Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States

OSCE Organization for Security and Co-operation in Europe

Published by the Organization for Security and Co-operation in Europe
Vienna, March 2023

Layout and design by: MaxNova, Belgrade

ISBN 978-92-9271-230-3
Transnational Threats Department
OSCE Secretariat
Wallnerstrasse 6, A-1010 Vienna, Austria
https://www.osce.org/secretariat/cyber-ict-security

The publication of this report was made possible thanks to generous contribution from the Italian Republic. The content of this publication, including the views, opinions, findings, interpretations and conclusions expressed herein do not necessarily reflect those of donors. It is not a consensus-based document.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

This report was prepared by the OSCE Transnational Threats Department (TNTD) Co-ordination Cell under the direction of Ms. Szilvia Tóth, Cyber Security Officer.

TNTD would like to thank Dr. Camino Kavanagh for her research and for drafting the report. Valuable support was provided by Mr. Gregor Ramuš of TNTD Co-ordination Cell.

List of acronyms and abbreviations

BTK	Turkish Information and Communication Technologies Authority
CBM	Confidence-Building Measure
CCB	Centre for Cyber Security Belgium
CCN-CERT	Spanish Government National Cryptologic Center - Computer Security Incident Response Team
CERT	Computer Emergency Response Team
C-HUB	Cybersecurity Digital Innovation Hub (Portugal)
CIPAC	Critical Infrastructure Partnership Advisory Council (United States)
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act (United States)
CISA	Cyber and Infrastructure Security Agency (United States)
CSIRT	Computer Security Incident Response Team
CSN	Cybersecurity Network Foundation (Serbia)
DEG	Information Technology and Information Systems Security Experts Group (Latvia)

eID	E-identity
EISA	Estonian Information Security Association
EU	European Union
FINMA	Swiss Financial Market Supervisory Authority
FS-CSC	Swiss Financial Sector Cyber Security Centre
FS-ISAC	Swiss Financial Services Information Sharing and Analysis Center
ICT	Information and Communications Technology
ISAC	Information Sharing and Analysis Center
ITS	Higher Technological Institutes (Italy)
IWG	Informal Working Group
NCSC	National Cyber Security Centre
NCSC-FI	National Cyber Security Centre Finland
NICE Framework	Workforce Framework for Cybersecurity (United States)
NIS	Network and Information Security
NIST	National Institute of Standards and Technology (United States)
OKTT	Objectively Recognisable Task (the Netherlands)
OSCE	Organization for Security and Co-operation in Europe
PPP	Public-Private Partnership
R&D	Research and Development
SBOM	Software Bill of Materials
SME	Small and Medium Enterprise
SOC	Security Operation Center
SOW	Safeonweb (Belgium)
TLP	Traffic Light Protocol
UK	United Kingdom
UKC3	UK Cyber Cluster Collaboration
UN	United Nations
USOM	Turkish National Computer Emergency Response Center

FOREWORD

I am pleased to present the Report on Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration in OSCE participating States. The report evidences the implementation of OSCE cyber/ICT security Confidence-Building Measure 14, which encourage states to establish public-private partnerships to respond to common security challenges stemming from the use of Information and Communication Technologies. It provides examples of existing practice from the OSCE region, as well as baseline recommendations to support future efforts.

Since 2013, OSCE participating States adopted 16 confidence-building measures for cyber/ICT security, making the OSCE the first regional organization to develop such measures. The OSCE continues to play a pioneering role in this regard, with recent United Nations processes on international ICT security recognizing the importance of regional and sub-regional organizations in developing and implementing confidence-building measures in their regions.

With CBM 14, OSCE participating States underlined the significance of a multistakeholder approach to cyber/ICT security, in particular through the structured co-operation with the private sector. There is broad recognition that such collaboration can increase cyber resilience and strengthen national preparedness. On an international level, the exchange of good practices and lessons-learned on this topic serves as a confidence- and capacity-building exercise, which the OSCE's Transnational Threats Department is privileged to support.

In the OSCE, we have already seen a number of such constructive exchanges. In fact, CBM 14 has received widespread attention and, as showcased by the concrete examples of public-private partnerships in this report, considerable national implementation. Through the 'Adopt a CBM' initiative, inaugurated in 2018 by the Chair of the Informal Working Group established by Permanent Council Decision No. 1039, this measure is sponsored by a group of six participating States, whose efforts were instrumental for this report.

The report builds upon previous studies done by participating States, which gathered examples of public-private collaboration in cyber/ICT security. It further develops on these findings through a series of interviews conducted with public sector representatives actively involved in co-operation with the private sector. By highlighting examples of emerging practices and discussing concrete modalities of public-private partnerships, the report hopes to serve as a capacity-building tool for experts and policy-makers and support the formulation and implementation of national policies related to cyber/ICT security.

Alena Kupchyna

Co-ordinator of Activities
to Address Transnational Threats

OSCE Secretariat

Executive summary

Today's societies are highly dependent on digital technologies or are transforming in a manner that suggests even higher levels of dependency in the future. Cyber/ICT security and resilience are and will remain critical to the economic and social wellbeing of societies and to national and international security. Today, it may be challenging for governments to have the means and capacity to fully understand and respond to the growing number of cybersecurity-related threats and challenges their countries are facing. As with other forms of dependencies, governments are increasingly relying on co-operation and collaboration with the private sector and other non-governmental actors to respond to these threats and challenges, and the public policy needs and concerns that stem from them.

