Opportunities for Cybersecurity Research in the New European Context

Adrian Victor VEVERA, Alexandru GEORGESCU, Carmen Elena CÎRNU
National Institute for Research and Development in Informatics – ICI Bucharest
victor.vevera@ici.ro, alexandru.georgescu@ici.ro, carmen.cîrnu@ici.ro

Abstract: Cybersecurity has become a priority in a rapidly shifting and complex security environment beset by hybrid threats. It has also become an important avenue for national development and for economic competition. Therefore, research in the field has become a priority. Key evolutions at the level of the European Union generate unique opportunities for Romania to increase its stature in the field, especially in the security aspects of the new digital technologies such as AI, quantum computing and more. This is a mix of funding priorities and institutional developments which the article presents in order to craft a Romanian approach to maximizing returns from these developments.
Keywords: Cybersecurity, Cyber research, European ecosystem, National development, Hybrid threats

INTRODUCTION

The present article highlights the opportunity for Romania inherent in the momentous changes in institutions and funding taking place at EU levels with regards to cybersecurity, but especially cybersecurity research, as well as related technological domains that are, nevertheless, beyond the scope of the paper. The article is composed of three main sections – a presentation of the cybersecurity research ecosystem being developed in the EU for the past decade, as understood by the authors, a non-exhaustive presentation of the funding opportunities for cybersecurity research in the new multiannual framework and other programmes, and a series of recommendations for how Romania may act to profit from these changes, in the context of national weaknesses in funding for research.

The European Union has developed an important and evolving ecosystem of institutions and organizations with impact in cybersecurity and related technologies in three related facets – operational security, research and development and policy formulation and implementation (ECA, 2019).

The list of entities is extensive because in cybersecurity, unlike other fields, there is often no clear demarcation between research and development activities and operational activities. Operational cybersecurity organizations engage in permanent research activity to identify the latest cyber threat and to update defenses in order to shield beneficiaries. Investigations into the capabilities of new threats, including their origin and their probable purpose, are also handled by groups responsible for operational security, in the same organizations, if not the same departments.

Therefore, our vision of the European ecosystem for cybersecurity research includes a host of non-research, operational or sectoral institutions that nevertheless have an important role in facilitating and coordinating cybersecurity research, if only for their own security needs.

At the same time, cyber is a cross-cutting issues that is permeating across all sectors, where it is becoming integrated as a key medium for command, control, coordination, data gathering and processing in the functioning of all infrastructures. For this reason, even sectoral research or governance organizations in the EU must develop a cyber component, which itself will require specialized cybersecurity products, services, policies and perspectives, which are the object of a cybersecurity R&D process.

Figure 1 presents the view resulting from the research, though it cannot be said to be complete or in sufficient detail, given the profusion of programmes, associations and other components of this vibrant and developing ecosystem.

