Information & Security

V. Kopchev
vol. 42 (2019): 67-81
https://doi.org/10.11610/isij.4204

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

The European Union Moves Ahead on Cybersecurity Research Through Enhanced Cooperation and Coordination

Valeri Kopchev

ABSTRACT:

Due to a dispersed research and industrial capacity and often disconnected national markets, it is challenging for the European Union to compete with world leaders providing cybersecurity products and services and thus to support its ambition to achieve strategic autonomy in the cyber domain. This article explores one of the intended remedies—the proposal for an EU Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Analysing legal, organisational and financial measures, the author posits that the expected regulation, if properly implemented, can fill in an important gap in the current legislative framework of the European Union.

ARTICLE INFO:

RECEIVED: 08 JULY 2019
REVISED: 12 NOV 2019
ONLINE: 03 DEC 2019

KEYWORDS:

cybersecurity, research and technology, competence, resilience, industrial capacity, legal framework, Regulation 630

Introduction

It is universally acknowledged that development and use of digital technologies creates new and unprecedented possibilities. It brings huge benefits to individuals and society as a whole and boosts economy and growth. At the same time, all this comes along with new risks to the end-users and economic actors. The

E-mail: adv.kopchev@gmail.com

risk of falling victim to cybercrime or a cyber-attack is constantly increasing and the societal and economic impact of it continues to raise.

All these risks are related to weaknesses in cybersecurity governance, both in the public and private sectors across the EU as well as at the international level. This impairs the global community's ability to limit cyber-attacks from occurrence, properly respond to them and mitigate their impact. The challenge is thus to strengthen cybersecurity governance at EU level, taking into account the cross-border nature of cybersecurity threats. The protection of many critical sectors and their underpinning infrastructures, such as health, energy, transport, finance, manufacturing and others, have become increasingly dependent on digital technologies. According to a survey [1] conducted by the European Commission in 2017, many EU citizens are concerned about the risk of falling victim to various forms of cybercrime, with the largest proportion of respondents being specifically concerned by becoming a victim of malware infection (69%), identity theft (69%) and bank card/online banking fraud (66%). According to another study,[2] cybercrime constitutes half of all the crimes occurring in EU Member States, and accounts for losses worth billions of euros each year. Therefore, it does not come by surprise that cybersecurity of products and services constitute an important element of ensuring the economic stability and thus developed as important and fast-growing market. There, however, Europe faces strong competition from third countries such as the United States, China, Japan and South Korea. A Commission analysis [3] attributes this to the fact that even though a lot of innovative cybersecurity research is taking place in Europe, its results are rarely commercialised.

According to a report [4] of the Commission's Joint Research Centre (JRC), the EU retains a wealth of expertise in cybersecurity, which is not fully exploited. This expertise, if transformed into marketable products and solutions, could allow the EU to cover the whole cybersecurity value chain. According to the Commission,[5] the cybersecurity industry in Europe developed largely on the basis of national government demand, including for defence purposes. Today, companies still find it difficult to grow beyond the boundaries of their national markets due to the divergent rules that govern them. As a consequence, while these companies tend to be strong and innovative, they are smaller in size in comparison to their American and Asian competitors. In addition to the civilian use of technologies, the fact that cyberspace is considered by military forces as the fifth domain (besides land, sea, air and space) of military activity, equally critical to European Union Common Security and Defence Policy (CSDP) [6] further demonstrates the need of an effort to streamline the EU legislative framework and address the existing fragmentation.

The analysis concludes that without policy intervention to address the fragmentation of European efforts and innovation capacities, the European cybersecurity industry may not be capable of taking advantage of its potential or competing with other global players. Europe also faces a shortage of skilled cybersecurity professionals. According to Commission's [7] estimates, the cybersecurity workforce gap in Europe will reach 350 000 by 2022.