Many governments have introduced aspirations relevant to public-private partnerships and other such arrangements into their national cybersecurity policies and strategies. Such aspirations were originally focused on a narrow conception of cybersecurity and a public-private relationship model in which the market and industry self-governance would ensure cybersecurity, while governments would ensure open markets so that innovation could thrive. The increase in the scope and scale of threats in parallel with growing dependencies on digital technologies over the past two decades has, however, confirmed that the market and voluntary mechanisms do not in themselves produce cybersecurity, let alone resilience, and can misalign with broader national security, societal and normative goals. An alternative approach is one centered on creating regulatory regimes anchored in norms, rules, oversight and enforcement procedures and practices. Yet, such regimes are difficult to put in place in a constantly shifting environment. Over-regulation may misalign with both existing and emerging security threats, and they can slow or undercut innovation and reduce the incentives for private sector participation. It can also misalign with other obligations and duties, including those aimed at minimizing harm to the public. Striking a balance between the two has therefore been the imperative of many countries as they seek to engage with the private sector on cybersecurity and resilience-related issues in recent years. Again, this is not always easy since motivations and interests can differ significantly. In this regard, ensuring that public-private partnerships and other such arrangements are underpinned by key principles such as transparency and accountability is essential, notably when they are established to solve specific public policy problems, upon which national security is also contingent.

As this report demonstrates, there is no one single model for how public and private actors work together on cybersecurity and resilience-related issues. The character of public-private partnerships and other such arrangements, how they emerge and are implemented is influenced by the political, economic and social system, as well as the governance structure of each country. They are also shaped by the character of a country's national digital eco-system, which in turn is influenced by a range of issues, including a country's level of economic development; its fiscal, regulatory, and industrial policies; levels of investment in research and development; a country's education system; and many other factors.

In the OSCE region public-private partnerships, co-operative and collaborative arrangements have been established for a wide range of purposes: for sector- or topic-specific information or threat intelligence sharing; vulnerability disclosure; for responding to a particular type of cybersecurity problem (e.g., for countering ransomware, phishing, botnet eradication); for general or sector/specific awareness raising, cyber hygiene, capacity-building and for educational purposes. These range from formal, contract-based or regulated public-private arrangements to informal, voluntary collaborative networks or clusters.

The modalities for implementing these arrangements are just as wide-ranging.

Many of the existing arrangements discussed throughout the report have emerged organically in response to a shifting cybersecurity threat landscape, sometimes at the initiative of a government agency or of a company that has identified a particular problem that requires solving. In other instances, national cybersecurity strategies provide a framework for co-operation and collaboration. In others, national legislation or regulation requires the private sector to co-operate with public authorities. This is increasingly the case where reporting of cybersecurity incidents affecting the networks and systems of critical sectors and services is concerned. Incentivizing participation and building trust across actors and sectors has emerged as both an objective and challenge in these relations.

That public-private partnerships and other such arrangements can enhance cybersecurity and resilience is not a new consideration. What is new is emerging thinking on how they can produce positive dividends, not just for meeting narrow national security objectives of individual countries, but also for meeting broader whole-of-society objectives both within and beyond national borders.

Finally, some participating States have noted that lessons shared on CBM 14 implementation within the OSCE Informal Working Group established by Permanent Council Decision No. 1039 (IWG) have been very useful, helping them shape similar initiatives in their own countries, redesign or redirect them. The report demonstrates that there is a clear appetite amongst most participating States to continue sharing emerging practices and lessons on cybersecurity-related public-private partnerships and other such arrangements within the OSCE framework, as long as these examples and lessons are topic-specific, focus on practical outcomes, and include both the public and private actors involved in the examples that are shared, as appropriate.

With the latter in mind, the report presents these emerging practices and lessons as baseline recommendations and organizes them under the rubrics of purpose, policy, process and people. It further suggests that they be taken up within further exchanges among OSCE participating States and between the OSCE and other regions in line with the spirit and intent of the OSCE cyber/ICT security Confidence-Building Measures, particularly CBM 14. Such discussions can potentially be organized around topics that OSCE participating States have identified for further discussion.

These include exchanges on

- how other participating States as well as governments in other regions establish and maintain collaborative relations with small and medium enterprises, research institutes or specific critical infrastructure sectors;
- trusted and secure platforms for information exchange;
- rapid response capacities;
- incentive-accountability structures in cybersecurity-related public-private partnerships;
- monitoring and oversight of such arrangements.

Purpose

Cybersecurity-related public-private partnerships (PPPs) and other such arrangements should have a clearly defined purpose.

Policy

Cybersecurity-related PPPs and other such arrangements should be clearly outlined in national policy and/or legislation.

Process

Cybersecurity-related PPPs and other such arrangements require clear implementation modalities or governance structures to help ensure that goals are met and that appropriate incentive-accountability structures are considered from the outset.

People

Cybersecurity-related PPPs and other such arrangements require clarity about who should be involved and for what purpose.

Background and introduction

In line with OSCE Confidence-Building Measure 14 "[p]articipating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs."[1] In 2021, the OSCE CBM 14 Group[2] launched a study to determine the level of engagement of OSCE participating States with this specific CBM.[3]

This report builds on that study and the accompanying report that was shared with participating States to provide an overview of emerging practices in cybersecurity-related public-private collaboration in OSCE countries. It also draws from an additional series of 23 interviews with participating States conducted between July and October 2022, as well as a review of publicly available documentation referenced during the interviews.

Throughout the report the term 'public-private arrangements' is often used in lieu of the term 'public-private partnerships'. This decision is informed by the interviews with and submissions of participating States on current practices relevant to CBM 14: while for some States there is a preference to use the term 'public-private partnerships' since it is enshrined in national law and policy, for others, the alternative more aptly captures the broad range of relational models involving public and private actors that leverage co-operation and collaboration to address cybersecurity threats affecting the economies, societies and security of OSCE participating States.

Finally, the views reflected in the report are principally those of government stakeholders, all of which acknowledged the need to include private actors in future work on this topic, including in relevant exchanges on CBM 14 at the OSCE.