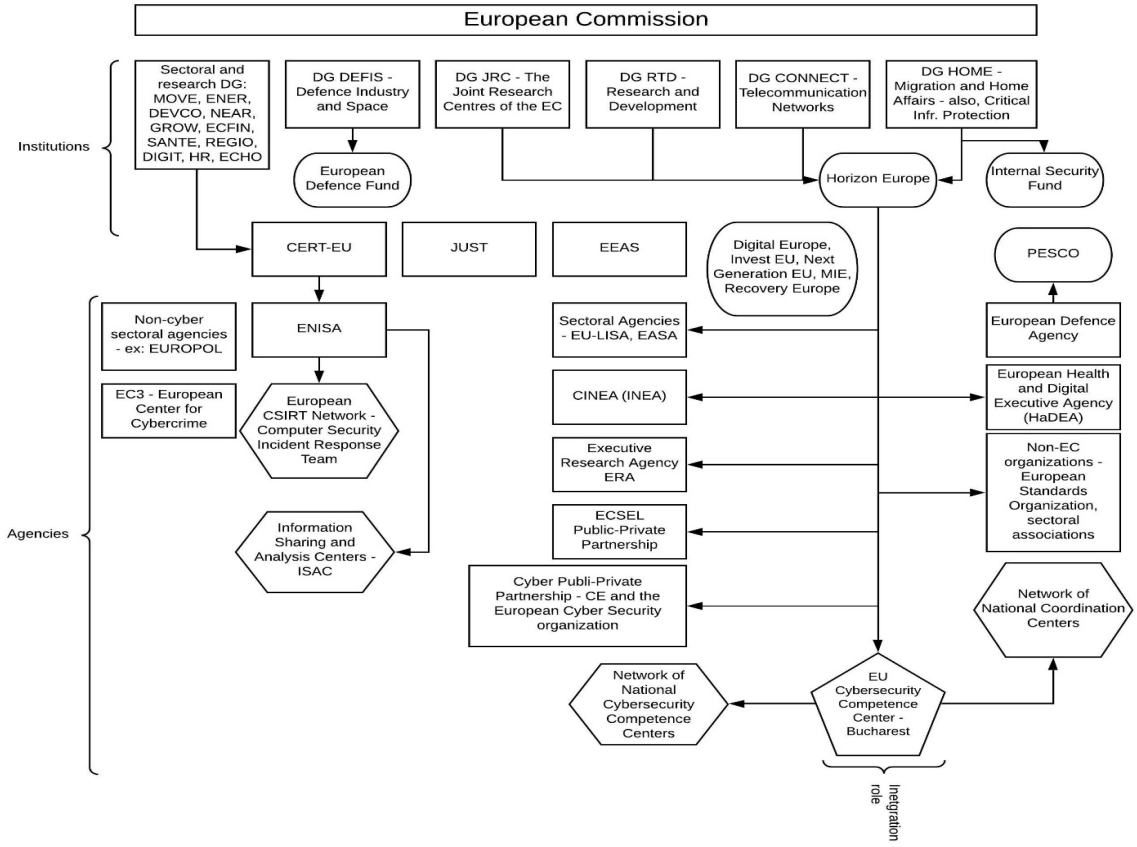

Fig. 1: *Chart of ecosystem for cybersecurity research and auxiliary capability in the EU (source: authors)*

This ecosystem is very fragmented, as a result of organic growth, changes in visions and priorities and the politics of the EU. At the same time, it is necessary because the EU itself and its governing institutions are increasingly vulnerable to a complex and challenging cybersecurity environment, while they, along with Europe itself, the Member States governing apparatus, its society and economy, are undergoing rapid digitalization and an anticipated implementation of new digital technologies (ECA, 2019).

The conclusion is that cybersecurity and related technologies' research in the EU will require trans-sector and multi-sector approaches by a series of European actors with specific sectoral competencies, alongside "pure" cyber oriented organizations and in a coordinated manner.

Some of the actors that can be found in figure 1 include also EU organizations with clearly delineated operational roles that can, nevertheless, serve a vital role in cybersecurity research. From our perspective, the main institutions which a Romanian approach to the new European context for Research, Development and Innovation in cybersecurity and related technology fields will have to encompass can be found in Table 1.

Table 1: *Main entities for the EU cybersecurity research ecosystem (source: authors)*

Main entities of EU cybersecurity research ecosystem		
Directorates	Decentralized agencies	Other entities and institutions
• DG Research and Innovation (DG-RTD) • DG Joint Research Centre (DG-JRC) • DG Communications Networks, Content and Technology (DG-CONNECT) • DG Defence Industry and Space (DG-DEFIS)	• European Union Agency for Cybersecurity (ENISA) • European Defence Agency • Executive Research Agency • Computer Emergency Response Team (CERT-EU) • EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA)	• European Cybersecurity Competence Network • Innovation and Networks Executive Agency (INEA), transformed on April 1st, 2021, into European Climate, Infrastructure and Environment Executive Agency (CINEA) • European Health and Digital Executive Agency (HaDEA) • European Cyber Security Organisation (industry organization in partnership with the EC)

There are several novelties in the EU cyber ecosystem overall. The most important is the European Cybersecurity Competence Centre announced recently for creation in Bucharest, whose role will be to coordinate EU investment into cyber across the ecosystem (European Council, 2020). It will also deal with connected fields, such as AI, hypercomputing, quantum computing and so on, with important security applications.