The EU policy-makers recognised that it is also in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services. From strategical point of view, the EU must be in a position to autonomously secure its digital assets and to compete on global cybersecurity market. Furthermore, it is stated that "the understanding is that the EU cannot have operational and political autonomy without industrial autonomy." [8]

The EU public investment today – both at the EU and national level - including in the development and the deployment of cybersecurity technology and solutions - is below the critical mass needed to protect EU economy and institutions, in particular if compared to other key international players. This has practical consequences on cybersecurity capacities of EU research and industrial communities.

As an example, in the USA, the government invested over USD 19 billion for cybersecurity as part of 2017 budget (35% increase from 2016 in overall Federal resources for cybersecurity).[9] It devotes USD 760 Million in 2017 alone for cybersecurity research and innovation.[10]

At the EU level the investment in cybersecurity is channelled through different programmes of the EU budget: about EUR 600 million have been invested in cybersecurity and cybercrime projects under Horizon 2020 for the period 2014-2020 (including EUR 450 million devoted to cybersecurity cPPP for 2017-2020); the European Structural and Investment (ESI) Funds foresee a contribution of up to EUR 400 million for investments in trust and cybersecurity; about EUR 30 million were invested from CEF in the period 2014-2017.

As a consequence of all abovementioned at the moment, the Union is a net importer of cybersecurity products and solutions and largely depends on non-European providers.[11] The cybersecurity market is globally a 600 billion EUR market that is expected to grow in the next five years on average by approximately 17% in terms of sales, number of companies and employment. However, in the top 20 of the leading cybersecurity countries from a market perspective, there are only 6 Member States.[12] What is more, up to 25% of the supply from within Europe is actually provided by companies with the headquarters outside Europe. At the same time major competitors (e.g. US, China) are net exporters in all cybersecurity sub-sectors.[13]

This, together with the cross-border nature of cybersecurity threats and the need to tackle them at EU level has been recognized already in 2013, when the first EU Cybersecurity Strategy [14] was adopted. Cybersecurity, cybercrime and cyber defence have been systematically included in the EU political priorities and key policy and legislative initiatives:

1. Digital Single Market Strategy – COM/2015/0192;
2. The European Agenda on Security – COM (2015) 185;
3. The Joint Framework on countering hybrid threats;
4. The Communication on Launching the European Defence Fund;

5. The Directive on concerning measures for a high common level of security of network and information systems across the Union, (the 'NIS Directive' – (EU) 2016/1148);
6. The contractual public-private partnership (cPPP) on cybersecurity C(2016) 4400 between the EU and the European Cybersecurity Organisation (ECSO);

On 13 September 2017, the Commission adopted a cybersecurity package containing a series of initiatives [15] to further improve EU cyber-resilience, deterrence and defence. In addition to this package it should be also mentioned that in May 2018 the first cybersecurity act – the Directive on Security of Network and Information Systems across the EU (the NIS Directive [16]) entered in force. It provides for legal measures to boost the overall level of cybersecurity in the EU with a focus on protecting critical infrastructure. Among other things, it established the NIS cooperation group,[17] to ensure strategic cooperation among Member States, and the CSIRTS network (computer security incident response teams [18]), to ensure the exchange of information on cybersecurity and cooperation on specific cybersecurity incidents. Currently, a Bulgarian CSIRT centre exists (https://govcert.bg), which assists in reducing the risks of information security incidents, and resolving such incidents if they have already occurred.

The Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [19]

The proposal was presented by the Commission on September 2018. It aims to create a new EU structure to pool and share cybersecurity research capacities and outcomes in a domain where EU capabilities and competences are considerable but still fragmented. The new structure described in the proposal – an EU-level Competence Centre with its Network of national-level competence centres – would apply a comprehensive approach supporting cybersecurity across the entire value chain, from research to the deployment and uptake of key technologies.