1 OSCE Permanent Council Decision No. 1202, 10 March 2016: https://www.osce.org/pc/227281

2 The OSCE CBM 14 Group currently consists of: Austria, Belgium, Estonia, Finland, Italy and Sweden. These participating States are championing the implementation of CBM 14 under the 'Adopt a CBM' initiative. The initiative was inaugurated in 2018 by the Chair of the OSCE Informal Working Group established by Permanent Council Decision No. 1039 to promote ownership of individual CBMs by interested participating States to explore concrete modalities of their implementation.

3 PC.CBM/3/21 "Report on main insights from the OSCE Cyber/ICT Security Confidence-Building Measure 14 questionnaire on public-private partnerships", circulated on 10 September 2021.

MAIN FINDINGS

Purpose (general)

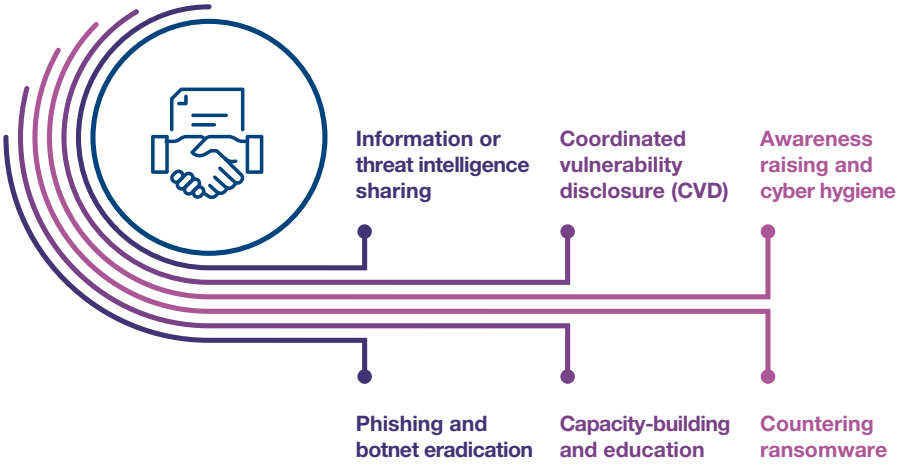
Cybersecurity-related public-private partnerships (PPPs) and other such arrangements should have a clearly defined purpose. This requires:

- A clear understanding of the national cybersecurity ecosystem.
- A clear understanding of the strengths and weaknesses of relevant public and private sector entities in the country vis-à-vis the cybersecurity and resilience challenges that need to be addressed.
- Identifying areas in which public-private co-operation could address identified challenges.
- Identifying how to incentivize engagement of relevant private sector and other actors.
- Identifying whether a dedicated government position for facilitating or co-ordinating relations between the public and private sector needs to be established.

Today, responding to cybersecurity threats involves having a clear understanding of the scope and scale of the cybersecurity and resilience-related threats and challenges the country is facing and setting clear goals. Co-operation and collaboration across sectors are increasingly viewed as an effective approach for meeting such goals, not least since private actors develop and own many of the technologies, products and services upon which the wellbeing of society depends and have insights that can differ significantly from those of government agencies.

There is acknowledgement across many OSCE participating States that while governments set policy and law, they alone may not be able to identify and attend to the scope and scale of cybersecurity-related challenges, nor cover the costs of doing so. Recent significant cybersecurity incidents and their spillover effects on businesses and societies across the globe are an important reminder of the need for partnerships and other forms of collaboration with the private sector, and with other actors.

Evidently, private sector entities cannot replace the role of government authorities where national security, public safety and other public goods are concerned, but they can contribute positively to meeting those goals. However, their motivations and incentives do not always align with those of governments. These misalignments can be particularly problematic where national security and public safety are concerned, since industry actors are often reluctant to invest resources that go beyond their immediate business needs or in initiatives that may increase costs, undermine their business activities and pose reputational risks. On their part, governments may not provide the necessary incentives to ensure meaningful engagement of private actors. This is particularly problematic where information or threat intelligence sharing is concerned. As in other public policy areas, these relationships come with many benefits and trade-offs. They can take time to nurture and may well start on the basis of limited trust.



As evidenced throughout the report, in the OSCE region public-private partnerships and other such arrangements have been established for a wide range of purposes: for sector- or topic-specific information or threat intelligence sharing; coordinated vulnerability disclosure; for responding to a particular type of cybersecurity problem (e.g., for countering ransomware, phishing, botnet eradication); for general or sector/specific awareness raising, cyber hygiene, capacity-building and educational purposes. These range from formal, contract-based or regulated public-private partnerships to informal, voluntary collaborative networks or clusters. The modalities for implementing these arrangements are just as wide-ranging.4 In the sections that follow, the report offers practical examples of public-private partnerships and other such arrangements from the OSCE region with reference to the purposes mentioned.

Approaching cybersecurity from a co-operative and collaborative perspective involves having a deep understanding of the cybersecurity ecosystem in the country and the strengths and weaknesses of relevant public and private sector entities vis-à-vis the cybersecurity and resilience challenges that need to be addressed. It also includes understanding how all stakeholders involved can benefit from the collaboration, in a manner that ensures that the public good is both a driver and a goal of the collaboration. For example, governments engaging with the private sector may draw from the resources, expertise, and insights of the private sector to address cybersecurity threats that prevent them from meeting public policy goals. For states with limited resources, this can be game-changing. Private sector entities benefit by having access to threat information that can help them protect their business. For SMEs, co-operation with the public sector can help secure more resources, skills and support for incident response and recovery. During the pandemic the increase in these forms of co-operation proved enormously valuable and, in some instances, have provided SMEs with an opportunity to help shape cybersecurity-related policy and regulation, as well as incentive structures within their respective sectors.

