also help organizations conduct efficient gap analysis in terms of compliance with specific regulations and in terms of inadequate security controls and procedures. Moreover, this framework can help any member state prioritise mitigation plans, related to cybersecurity, that need to be implemented through funding of specific actions and launching of new security tools.



Value	Explanation	Icon
N/A	Not Applicable	(No icon)
0	Ad hoc, unknown, incomplete or not existing	○
1	Unpredictable and reactive. Work may be completed but usually by chance or personal effort and not systematically.	◎
2	The operation is implemented and managed.	◎
3	Proactive, rather than reactive. Organization-wide standards provide guidance across projects, programs, and portfolios.	◎
4	Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.	◎
5	Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change.	◎

Fig. 2. The maturity levels of the proposed NIS compliance maturity model.

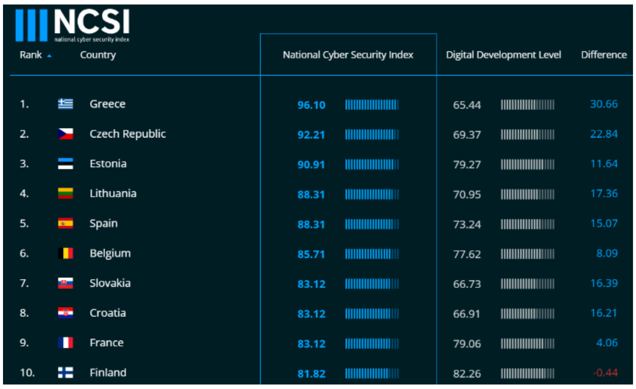
The developed framework was applied in three different OESs in order to test its efficiency, usability and also the level of adoption by security officers. Other similar studies that propose light, web-based models that incorporate all security and privacy regulations and best practices for several organizations were also recently introduced [16], and this is probably where the trends will be heading in the near future.

VII. The NCSI Index

The NCSI index measures the preparedness of countries to prevent cyber threats and manage cyber incidents and is a measure of the maturity of a nation in terms of cybersecurity posture. The NCSI focuses on measurable aspects of cyber security implemented by the central government of each country in four main pillars [17]:

1. Legislation in force: legal acts, regulations, decrees, etc.
2. Established units: existing authorities, organisations, departments, etc.
3. Cooperation formats: committees, working groups, etc.
4. Outcomes: policies, exercises, technologies, websites, programmes, etc.

Greece by following a structured development plan, managed to climb several places and reach the 1st place among 160 countries. This index measures the actions taken by all relevant authorities in Greece, including the Cyber Defense Unit, the Cybercrime Unit, the National CERT, the Hellenic Authority for Communication Security and the Hellenic Data Protection Authority, among others.



NCSI
national cyber security index

Rank	Country	National Cyber Security Index	Digital Development Level	Difference
1.	Greece	96.10	65.44	30.66
2.	Czech Republic	92.21	69.37	22.84
3.	Estonia	90.91	79.27	11.64
4.	Lithuania	88.31	70.95	17.36
5.	Spain	88.31	73.24	15.07
6.	Belgium	85.71	77.62	8.09
7.	Slovakia	83.12	66.73	16.39
8.	Croatia	83.12	66.91	16.21
9.	France	83.12	79.06	4.06
10.	Finland	81.82	82.26	-0.44

Fig. 3. Greek ranking in the NCSI index

As shown in Figure 3, in the 4th quarter of 2019 Greece managed to reach the 1st place. This was mainly boosted by the Ministerial Decree 1027/2019 that included incident response procedures, the list of OESs in Greece and relevant minimum security requirements.

VIII. Discussion

The Greek NCSA in cooperation with all relevant stakeholders inside Greece and worldwide managed to climb 31 places and rank 1st in the NCSI index (Figure 4). Except from the legal initiatives, NCSA has also participated in several educational, awareness and research activities. Being one of the first National Authorities that participated in the consortium of CONCORDIA, one of the four pilots (the other three are ECHO, SPARTA and CyberSec4Europe) which are chosen to address the Horizon 2020 Cybersecurity call "Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap". The purpose of the European Cybersecurity Competence Network is to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market. These four pilots are also the basis for strengthening and sustaining Europe's cybersecurity competence, placing Europe in a leading position in the cybersecurity marketplace worldwide. NCSA of Greece participates in the policy making and dissemination work packages, and the participation in this consortium further improves its cooperation and awareness capabilities.

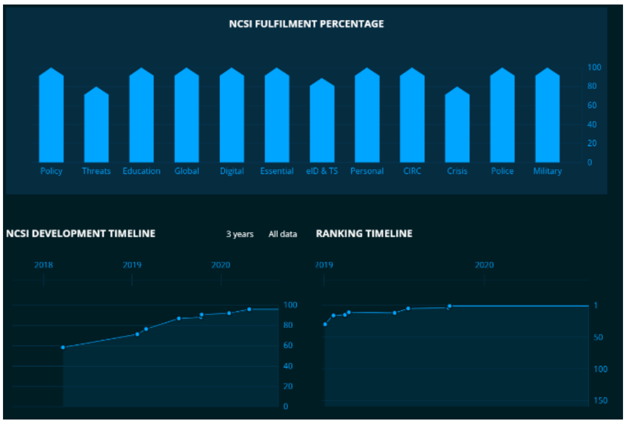


Fig. 4. Greek position per sector and over time

Since its establishment, the Greek NCSA has issued several laws and regulations that helped formulate the Greek cybersecurity framework. This effort can be used as best practice for other states and can be a good basis for advancing to the difficult next steps of implementation and enforcement.