The proposal aims at:

- Building cyber resilience, i.e. create and increase the ability to respond to and limit cyberattacks and ensures a coherent EU-wide approach;
- Improving relevant skills and filling the skills gap – raising skills and awareness across all sectors and levels of society is essential, given the growing global cybersecurity skills shortfall. There are currently limited EU-wide standards for training, certification or cyber risk assessments;
- Ability to improve information exchange and coordination between the public and private sectors – current situation is considered as unsatisfactory;

- Ability for rapid detection and response. Cybersecurity is not yet fully integrated into existing EU-level crisis response coordination mechanisms, potentially limiting the EU's capacity to respond to large-scale, cross-border cyber incidents;
- Ability to improve the protection of critical infrastructure and societal functions;
- Control of EU spending – based on the fact that there is no dedicated EU budget to fund the cybersecurity strategy, there is no clarity/visibility of how money is being spent;
- Ability to pool expertise in the relevant area of cybersecurity - industrial, research and public sector (including defence) communities also identified difficulties to find skilled cybersecurity professionals for both research and business tasks. This is coupled with huge global competition for talent. Two-thirds of the European security professionals surveyed for the 2017 Global Information Security Workforce Study [20] said there was too few positions available in their field, a proportion in line with the worldwide figure, which rose from 62 % worldwide in 2015;
- Consistency with existing cybersecurity policy provisions in the policy area as well as other EU policies – to facilitate and accelerate standardization and certification processes, in particular those related to cybersecurity certification schemes in the meaning of the proposed Cybersecurity Act.[21, 22]

The proposal should be considered as big step in the right direction, taking into account the fact that the EU's international competitors already have a clear strategy and make significant cybersecurity investment designed to increase technological and innovation capacities. They are developing competence centres bringing their assets (human, knowledge, financial) together to support their industries in the quest to become global cybersecurity leaders.

Under the provisions of the proposal, the Competence Centre (at EU level) with its Network (the national-level competence centres) is expected to stimulate the European cybersecurity technological and industrial ecosystem to overcome the lack of concerted efforts, actions and expertise, to support cybersecurity across the entire value chain – from research and development to deployment and uptake at large scale of key technologies.

The Competence Centre will "facilitate and help coordinate the work of the Network and nurture the Cybersecurity Competence Community, driving the cybersecurity technological agenda and facilitating access to the expertise so gathered. The Competence Centre will in particular do so by implementing relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements. In view of the considerable investments in cybersecurity made in other parts of the world and of the need to coordinate and pool relevant resources in Europe, the Competence Centre is proposed as a European Partnership,[23] thus facilitating joint investment by the Union, Member States and/or industry. Therefore, the proposal requires Member States to

contribute a commensurate amount to the actions of the Competence Centre and Network.

The principal decision-making body is the Governing Board, in which all Member States take part but only those Member States which participate financially have voting rights. The voting mechanism in the Governing Board follows a double majority principle requiring 75 % of the financial contribution and 75 % of the votes. In view of its responsibility for the Union budget, the Commission holds 50 % of the votes. For its work on the Governing Board, the Commission will avail itself, wherever appropriate, of the expertise of the European External Action Service. The Governing Board is assisted by an Industrial and Scientific Advisory Board to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders." [24]

Working in close collaboration with the Network of National Coordination Centres and cybersecurity competence community (established by the proposed Regulation), the European Cybersecurity Industrial, Technology and Research Competence Centre would be the main implementation body for EU financial resources dedicated to cybersecurity under the proposed two programmes: Digital Europe Programme and Horizon Europe Programme.

Competence Centre

The Competence Centre shall have legal personality and its legal seat shall be located in Brussels, Belgium. As stated in Art. 3 of the proposal for Regulation, the mission of the Centre and the Network is to:

1. retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market;
2. increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.