4 PC.CBM/4/21 "CBM 14 Projects from the questionnaire", circulated on 06 December 2021.

Policy

Cybersecurity-related PPPs and other such arrangements should be clearly outlined in national policy and/or legislation. This requires:

- Acknowledgement of the importance of public-private arrangements in national cybersecurity policy and strategy, including through the articulation of how the arrangement will contribute to attaining national security, economic and social development goals, details of which can be included in related action plans.
- Consultation with relevant private entities in policy, legislative and regulatory decisions that will affect them.
- A commitment to establishing transparency and oversight mechanisms for public-private arrangements and related activities.

OSCE participating States increasingly highlight the importance of working with private sector entities on cybersecurity issues in domestic legislation, policy and strategy. Some participating States anchor their engagement with the private sector in national legislation. Many more use policy instruments for that purpose. This is evident in the number of national cybersecurity strategies that include provisions on public-private collaboration, which generally cover opportunities of collaboration with the private sector for the economy, society and the general national interest. Such provisions provide the rationale – sometimes value-based – for such collaboration.

Examples of references to public-private partnerships and other such arrangements in the national cybersecurity strategies of OSCE participating States

Albania, National Cyber Security Strategy (2020-2025)

"Coordination and cooperation among all actors are the core element to guarantee success. Cooperation with the private sector should be strengthened because of the Information and Communication Technology (ICT) rapid development dynamic. ICT security and development in the state administration can only be enhanced with close cooperation and in coherence with technology developments and trends".

Czech Republic, National Cyber Security Strategy (2021-2025)

"Ensuring cyber security involves coordination among many states and non-state bodies to enable the Czech Republic to effectively face even the most serious and complex challenges and threats. A common, integrated, and national approach to providing security in cyberspace and the fight against cyber threats is essential. (…) Leaving cyber security solely to the Czech state is not enough, however. Every institution, private company, and individual has their role and can positively contribute to cyber security. The Czech Republic must therefore set up and support a cyber security policy that will consistently incorporate all of society into cyber security processes and thus increase its resilience to cyber threats".

Denmark, National Strategy for Cyber and Information Security (2022-2024)

"Through a number of concrete actions in the strategy, the government is strengthening public-private cooperation on cyber and information security. The initiatives ensure better opportunities for knowledge and experience exchange, strengthen the advisory efforts towards public authorities, companies and citizens and contribute to the competitiveness of Danish companies through concrete tools".

Estonia, Cybersecurity Strategy (2019-2022)

"We will maintain an active and cohesive cybersecurity community. To do so, we will offer technical information streams, organize joint exercises and involve the private sector and academic competence in legislative drafting and strategic planning processes. (…)We will support effective cooperation between state, academia and the private sector's key partners. To this end, we will launch a cluster that facilitates both domestic and international cooperation".

Finland's Cyber Security Strategy (2019)

"Cyber security preparedness requires cooperation among various actors in society, the central government and the business community as well as skills strengthening in different sectors. Interdependencies in the digital operating environment require a comprehensive architecture that takes cyber security into account. Continuity of operations and preparedness for incidents require expertise in procurement and tendering, implementation assessment of contractual obligations and comprehensive management of the supplier network and supply chains. (…) National cyber security will be built in cooperation among the authorities, the business community, organisations and citizens, when everyone can contribute to our shared cyber security".

Italy, National Cybersecurity Strategy (2022-2026)

"Transversal to the (…) goals of protection, response, and development, as well as to the enabling factors of training, promotion of the cybersecurity culture, and cooperation, is the Public-Private Partnership (PPP) that fully permeates this strategy [which is] based (…) on a "whole-of-society" approach in which the public sector acts synergically with the industry, civil society, academia and research, as well as the media, families, and individuals, to strengthen the cyber resilience of the Country and the society as a whole. Moreover, cyberspace is made up of ICT products and services mainly produced or provided by private entities. For this reason, this strategy cannot exclude the close cooperation and continuous public-private consultation which translates into a series of structured actions, such as cyberspace monitoring through the cooperation of SOCs, incidents mitigation through CSIRTs collaboration and qualified incident response, the network of test laboratories, as well as training and awareness dissemination".

Slovakia, The National Cyber Security Strategy (2021-2025)

"Security in general is one of the primary interests of any democratic country with the rule of law. The field of cybersecurity is no exception, and it is more globalized as cyberattacks do not recognize national borders and attackers need not be explicitly citizens of the country in which the attack originates from. Therefore, it is very important that the state creates very strong partnerships at international level, exchanges experiences, knowledge and information, and afterwards applies them at national level. Cooperation and confidence building between entities of public administration, the private sector and academia ensures cybersecurity development".

Republic of Serbia, National Information Society and Security Development Strategy (2021-2026)

"Cooperation between the public and the private sectors is one of the key elements of information security of every country. Namely, limitations which exist on both sides in responses to challenges of information security impose the need to establish partnerships, particularly in case when incidents significantly jeopardise information security. In public-private partnership, finding the appropriate cooperation mechanism is not the only issue; instead, there is also the issue of creating trust between them that will contribute to strengthening of capacities and increasing the level of information security".

Türkiye, National Cyber Security Strategy (2020-2023)

"By establishing an organic cyber security network, it is aimed to develop cooperative efforts where people from all segments who are working or interested in cyber security field can share knowledge and experience. (…) It is of great importance to increase knowledge exchange between public institutions and private sector regarding cyber threats and form new connections with stakeholders, mainly the young population who have studies in the field of cyber security".

United Kingdom, National Cyber Security Strategy (2022)

"Central to our strategy will be a whole-of-society approach to cyber. We need to build an enduring and balanced partnership across the public, private and third sectors, with each playing an important role in our national effort".