In addition to this institute, there will also be a trend to form National Coordination Centers on cyber in every EU Member State and also Communities for Cybersecurity Competencies. These two entity types will be networked at European level and with the European Cybersecurity Competence Centre in Bucharest, as planned in COM (2018) 630 and was reiterated in the new Strategy for the Security Union (COM(2020) 605). Another important development is the creation of the new Directorate-General for Defence Industry and Space (DG-DEFIS), especially since the advanced militaries consider cyber to be a new domain of operations and cyber warfare and resilience

to hybrid threats combining also cyber-attacks are a priority. Lastly, as can be seen from Table 1, there are examples of reorganizations of EU bodies to better adapt them to current demands and functions, based on stated EU priorities, including digitalization and climate change.

FUNDING OPPORTUNITIES

The European Union is doubling down on cybersecurity, cyber infrastructure and new digital-related technologies as part of a strategy for long-term growth and resilience. This is evident also from the funding made available for research into these fields and the comprehensive approach to ensure that cybersecurity and digitalization in all of their aspects are covered. At the same time, new funding mechanisms are also being developed, which try to make public-private partnerships into a reality and to avoid the pitfalls of adverse incentives in project selection that public entity driven research is predisposed to. The hope is that these investments into research are not only comprehensive and resilience-enhancing, in the context of the inevitable digitalization taking place, but also a source of growth in a world in which cybersecurity is also an important economic sector.

The following are the main funding opportunities for cybersecurity research and related technologies, such as AI, quantum technology and so on. A couple of things must be kept in mind – the complicated nature of European institutionalized funding, as highlighted in the previous section, means that there is a significant overlap between funding initiatives and programmes which are presented separately herein, because the funding entity and the disbursement and tracking entity are not always the same ones. An example of this is the Next Generation EU Programme providing funding that will be disbursed and tracked through Horizon Europe. Nor is there yet an accurate and complete delineation of funding across sectors, meaning that there are programmes where cyber infrastructure, security and education may fall under the same heading, in an undifferentiated form. These are the main headings for funding, as highlighted from official EU websites, press releases and documents:

1. Digital Europe – out of a total budget of 9.2 billion euros for the period of 2021-2027, around 2.3 billion euros are earmarked for cybersecurity; 2.1 billion are said to be allocated for Artificial Intelligence research and 2.2 billion euros for supercomputing, an area where the EU has been trailing behind the US and China;
2. Connecting Europe Facility – digital pillar: 1.7 billion euros for 2021-2027;
3. Horizon Europe, the replacement for Horizon 2020, has two main avenues relevant for cybersecurity – Civil Security for Society, in partnership with Digital Europe, features 1.9 billion euros earmarked for 2021-2027 for cyber protection, cyber infrastructure investment and support for the EU cybersecurity industry. Pillar 2, Theme 4 (Digital, Industry and Space) has 5.5 billion euros allocated through financing from the European Health and Digital Executive Agency (HaDEA);
4. InvestEU lists cybersecurity and AI as priorities. It is an innovative programme run through a combination of European, national and private funding, where estimated levels of expenditures were made through targets in multiplication coefficients for public investment. For 2021-2027, InvestEU is targeting 650 billion euros in total expenditures, consisting of 15.2 billion euros from the European Commission, 38 billion euros from the Member States (11 billion of which are guaranteed for cybersecurity research), 9.5 billion euros from various partners. The rest of the funding is estimated to come from the private sector based on a funding multiplier coefficient of 13.8. There are multiple priorities, so it is uncertain to what extent cybersecurity will receive funding and attention (European Commission, 2019a);
5. Recovery Europe Plan – its total funding is 1.8 trillion euros for 2021-2027, based on

three pillars, two of which, digitalization and resilience enhancement, are related to cybersecurity and connected areas. There is no concrete breakdown of spending by sector, however we may note that three of the main chapters of the plan are directly related to this article's field of interest – "Single market, innovation and digital" (132.8 billion euros), "Cohesion, resilience and values" (377.8 billion euros), "Security and defence" (13.2 billion euros). These sums come from the multiannual financing framework of the EU and will be supplemented by Next Generation EU additional funding;