The Competence Centre shall have the following objectives and related tasks:

1. facilitate and help coordinate the work of the National Coordination Centres Networks;
2. contribute to the implementation of the cybersecurity part of the Digital Europe Programme and of the Horizon Europe Programme;
3. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:

    a. Acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;

    b. Providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and

related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;

c. Providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;

4. contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy, by carrying out the following tasks:

a. Stimulating cybersecurity research, development and the uptake of EU cybersecurity products and solutions by public authorities and user industries;

b. Assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;

c. Supporting in particular public authorities in organizing their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;

d. Providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;

5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by supporting further development of cybersecurity skills, where appropriate together with relevant EU agencies and bodies including ENISA;

6. contribute to the reinforcement of cybersecurity research and development in the Union by providing financial support to cybersecurity research efforts; support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network; support research and innovation for standardization in cybersecurity technology;

7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by supporting Member States and industrial and research stakeholders with regard to research, development and deployment; contributing to cooperation between Member States by supporting education, training and exercises; fostering synergies between civil and defence cyber security research and markets;

8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by providing advice, sharing expertise and facilitating collaboration among relevant stakeholders; The Competence Centre shall cooperate with relevant EU institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security (ENISA or soon to be called the EU Agency for cybersecurity as provided in the draft Cybersecurity Act), the EU Computer Emergency Response Team (CERT-EU), the European External Action Service (EEAS), the Joint Research Centre (JRC) of the Commission, the Research Executive Agency, the Innovation and Networks Executive Agency, the European Cybercrime Centre (EC3) at Europol as well as the European Defence Agency. Such cooperation shall take place within the framework of working arrangements which are subject to the prior approval of the Commission.

Organisation, Membership and Structure of the Competence Centre

The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States. The structure of the Competence Centre shall comprise number of bodies, among which the:

1. Governing Board

The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union. The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate. ENISA shall be a permanent observer in the Governing Board.

The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities. It shall adopt its rules of procedure, including specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information. The strategic decision includes: a) adopting a multi-annual strategic plan containing main priorities; b) adopting the Competence Centre's work plan, annual accounts and balance sheet; c) adopting the specific financial rules of the Competence Centre in accordance with financial regulations; d) adopting the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community; e) adopting the annual budget of the Competence Centre; f) adopting a procedure for appointing the Executive Director; g) establishing working groups with members of the Cybersecurity Competence Community; h) appointing members of the Industrial and Scientific Advisory Board; i) adopting security rules and anti-fraud strategy;

1.1. Chairperson and Meetings of the Governing Board

The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. The ordinary meetings shall be held at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks. The Executive Director shall take part in the deliberations, but have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.

1.2. Voting rules of the Governing Board

The Union shall hold 50% of the voting rights. The voting rights of the Union shall be indivisible. Every participating Member State shall hold one vote. Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights. The Chairperson shall take part in the voting. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre.

2. Executive Director

The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, with proven expertise and high reputation in the areas where the Competence Centre operates. S/he shall be engaged as a temporary agent of the Competence Centre, the term of office is four years, extendable once for no more than four years. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission.

The Executive Director shall be responsible for the operations and for the day-to-day management of the Competence Centre and shall be its legal representative. S/he will perform his or her duties with complete independence within the powers assigned to him or her.

3. Industrial and Scientific Advisory Board

The Industrial and Scientific Advisory Board (ISAB) shall consist of no more than 16 members, appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community. Members of the ISAB should have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The term of office of members of the ISAB shall be three years. That term shall be renewable. Representatives of the Commission and of the ENISA may participate in and support the works of the Industrial and Scientific Advisory Board.

The ISAB shall have meetings at least twice a year. It shall advise the Competence Centre and provide to the Executive Director and the Governing Board

strategic advice and input for drafting the work plan and multi-annual strategic plan; organise public consultations open to all public and private stakeholders; promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre.

4. Financial Provisions

The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:

(a) EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;

(b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined.

The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as abovementioned.

The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, are subject to continuous and systematic monitoring and periodic evaluation. Also, the Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.

5. National Coordination Centre

Each Member State shall nominate, after compliance assessment, the entity to act as the National Coordination Centre. The European Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. All accredited Centres compose the "Network". The Member States may at any time nominate a new entity as the National Coordination Centre. The members of the Network shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.