United States Department of Homeland Security, Cybersecurity Strategy (2018-2023)

"The growth and development of the Internet has been primarily driven by the private sector and the security of cyberspace is an inherently cross-cutting challenge. To accomplish our cybersecurity goals, we must work in a collaborative manner across our Components and with other federal and nonfederal partners.".

European Union, NIS2 Directive (2022)

"Public-private partnerships (PPPs) in the field of cybersecurity can provide an appropriate framework for knowledge exchange, the sharing of best practices and the establishment of a common level of understanding among stakeholders. Member States should promote policies underpinning the establishment of cybersecurity-specific PPPs. Those policies should clarify, inter alia, the scope and stakeholders involved, the governance model, the available funding options and the interaction among participating stakeholders with regard to PPPs. PPPs can leverage the expertise of private-sector entities to assist the competent authorities in developing state-of-the-art services and processes including information exchange, early warnings, cyber threat and incident exercises, crisis management and resilience planning".

Associated action plans often include explanations of ***how*** such aspirations will contribute to greater cybersecurity and resilience and provide more detail regarding key areas for collaboration such as information/threat intelligence sharing, including

- around critical infrastructure protection;
- early warning;
- education;
- workforce development;
- up-skilling and cybersecurity-related R&D;
- growth and innovation.

In most cases, OSCE participating States have included consultations with private actors in the process of developing their national cybersecurity strategy. This is a significant development from just a decade ago.

Sometimes such collaboration can happen at the stage of action plan development. For instance, in **Kazakhstan**, a working group involving a wide range of actors including professional and industry associations, higher educational institutions, and industry was established "to analyse the status of informatization at government agencies, automation of public services, prospects for the digital economy, and modernization of production processes, aiming to expand the scope for ICT services".[5] It also studied international experience in protecting national ICT infrastructure. The resulting Action Plan is currently being implemented.

Some OSCE participating States also establish specific public-private bodies to accompany implementation of their cybersecurity strategy. The **UK National Cyber Advisory Board** is one such example, set up to ensure government exposure to alternative viewpoints and networks from across the national cyber ecosystem, "to support the delivery across all five pillars of the strategy".[6]

Such consultative efforts help ensure that strategies are comprehensive and reflect the diversity of issues to be tackled and the diversity of voices of the stakeholders involved. It can help reinforce the legitimacy of the strategy and its implementation modalities and manage expectations.

Other policy-related developments are evident in OSCE countries. For instance, the past few years have seen a policy shift in some jurisdictions regarding whether and how regulation can contribute to strengthening cybersecurity and resilience. Breaking with the norm of leaving cybersecurity to the self-correcting forces of the market and to voluntary industry measures, governments are increasingly looking to regulate the cybersecurity practices of entities viewed as critical to enabling digital transformation dividends, and to national security. For instance, due to the increase in cyber threats, several participating States have enacted or are enacting rules requiring entities within certain sectors to report serious cybersecurity incidents affecting their networks and systems and to regularly share information. Such efforts can be met with resistance. Nonetheless, transparent consultative processes on new rules, including on incentive-accountability structures, and public-private arrangements to accompany the development of the new rules as well as their implementation, can help accommodate concerns.

For members of the **European Union (EU)**, reporting and information sharing requirements were introduced into the 2016 Network and Information Security (NIS) Directive. The revised **Directive (NIS2)** aims to strengthen existing cybersecurity risk-management measures and reporting obligations across the sectors that fall within the scope of the Directive (energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure).

5 https://www.itu.int/hub/2022/08/implementing-kazakhstan-cybersecurity/

6 https://www.gov.uk/government/news/cabinet-office-appoints-national-cyber-advisory-board-co-chair

To this end, the revised Directive "(…) provides that Member States shall lay down cybersecurity risk management and reporting obligations for entities referred to as essential entities in Annex I and important entities in Annex II; (c) provides that Member States shall lay down obligations on cybersecurity information sharing".[7]

The review of the Directive involved consultations with a broad range of stakeholders through different formats including open consultations, workshops, country visits and interviews. A co-ordinating body – the Co-operation Group – is expected to act as a forum for engaging with private stakeholders from across the EU on the Group's activities and challenges that may emerge around NIS2 implementation.

In the **United States**, the 2022 **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)** lays the basis for the national Cyber and Infrastructure Security Agency (CISA) "to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA". The aim of these reports is to allow CISA to rapidly deploy resources and render assistance to victims suffering attacks. They are also expected to help CISA strengthen existing capacities to spot trends, and quickly share information with network defenders to warn other potential victims. The Act also requires CISA to consult with a broad range of public entities throughout the rulemaking process and has committed to receiving input from private actors that will be covered by the regulations. Until the CIRCIA rulemaking process is finalized and the reporting requirements come into effect, CISA has encouraged voluntary reporting by relevant entities, including through existing threat intelligence and information-sharing partnerships.

7 The Directive applies to public or private essential entities operating in the energy; transport; banking; financial market infrastructures; health, drinking water; waste water; digital infrastructure; public administration and space sectors and to certain important entities operating in other sectors including postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0823

Process

Cybersecurity-related PPPs and other such arrangements require clear implementation modalities or governance structures to help ensure that goals are met and that appropriate incentive-accountability structures are considered from the outset. This includes joint confirmation by the public and private actors involved on:

- The specific goals of the arrangement and the specific problems it is setting out to solve.
- The activities that the arrangement will undertake to attain the agreed goals.
- Lifespan and funding sources.
- Security or non-disclosure requirements and protocols that need to be put in place and the cyber hygiene practices that need to be promoted amongst participants.
- Mechanisms for monitoring and oversight of activities undertaken.
- Mechanisms for reviewing and updating implementation modalities or governance structures of the overall PPP/arrangement.
- Communications/outreach strategy.