6. Next Generation EU – this Fund has been financed from the European Commission's own resources and from long term loans contracted by it. The following relevant components may be mentioned:

- The Recovery and Resilience Facility, with 560 billion euros for digitalization, resilience and the green transition;
- InvestEU, with 15.3 billion euros;
- The Strategic Investment Facility, worth 150 billion euros and targeting strategic sector resilience including the digital sector and supply and production chains, which are also important for cybersecurity and related technologies. Applicable European documents list the following priorities for the Next Generation EU funds: "connectivity and infrastructure in the digital domain", "industrial development in strategic sectors such as cybersecurity, AI, quantum computing, cloud computing, supercomputing", "cyber resilience", "building a real data-based economy";

7. The Internal Security Fund has doubled its allocation for security compared to the previous multiannual exercise. The Fund itself has grown from 3.44 billion euros to 4.8 billion, but allocations for security have gone from 1.18 billion to 2.5 billion (European Commission, 2019b). Multiple security domains are targeted, of which cybersecurity is one. These funds are separate from those of other decentralized agencies such as the European Defence Agency;

8. The European Defence Fund has 13 billion euros allocated for 2021-2027, of which European financing is 4.2 billion and the rest is Member State co-financing. One component of the spending plan is the European Programme for Defence and Industry Development, with 500 million euros and a remit that encompasses also cybersecurity products, though military oriented (European Commission, 2019c). These programmes are particularly important, and designated as such in documents of reference, because of the emphasis place by the European Commission on resilience to hybrid risks, vulnerabilities and threats, to cyber-attacks, electromagnetic spectrum warfare, the development specialized software and the harmonization of solutions at Member State level through common coordinated acquisitions in a multiyear framework;

9. The Mechanism for Interconnecting Europe (MIE) has 3 billion euros allocated for digitalization, out of a total of 42.3 billion euros in 2021-2027. The Fund is focused on network, wireless connectivity (5G), facilities connection, but will automatically acquire an important cybersecurity component both for infrastructure which is resilient by design, but also because it will feature the new digital technologies as they become integrated into infrastructures, systems, products and services.

10. The EU Quantum Technologies Flagship – 1 billion euro funding between 2021-2027;

The focus on co-interesting the private sector and attracting resources into research is very welcome, if the EU is to reduce the financing lag with the United States and become a peer in R&D for the cyber domain and any other priority domain that can be identified.

RECOMMENDATIONS FOR ROMANIA

Firstly, Romania needs to create a political consensus on the need to finance research overall. Without this consensus, it is unlikely that resources will be allocated that enable Romania to take advantage of

the opportunities presented by European developments. According to Eurostat data, Romania spent just 0.8% of GDP on research and development efforts according to European definitions, compared to a European average of 2.19%. This level is insufficient either, since the Europe 2020 strategic document proposed a 3% allocation by the year 2020. Only three European countries (Sweden, Austria and Germany) surpass the 3% level. Romania is in last place and Bulgaria in 21st place, with 0.84% of GDP (Eurostat, 2020). These data can be seen in figure 2, which also highlights the source of funding.