The National Coordination Centres shall have the following tasks:

a. Supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;
b. Facilitating the participation of industry and other actors at the Member State level in cross-border projects;
c. Contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;
d. Acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre and seeking to establish synergies with relevant activities at the national and regional level;
e. Implementing specific actions for which grants have been awarded by the Competence Centre.
f. Promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level;
g. Assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.
h. Receiving a grant from the EU in relation to carrying out the abovementioned tasks, and where relevant, cooperate through the Network for the purpose of implementing these tasks.

6. The Cybersecurity Competence Community

The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the EU. It shall involve National Coordination Centres as well as EU institutions and bodies with relevant expertise. The requirements for accreditation as member of the Cybersecurity Competence Community are compliance with national law where established and proven cybersecurity expertise in: a) research; b) industrial development; c) training and education. The Competence Centre shall accredit relevant bodies, agencies and offices of the EU as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the relevant criteria. The accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria for membership or other relevant provisions.

The main tasks of the members of the Cybersecurity Competence Community, as described in the proposal shall be to support the Competence Centre in achieving the mission and the objectives, as well as to work closely with the Competence Centre and the relevant National Coordinating Centres.

Concluding Remarks

The Competence Centre proposal strives to implement the relevant parts of Horizon 2020 and Digital Europe programmes by allocating grants, enhancing coherence and synergies between them, and carrying out procurements. The Commission proposes to allocate nearly € 2 billion from Digital Europe for the 2021-2026 period and € 2.8 billion from Horizon Europe for setting up the Competence Centre. These substantial resources reflect the EU's commitment to investing more in cybersecurity policy. The proposal aims to create synergies between funding programmes and tools for cybersecurity related research and innovation both in civilian and defence areas. In fact, the proposal entitles the Competence Centre also to manage EDA resources, that would complement those earmarked under Horizon Europe.

EU's strategic interest is to ensure that the EU retains and develops essential capacities to secure its digital economy, infrastructures, society, and democracy. Europe's cybersecurity research, competences and investments are spread across Europe with too little alignment, which is considered as obstacle that has to be overcome as soon as possible. There is an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities. Europe has to master the relevant cybersecurity technologies from secure components to trustworthy interconnected Internet-of-Things ecosystems and to self-healing software. European industries need to be supported and equipped with latest technologies and skills to develop innovative security products and services and protect their vital assets against cyberattacks. This should contribute inter alia to achieve the objective of European strategic autonomy.

That being said, for the EU, it is a priority to promote democracy, the rule of law, human rights and fundamental freedoms worldwide. Therefore, the Centre should foster the development and investments into the resilience and integrity of networks and information systems. Offensive military applications such as backdoors, withheld vulnerabilities, or exploits bear an inherent security risk for society at large and run counter to these European goals.

With regard to the Bulgarian Expert Community, it should be noted that it is of the utmost importance to successfully integrate into the European Community through Horizon Europe. Currently there are 4 Bulgarian teams (the Bulgaria Defence Institute, the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences, the European Software Institute-Center Eastern Europe, and Telelink Business Systems) in ECHO consortium.

In October 2017, under the Horizon 2020, a call SU-ICT-03-2018 for "establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap" [25] was announced. This call is part of the Horizon 2020 focus area "Boosting the effectiveness of the Security Union" (SU). As stated in the topic description, main objective of this pilot is to scale up existing research for the

benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable. All approved pilot projects should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub. Projects under this pilot should help building and strengthening cybersecurity capacities across the EU as well as providing valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre. This shall contribute to strengthening the EU's cybersecurity capacity and tackling future cybersecurity challenges.

In 2018 four pilot projects were announced as winning and earlier this year were launched in order to operate a pilot for a European Cybersecurity Competence Network and to develop a common European Cybersecurity Research & Innovation Roadmap. CONCORDIA, CyberSec4Europe, ECHO [26] and SPARTA are the four projects which were chosen by the European Commission. These pilot projects bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States. The overall EU investment in these projects will be more than 63.5 million Euros. They will not only develop a sustainable European cybersecurity competence network, but will also implement a variety of tasks, e.g. cybersecurity demonstration cases (in eHealth, finance, telecommunications, smart cities, transportation, etc.), provide trainings and programmes to tackle the cybersecurity-skills gap in EU, etc.