As noted, a national cybersecurity strategy may lay out the broad contours of public-private collaboration. In addition to determining the purpose of a given public-private arrangement, its proponents will also need to suggest ***how*** it intends to achieve said goals.

Implementation modalities / governance structure

There is no single governance model of a cybersecurity-related public-private partnership or other such arrangement. The model will generally be informed by context, including the political and economic system and governance structure of a given country, as well as the nature of the problem or issue to be resolved, i.e., its actual purpose. This makes it difficult to propose a general definition of or blueprint for establishing them. Nonetheless, there are commonalities among most of the public-private arrangements identified in the report, notably that there tends to be clarity around their scope, the stakeholders that are involved, the implementation modalities or governance structures of the arrangements - which range from highly structured, to informal. Many also require trusted and secure forms of participation and communication. Where there appears to be less focus across all examples is on how participating States monitor and assess the contribution of these arrangements to broader cybersecurity and resilience goals.

Common models or structures of cybersecurity-related public-private partnerships and other such arrangements in OSCE participating States include those organized under the umbrella term of 'cybersecurity clusters' or 'hubs'. They are an approach, generally emerging from the private sector and/or academia, that bring together the resources, capabilities and competencies of industry, academia and government within a country's cybersecurity ecosystem. Incentives are created by sharing information, pooling knowledge, identifying workforce challenges, creating networking opportunities and R&D activities, including for locally developed cybersecurity solutions that can be scaled nationally and internationally.

Cyber clusters or hubs vary in sophistication. Some can be quite simple arrangements, serving as basic information sharing and networking platforms and for encouraging collaboration around emerging issues. For countries or regions within a country with an emerging digital ecosystem, these kinds of arrangements are an important starting point for collaboration. In some such instances, other more elaborate or mature clusters have been approached to provide advice on their establishment. There is also a healthy interaction between national cybersecurity clusters, including through Global Epic, an international confederation of clusters.

In terms of concrete activities, some of these arrangements provide services or facilitate access to knowledge and solutions. This is the case **of Portugal**'s **Digital Innovation Hub - C-HUB**, which offers innovative multi-disciplinary cybersecurity services across the country, specifically targeting SMEs, or **Denmark**'s **Cyber-Hub**, which facilitates partnerships between innovative Danish start-ups in cybersecurity and research and/or the public service. Similarly, the **Estonian Information Security Association (EISA)** boosts cross-sectorial co-operation between academia, private sector as well as the government and intends to enhance R&D activities in the domain of cybersecurity.

Cybersecurity clusters can also identify and provide opportunities for responding to the needs of a national cybersecurity ecosystem, including systemic workforce challenges. This includes developing mechanisms and tools that can categorize cybersecurity work and roles, while also assisting cybersecurity jobseekers by matching their skills with industry needs. An example of such a tool is **Cyber Ireland's National Initiative for Cybersecurity Education workforce framework**, in turn developed on the basis of the **United States National Institute of Standards and Technology (NIST)** workforce framework.[8] Such cybersecurity clusters may be managed by a dedicated privately-run secretariat, as in the case of the **Hague Security Delta** or in their early stages, an academic institution as in the case of **Cyber Ireland**. In others, such as the **Turkish Cyber Security Cluster**, government bodies may be the co-ordinators.

Often, national cyber cluster arrangements develop operational guidance. For instance, the **UK Cyber Cluster Collaboration (UKC3) Network** has worked with national cluster leads from across the country to develop an agreed operating framework for cyber clusters. The **Cyber Cluster Operating Framework**[9] comprises a common set of principles, objectives and outcomes that provide a clear definition of a cluster's remit and objectives, enabling stakeholders to better understand and support the work that clusters do in developing and growing their local cyber ecosystem. To incentivize the use of the framework, there is an expectation that cyber clusters seeking formal recognition and funding from UKC3 apply it.

8 'Workforce Framework for Cybersecurity (NICE Framework), National Institute of Standards and Technology (NIST), Special Publication 800-181, Revision 1, https://doi.org/10.6028/NIST.SP.800-181r1

9 https://ukc3.co.uk/cyber-cluster-operating-framework/

Other kinds of structures that promote public-private collaboration include those led by government. These are wide-ranging across OSCE participating States. They include **Sweden**'s **Cyber Security Council**, a co-operation forum with broad representation from the public and private sector, as well as academia. The Council serves as a strategic resource for the Swedish Civil Contingencies Agency in its work to support and co-ordinate cybersecurity as well as in analyzing and assessing external developments within the area. **Latvia**'s **Information Technology and Information Systems Security Experts Group (DEG)**, involves experts from various national organizations including from the private sector. The Group

- provides a platform for information exchange on IT/IS threats;
- encourages and supports professional growth of members of the group;
- pools resources for capacity-building / educational purposes on IT/IS security topics;
- supports the national computer incident response team, CERT.LV.

Beyond cyber clusters, hubs and similar structures, several OSCE participating States highlighted work underway with private actors on specific cybersecurity problems, such as

- protecting the healthcare sector;
- strengthening e-government services, including e-identity solutions;
- early warning;
- software security and supply chain risk management;
- phishing mitigation;
- coordinated vulnerability disclosure;
- botnet eradication, to name but a few.

Each of these initiatives have very different goals and governance modalities and involve very different actors. For instance, since the onset of the COVID-19 pandemic, healthcare sector entities across the globe have been the target of cyberattacks that have had significant economic implications as well as direct and indirect impacts on patients. Significant attention is now being paid to strengthening public-private efforts to prevent and mitigate such attacks. One such effort is the collaboration between the **Czech Republic**, **Microsoft** and the **Cyber Peace Institute** that has resulted in a Compendium of Multistakeholder Perspectives on **Protecting the Healthcare Sector from Cyber Harm**.[10] The Compendium is the result of several workshops involving public and private actors on a range of technical, operational and normative aspects relevant to the protection of the healthcare sector.