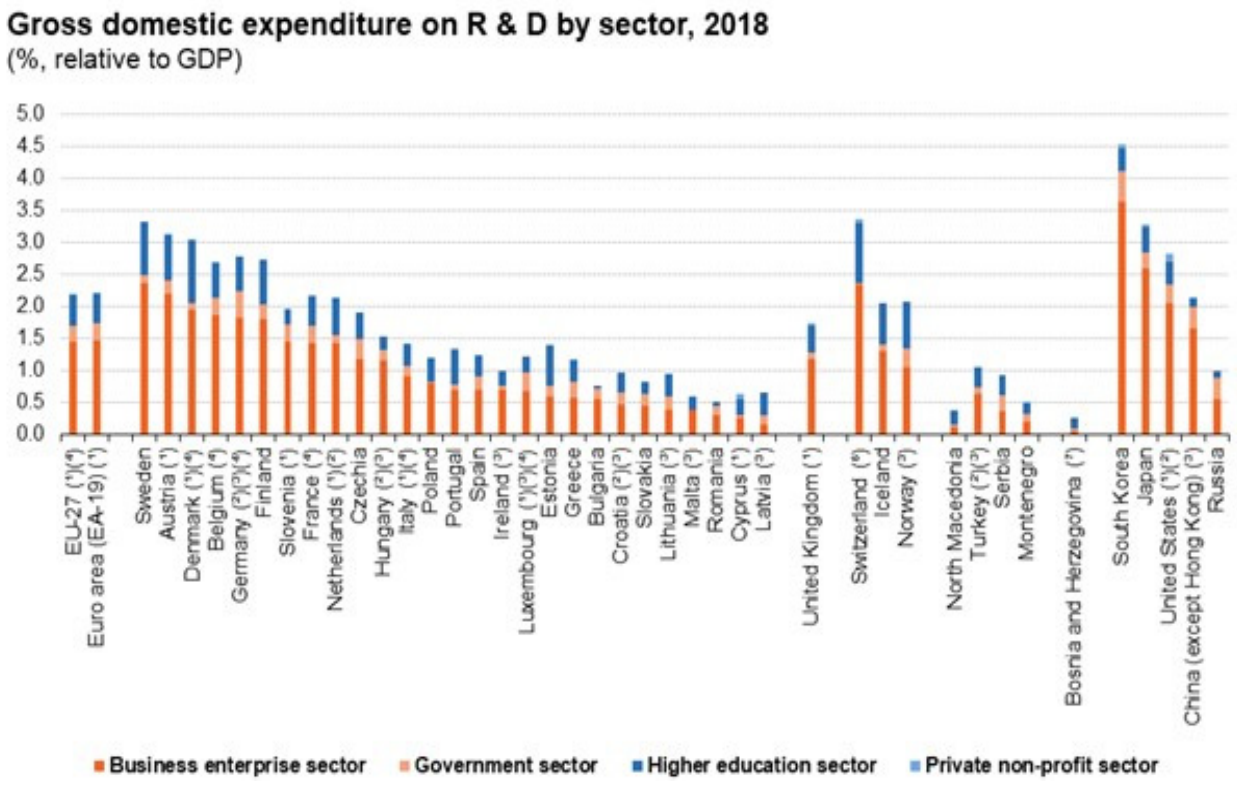

Fig. 2: *Gross domestic expenditure on R&D by sector (source: Eurostat, 2021)*

We do not have a delineation by sector of investment to see where cyber fits in. We can, however, speculate that investment in cyber would be very strong in the private sector as well, especially in the developed countries, which means that Romania, despite its performance in the ITC sector, will lag Europe here as well, because of the reduced contribution of exclusively national firms in the make-up of the ITC industry (exceptions notwithstanding). In general, the more advanced the economy, the more added value it creates, usually through investment in research, development and innovation. In the highest performing European countries from an R&D perspective, government investment in RDI activities is much lower than that of the private and other sectors. The European average is 66% in the private sector, 22% in academia, 11% in the government sector and 1% in the non-profit one. When it comes to government investment in R&D, the European average is 0.25% of GDP (excluding the United Kingdom), while Romania allocates just 0.15% of GDP, nevertheless more than actors like Portugal, Ireland, Cyprus and Latvia and comparable to other actors. Therefore, Romanian research cannot be wholly reformed through political will, but also through a structural transformation of the economy that incentivizes such investment. Figure 3 shows the delineation of research spending by type of sector in European countries.