References

1 European Commission, "Public Opinion," 2020, http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171.

2 Andreas Schmitz, "PwC Study: Biggest Increase in Cyberattacks in Over 10 Years," January 21, 2016, https://news.sap.com/2016/01/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/.

3 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres," Document 52018SC0403, European Union law, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537349553647&uri=CELEX:52018SC0403.

4 Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, Gian-Luigi Ruzzante, "European Cybersecurity Centre of Expertise - Cybersecurity Competence Survey," JRC111211, Publications Office of the European Union, 2018, http://publications.jrc.ec.europa.eu/repository/handle/JRC111211.

5 "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry," Document 52016DC0410, European Union law, 2016, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410.

[6] European Defence Agency, "Cyber Defence," 6 September 2017, https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-09-06-factsheet_cyber-defence.pdf.

[7] European Commission, "The Commissioners: The European Commission's political leadership," 2020, https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-eu-cybersecurity-conference-digital-single-market-common-digital-security_en.

[8] Council of the EU, "Conclusions on implementing the EU Global Strategy in the area of Security and Defence," 14149/16, Brussels, November 14, 2016.

[9] White House, "Factsheet Cybersecurity National Action Plan," 2018.

[10] National Science and Technology Council (NSTC) Committee on Technology, "The Networking and Information Technology Research and Development Program," October 2017, https://www.nitrd.gov/pubs/2018supplement/FY2018NITRDSupplement.pdf.

[11] "Draft Final Report on the Cybersecurity Market Study," 2018.

[12] "Draft Final Report on the Cybersecurity Market Study".

[13] "Draft Final Report on the Cybersecurity Market Study".

[14] "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspac," Document 52013JC0001, European Union law, 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001.

[15] European Commission, "Cybersecurity," Shaping Europe's digital future, 2020, https://ec.europa.eu/digital-single-market/en/cyber-security.

[16] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," Document 32016L1148, European Union law, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[17] "European Commission, NIS Cooperation Group," 2020, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

[18] ENISA – European Union Agency for Cybersecurity, 2020, www.enisa.europa.eu/.

[19] European Commission, "Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres," 2 September 2018, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research.

[20] (ISC)², Global Information Security Workforce Study, 2017, https://www.isc2.org/pressreleasedetails.aspx?id=14570.

[21] Proposal for a Regulation of The European Parliament and of the Council on ENISA (the EU Cybersecurity Agency), repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act," COM(2017) 477).

[22] This is without prejudice to the certification mechanisms under the General Data Protection Regulation, in which data protection authorities have a role to play, in line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, "General Data Protection Regulation".

[23] As defined in COM(2018) 435 Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination; and as referenced in COM(2018) 434 Proposal for a Regulation of the European Parliament and of the Council establishing Digital Europe Programme for the period 2021-2027.

[24] EU, "Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres,"

[25] European Commission, "Dynamic countering of cyber-attacks," 2018, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-01-2018.

[26] European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO), https://echonetwork.eu/.

About the Author

Valeri **Kopchev** is a lawyer with a Master in International Business Law degree from Université Libre de Bruxelles (Belgium) and Master in the field of Law of the European Union (Sofia University) with profound and diverse legal expertise and background covering various legal issues related to public procurement, data protection, European law, etc. Specializing in the field of interaction between data protection/privacy and artificial intelligence. Mr. Kopchev is a legal expert in Public Procurement and Concessions Directorate of the Commission on protection of competition – Bulgaria. Previously, he was working as attorney-at-law in the field of public procurement and data protection (2016-2019), a legal expert in the Geodesy Cartography and Cadastre Agency (2013-2016).