10 https://cyberpeaceinstitute.org/compendium-of-multistakeholder-perspectives/

Another example relates to the development of e-identity (eID) solutions, currently a concern of countries across the globe as they move to digitalize and ensure the security and resilience of government services. In **Estonia**, for example, the government has co-operated closely with the private sector in developing and implementing such solutions since the beginning of 2002. While the **Information Systems Authority** is responsible for shaping a vision and strategy for the development of the eID field, a private sector company, **SK Solutions**, provides trusted authentication services to both the private and public sector.

Where awareness raising and early warning is concerned, National Cyber Security Centres across a growing number of countries are providing new services. In **Finland**, for instance, the National Cyber Security Centre (NCSC-FI) established and manages the automated **Autoreporter system**, a tool which collects global information on malware traffic originating from Finland. NCSC-FI shares this information with telecommunications operators, who further distribute it to their end customers in an effort to raise awareness and combat the spread of malware.

Some participating States also view their engagement with the whole-of-society on cybersecurity-related issues as a form of public-private engagement. Examples include **Belgium**'s annual cybersecurity awareness campaign. Its **Safeonweb (SOW)** application is a result of the latest campaign.

The app collects news about phishing and warns of cyber threats and new forms of online scams. It provides regular updates to subscribers on vulnerabilities and threats via a dedicated application. The application also serves as an e-learning platform where users can learn basic security and cyber hygiene practices and test their knowledge and awareness. Participation in this initiative is voluntary. It emerged from an earlier initiative – the **BePhish campaign** – through which internet users voluntarily alert the Belgian Centre for Cybersecurity (CCB) when they receive a suspected phishing message. An automated process then checks the links or attachments and determines whether to block them.

Where software security and supply chain risk management are concerned, public-private collaborative work has been underway for some time. Recent initiatives include the **Securing the Software Supply Chain: Recommended Practices Guide for Customers**[11], developed in the **United States** by the **Enduring Security Framework Working Group** that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC), a cross-sector, public-private working group. The publication is the third in a three-part series providing best practices to software customers for procuring and deploying secure software. It also includes guidance for the Software Bill of Materials (SBOM), a list of all the 'ingredients' that make up software components and on which collaborative efforts have been underway since 2018.

11 https://www.cisa.gov/uscert/ncas/current-activity/2022/11/17/cisa-nsa-and-odni-release-guidance-customers-securing-software

In the **European Union**, a **voluntary cybersecurity certification framework for ICT products, processes and services** also depends on deep public-private collaboration, including around software products. The recently proposed **Cyber Resilience Act**, which aims to ensure greater security of hardware and software products, counts on significant public-private collaboration in developing the rules, and will require continued collaboration between public and private actors once the new rules are adopted.[12]

Cross-border promotion of cybersecurity-related public-private partnerships and other such arrangements

The importance of public-private co-operation and collaboration across borders cannot be underestimated. The increase in ransomware attacks and their impact on the functioning of societies across the globe has laid bare the need for these kinds of arrangements, including to strengthen rapid response capacities across all countries. Recent ransomware incidents demonstrate the value of such public-private response arrangements and collaboration across regions. For instance, **Spain** sent two mixed teams comprised of members of the Spanish Government National Cryptologic Center - Computer Security Incident Response Team (CCN-CERT) and private companies to support the incident response and recovery effort in Costa Rica in April and June 2022 respectively. The recent announcement by **Spain** and the **United States** on the development of a **capacity-building tool** to help countries use **public-private partnerships to counter ransomware** can bolster such efforts. The project aims to "provide guidance to States around the world seeking to develop or deepen public-private partnerships", including by showcasing innovations in countering ransomware, and by creating 'financing schemes' to support such public-private collaborations.[13]

Ensuring trust and security in public-private partnerships and other such arrangements

In most instances, the purpose of the public-private arrangement and the character of the entities involved dictate the level of trust and security needed to enable co-operation. Many of the examples of such arrangements in OSCE participating States are open to broad participation and do not involve any formal vetting process. These tend to be oriented towards general awareness raising, capacity-building or cyber hygiene.

12 Cyber Resilience Act – new cybersecurity rules for digital products and ancillary services. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en

13 https://www.cisa.gov/news-events/news/united-states-and-spain-announce-development-new-capacity-building-tool-combat

> The closer an issue is to national security, however, the more closed the platform will be and participants will likely be required to have a security clearance or sign some form of confidentiality or non-disclosure agreement.

These kinds of requirements can, however, foster distrust, in addition to taking time to establish. Conversely, the report shows that closed platforms can be mutually beneficial to the public and the private stakeholders involved: they help protect confidential and proprietary information, while also expanding the scope of information that the involved stakeholders have access to. Such platforms also provide members or participants with the potential to influence policy and operations within a certain community or sector. Consultative processes leading to the establishment of a given public-private arrangement can also contribute to incentivizing participation and help ensure that the arrangement responds to the security and/or confidentiality concerns and requirements of all involved, and not just the national security concerns of the government.

Across OSCE participating States, efforts are being made to establish secure and trusted platforms to strengthen public-private collaboration, particularly when the objective is to share sensitive information or threat intelligence in a timely manner. Some countries use the 'Traffic Light Protocol', "a set of designations used to ensure that sensitive information is shared with the appropriate audience".[14] The latter is used, for instance, by the **Cyber Security Coalition of Belgium**, a non-profit association that promotes collaboration between government, the private sector and academia to accelerate digital resilience and respond to emerging threats.