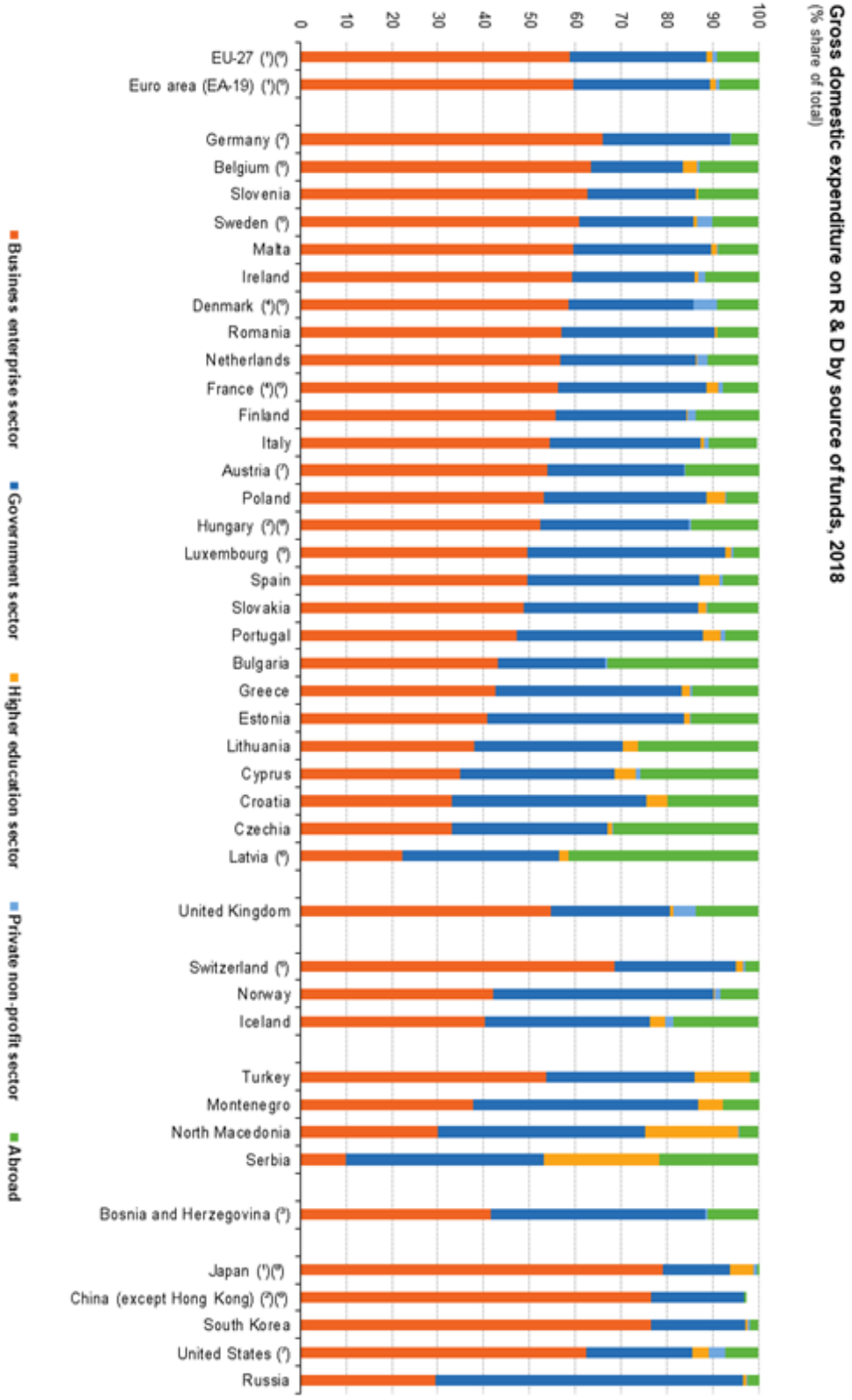

Fig. 3: *R&D expenditure by source of funding (source: Eurostat, 2021)*

In order for Romania to increase its performance in cybersecurity research, it will need to increase the contribution of the private sector to this area and set off a virtuous cycle of development, growth and investment into research that can complement government and European funding. Some of the proposals we may identify include, but are not limited to:

- Encouraging the growth of Romanian entities so they can become more valuable partners in European research consortia;
- Encouraging the formation and retention of trained research personnel;
- Adopting methods for the successful formation of start-ups, including through university-based start-up incubators;
- Developing tools and partnerships for the protection of Romanian intellectual property right holders, especially against IP predator entities (like patent trolls);
- Developing the means for the retention of value added from the cybersecurity industry in Romania (including the conditioning of national research fund receipt on respecting key policies, such as not transferring intellectual property and products to foreign subsidiaries), not transferring personnel, not outsource parts of the project to other foreign subsidiaries;
- Developing specific infrastructure that supports cybersecurity and related fields RDI, including cyber ranges, supercomputing centers, specialty laboratory facilities and so on.