One of the produced outcomes, the maturity assessment framework, can help organizations achieve progressive improvements in their cybersecurity maturity by first achieving stability at the current level, then continuing to a more advanced-level in an organization-wide, continuous process improvement, using both quantitative and qualitative data to make decisions. For instance, at maturity level 2, the organization has been elevated from an "ad hoc" to a "managed" level, by establishing sound security controls, procedures, and processes. Moreover, the developed framework can be used at a European level in order to prioritise mitigation plans and funding related to cybersecurity. When a full security review or assessment cannot be implemented, undertaking efficient cyber security risk assessments and implementing mitigations in large, established critical infrastructures could also be a tentative solution [18].

Finally, by following the recently issued GDPR regulation and the NIS directive that aim at protecting organisations against cyberattacks we can observe an overlap in several aspects [19]. Adoption from the organisations is often a challenging task as CISOs and DPOs face difficulties to understand their roles and design consistent cybersecurity frameworks inside their organisations, due to the regulations' requirements overlapping. To address this issue a mapping of GDPR and NISD requirements is needed [8]. In that way organisations will be able to adopt properly these regulations and help them to identify current potential security issues and structure new security plans.

IX. CONCLUSIONS

In this article we present and analyze the steps that Greece has taken in order to establish a cybersecurity framework at a national level. The focus of the article is on the newly established National Cyber Security Authority and the actions taken in collaboration with other National stakeholders and international institutions (ENISA, NIS cooperation group, etc.) that led Greece to reach the first place in the NCSI index that assesses the preparedness of a Nation to prevent cyber threats and manage cyber incidents.

While Europe continues to issue new regulations and directives regarding electronic communications, data protection, security certification of products and others that follow, proper mapping and coordination of the imposed requirements and procedures, at a technical and organizational level, must be conducted. Except from policies, cybersecurity strategies and specific procedures and incident notification processes that can help manage a cybersecurity incident and prepare for cyber threats, specific security measures must be deployed [20]. In order to prevent and reduce additional fragmentation at national and regional level both member states and the European Union must take appropriate actions.

X. Acknowledgements

We thankfully acknowledge the support of the CONCORDIA H2020 (GA no. 830927) EU project

XI. References

[1] T. Limba, T. Plėta, K. Agafonov and M. Damkus, "Cyber security management model for critical infrastructure," *Entrepreneurship and Sustainability Issues*, vol. 4, p. 559-573, 2017.

[2] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee and H. Janicke, "Cyber security: From regulations and policies to practice," in *Strategic innovative marketing and tourism*, Springer, Cham, 2019, pp. 763-770.

[3] I. Onyeji, M. Bazilian and C. Bronk, "Cyber security and critical energy infrastructure," *The Electricity Journal,* vol. 27, no. 2, pp. 52-60, 2014.

[4] A. Barrinha and H. Farrand-Carrapico, *How coherent is EU cybersecurity policy?,* LSE European Politics and Policy (EUROPP) Blog, 2018.

[5] T. Tagarev and Y. Yanakiev, "Business Models of Collaborative Networked Organisations: Implications for Cybersecurity Collaboration," in *IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2020.

[6] L. Brun, The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity, Université catholique de Louvain, 2018.

[7] T. Wallis and C. Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020.

[8] N. Saqib, V. Germanos, W. Zeng and L. Maglaras, "Mapping of the Security Requirements of GDPR and NIS," SESA, EAI Transactions, DOI: 10.4108/eai.30-6-2020.166283.

[9] L. Maglaras, L. Drivas, K. Noou and S. Rallis, "NIS directive: The case of Greece," *EAI Transactions on Security and Safety,* 2018.

[10]R. o. Greece, "Approval of the National Cybersecurity Strategy of Greece," in *Diavgeia Governmental Platform, ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω*, Athens, 2018.

[11]K. Farahbod, C. Shayo and J. Varzandeh, "Cybersecurity indices and cybercrime annual loss and economic impacts," *Journal of Business and Behavioral Sciences,* vol. 63, 2020.

[12]G. Drivas, L. Maglaras, H. Janicke and S. Ioannidis, "Cybersecurity assessment of the public sector in Greece," in *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, 2019.

[13]G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook and H. Janicke, "A NIS Directive compliant Cybersecurity Maturity Assessment Framework. arXiv preprint arXiv:2004.10411," in *IEEE Computer Society Signature Conference on Computers, Software and Applications*, 2020.

[14]M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke and L. A. Maglaras, "Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form," *IEEE Access,* vol. 7, pp. 102087-102101, 2019.

[15]G. Drivas, L. Maglaras, H. Janicke and S. Ioannidis, "Assessing Cyber Security Threats and Risks in the Public Sector of Greece," *Journal of Information Warfare,* vol. 19, no. 1, 2020.

[16]A. Aliyu, L. Maglaras, H. Y. I. Yevseyeva, E. Boiten, A. Cook and H. Janicke, " A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom," *Applied Sciences,* vol. 10, no. 10, p. 3660, 2020.

[17]R. Rick, *National Cyber Security Index 2018,* Talinn: e-Governance academy, 2018.

[18]A. Cook, H. Janicke, R. Smith and L. Maglaras, "The industrial control system cyber defence triage process," *Computers & Security,* vol. 70, pp. 467-481, 2017.

[19]L. Kalman, "New European data privacy and cyber security laws: One year later," *Communications of the ACM,* vol. 62, no. 4, 2019.

[20]Maglaras, L. A., & Jiang, J. (2014). A real time OCSVM intrusion detection module with low overhead for SCADA systems. International Journal of Advanced Research in Artificial Intelligence (IJARAI), 3(10).