Among the specific proposals that we may cite, we could mention:

- The development of "white hat hacking" companies and collectives, authorized to test security of state and non-state entities in Romania and to report vulnerabilities. Their remuneration could be partially subsidized by the authorities from a subsidy fund for cyber reform for critical entities, including owners/operators of critical infrastructures (state companies, banks etc.);
- The development of a national IP fund that would serve as collective insurance against frivolous property right suits, especially since the cyber field presents difficulties when it comes to the defense of intellectual property and against actors bringing nuisance suites;
- The development of a national mechanism, preferably on a voluntary basis, by which entities affected by cyber-attacks can disclose the incidents and offer valuable data while maintaining anonymity, protecting trade secrets, incentivizing even global companies to cooperate or even waiving liability for certain forms of negligence or insurance invalidation related to the impact of the attack. There is an important literature in the field of these voluntary cooperation mechanisms and examples that area already working such as the Automated Indicator Sharing mechanism of the Cybersecurity and Infrastructure Security Agency within the US Department of Homeland Security. It is an automated, voluntary, incentivized and two-way program (meaning that public authorities also disclose cyber attacks to private entities through it) (DHS, 2021). This development not only increases operational security by revealing cyber-attacks and reducing the amount of time that an attacker spends undetected in networked systems, but it also provides immensely valuable resources for cybersecurity research, development and innovation efforts. What is missing is a culture of trust and cooperation to establish these private-public partnerships;
- Lastly, Romania should consider creating a special liaison unit within the competent ministry to permanently link with the Cybersecurity Competencies Centre in Bucharest and liaise also with the additional bodies that will be created, in order to reduce informational asymmetries regarding opportunities and priorities for funding between the EU and Romanian entities with specialized capabilities.

The private sector is again key for the development of the cybersecurity, not just

in the form of actor, but also of demand to drive development of products and services with higher RDI content. The global market for cybersecurity products and services reached 230 billion by the end of the year 2020, and the Cyber Threat Report CEE report stated that Romania's region has a market dynamic that is much stronger than the rest of Europe (Kosciuszko, 2019). 20% of the European imports of cybersecurity products (2.2 billion euros) took place in the new Member States in 2016, which the authors suggest highlights growth in demand outstripping national supply (Kosciuszko, 2019). The European Commission has estimated that imports to the region will grow by 50% by the end of 2021, reaching 3.3 billion euros yearly (Albrycht et al, 2019). Figure 4 highlights the size of the cybersecurity market in the Three Seas Initiative countries, as drawn from the report Securing the Digital DNA in the Three Seas Initiative region (Albrycht et al, 2019).

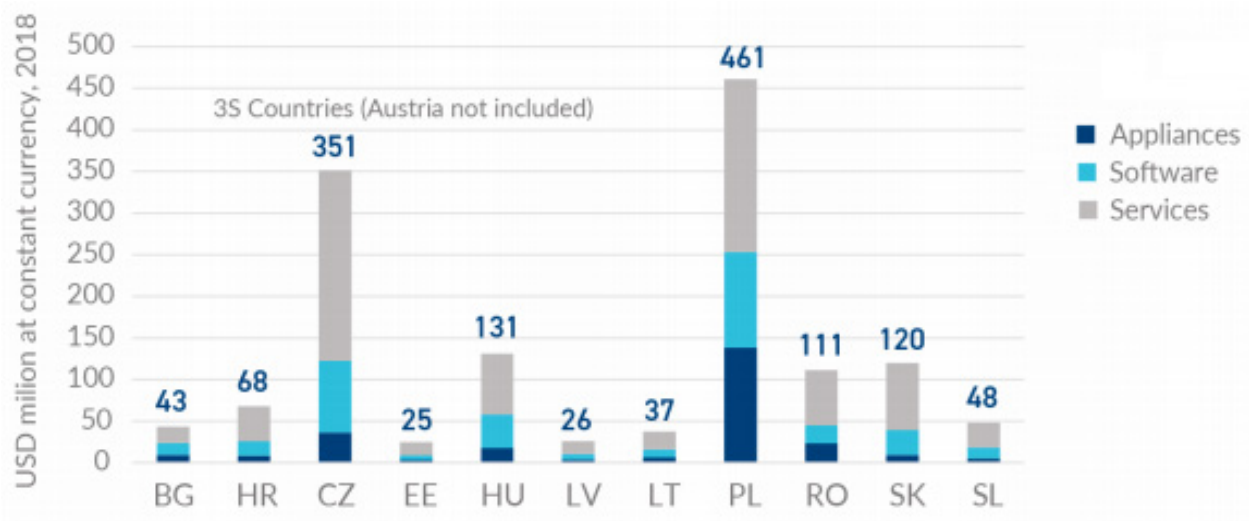

Fig. 4: *Size of cybersecurity products market in 2018 (source: Albrycht et al, 2019)*

There is ample room to grow since the 2019 "Cybersecurity leaders and followers report" stated that only 17.3% of companies in Central and Eastern Europe had formal cybersecurity policies, only 23% of employees had basic digital skills (which tie into cybersecurity culture) and only 11% of companies provided IT training to employees, despite the rapid growth in digitalization (Lepore and Siudak, 2019). Expenditure on cybersecurity products, according to the Cyber Threat Report CEE, are concentrated between 50% and 70% on antispam and antivirus products and represents just 2000 euros per year, per firm on average (Kosciuszko, 2019). Figure 4 also shows Romania lagging in cybersecurity market size compared to its neighbors, suggesting that policies addressing this gap could be very successful in increasing the market size, thereby increasing demand, bolstering competition and stimulating investment into new products and services with a higher RDI content.

CONCLUSIONS

Romania has a significant opportunity to jumpstart its research, development and innovation capabilities in cybersecurity and related fields in the emerging European institutional and financial context. Among these factors, we may mention the selection of Bucharest to host the EU Cybersecurity Competence Centre which will coordinate European research efforts in this and related

fields, while also entering a new financial exercise for which the EU has prioritized funding for digitalization, resilience, infrastructure and industrial competitiveness, all with applicability in the realm of cybersecurity. This article has detailed these factors and also a series of recommendation for how Romania may make the most of these developments. The proposals herein are just the beginning in terms of planning a new approach not just for cybersecurity, but also for the entire security (and defence) industry.

AKNOWLEDGEMENTS

The findings presented in this article are based on a research project, 'The strategy of national participation in the new European context to coordinate research in the security industry and space', undertaken by a consortium led by the Romanian Space Agency. The project was funded through a grant of the Romanian National Authority for Scientific Research, CNDI-UEFISCDI, registration number PN3/P2/876/17.11.2020.

REFERENCE LIST

Challenges to effective EU cybersecurity policy. Briefing Paper, European Court of Auditors, March 2019, as ECA (2019), https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

*** (2019). Cyber Threat Report CEE 2018. Kosciuszko Institute, As Kosciuszko (2019). https://cybermadeinpoland.pl/wp-content/uploads/2020/06/Cyber-Threat-CEE-500-CYBERSEC-HUB-report.pdf

*** (2019). European Defence Fund. European Commission, as European Commission (2019c), https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-eu-defence-fund_en_0.pdf

*** (2019). Internal Security Fund. European Commission, as European Commission (2019b), https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-internal-security-fund_en.pdf

*** (2019). InvestEU Programme. European Commission, as European Commission (2019a), https://ec.europa.eu/commission/sites/beta-political/files/what_is_investeu_mff_032019.pdf

*** (2020). Bucharest-based Cybersecurity Competence Centre gets green light from Council. European Council Press Release, as European Council (2020), https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/

*** (2020). R&D expenditure in the EU at 2.19% of GDP in 2019. Eurostat, as Eurostat (2020). https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20201127-1

*** (2021), Research and development expenditure, by sectors of performance. Eurostat, as Eurostat (2021) https://ec.europa.eu/eurostat/databrowser/view/tsc00001/default/table?lang=en

*** (2021). Automated Indicator Sharing Documentation. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, USA, as DHS (2021). https://www.cisa.gov/publication/automated-indicator-sharing-ais-documentation