Some companies can also play a trusted bridging role between government agencies and the private sector. For example, in the Netherlands, non-vital companies can receive a special status called an **Objectively Recognizable Task (OKTT)**, which allows them to serve as a kind of information- and advisory-sharing bridge between the National Cyber Security Agency and organizations in their respective networks.

14 Traffic Light Protocol (TLP) definitions and usage. Available at: https://www.cisa.gov/tlp

Sometimes, it is the government itself that establishes secure platforms. Upon adoption of its National Cyber Security Strategy and Action Plan, Türkiye established the **National CERT (USOM)** under the existing national Information and Communication Technologies Authority (BTK) to co-ordinate incident response at the technical level. USOM has since established a collaboration between public and private CERTs. A secure platform - **USOM 24/7** – is used to collect and share data, threat information and intelligence between public and private CERTs. USOM also contributes to the growth of the national cybersecurity ecosystem by training experts and supporting the development of cybersecurity solutions.

When an initiative is led by the government, clarity around requirements such as security clearances and ensuring that industry participation is voluntary can help nurture confidence in the initiative within industry and the broader public. Take, for instance, the **United Kingdom's Industry 100 initiative**. It facilitates close collaboration between the National Cyber Security Centre (NCSC) and UK industry. Through the collaboration, the NCSC seeks to "learn lessons, identify systemic vulnerabilities and reduce the impact of cyber attacks".[15] The initiative works on a secondment basis whereby industry actors can seek a part-time placement at the NCSC (ranging from one day per week to one day per month). NCSC teams place advertisements on the NCSC website when they are looking for specific skill sets. To maintain independence, the selected candidates' organizations are expected to pay the salary of their staff member while on secondment. To ensure security, selected secondees are expected to have a security clearance.

Countries hosting multinational companies or services may face unique challenges with information sharing, particularly when there is a need to enable threat intelligence sharing with non-national entities. In **the Netherlands, a 'Circle of Trust'** was established to deal with these and other such challenges. Comprising the CERTs of 10 multinational companies based in the country and the National Cyber Security Centre, it serves as a safe and secure space for exchanging information, including on cybersecurity and supply chain risks, and talent development. The Circle of Trust does not replace the work of national, sector specific ISACs, which are bodies dedicated to collecting, analyzing and disseminating actionable threat information to members and for providing members with tools to mitigate risks and improve resilience.

Since multinational companies or services often fall within designated critical sectors, additional measures may need to be taken to ensure a trusted and secure environment for information sharing. In **Switzerland**, an elaborate structure has been established to enable collaboration within the financial sector, including non-Swiss entities, and between the financial sector and government authorities. Established in April 2022, the **Swiss Financial Sector Cyber Security Center (FS-CSC)** has over 50 founding members, including banks, insurers and industry associations as well as affiliated government agencies such as the Swiss Financial Marker Supervisory Authority (FINMA), the National Cyber Security Centre and the State Secretariat for International Finance. The body is structured around a Steering Board, which activates a Cri-

15 https://www.ncsc.gov.uk/section/industry-100/about

sis Co-ordination Cell in the event of a systemic incident; an Expert Group, which runs projects aimed at strengthening cyber resilience and organizes strategic and operational exercises; and an Operational Cybersecurity Cell, which manages information sharing, monitors events relevant to the sector, provides sector-specific reports and supports crisis management. It operates as an association and membership is fee-paying for private entities. To ensure a trusted and secure environment, banks, insurers, securities firms and financial market infrastructures seeking membership require FINMA authorization. In addition, the FS-CSC recently acquired the services of the Financial Services Information Sharing and Analysis Centre (FS-ISAC), a global trusted provider of cybersecurity services, to support the operations of the Operational Cybersecurity Cell.

Lifespan and funding arrangements

The lifespan or duration of a specific public-private partnership or collaboration can vary significantly. Those identified in the report are generally permanent or open-ended models of collaboration (e.g., critical infrastructure sector ISACs or other threat intelligence sharing platforms). Some have a very specific duration, for instance, **rapid response arrangements,** annual **cybersecurity awareness months**, or festivals such as the **Czech Republic**'s annual **Internet Security Festival**. The lifespan of others may well be determined by the immediacy, scope and scale of the threat, by budgetary cycles and the overall availability of resources.

Ensuring adequate funding, is of course, key to any form of collaboration, and as mentioned, available funding will generally dictate the duration of any given initiative. Including references to such forms of collaboration in national security strategies as well as more specific detail in associated action plans helps ensure adequate allocation of resources, as well as identify where additional budgetary allocations may be necessary and where burden sharing with private entities may be most useful. Out of the public-private collaborations identified by participating States, many are government-funded through specific budgetary allocations. Others – generally those initiated by industry actors – tend to be funded by private entities or through membership, events or other such fees. Yet others involve the pooling of different types of resources. These sources of funding can change over time as the arrangement matures. Take, for example, cybersecurity clusters. In some instances, they start off with government funding, although the overarching aim of most clusters is to ensure independence through financial contributions from all participating entities and through other forms of fund raising such as membership fees and events. Some also pool resources, such as workspaces, often in locations other than capital cities, as in the **Hague Security Delta Campus**, which in turn can help promote the value of such locations in strengthening cybersecurity and resilience, while also ensuring efficiency, fostering employment at regional or local levels and attracting investment.

In the case of the **Cybersecurity Network Foundation (CSN) in Serbia**, the OSCE Mission to Serbia provided part of the seed funding for the initiative. Formerly known as the 'Petnica Group', CSN is an independent foundation whose main goal is to bring together stakeholders from across society to exchange information and pool ideas. It facilitated consultations leading to the development of several legal documents in the field of information security in Serbia, including the country's National Information Society and Security Development Strategy (2021-2026), which has highlighted the importance of cybersecurity-related public-private collaboration. With the agreement and support of competent authorities, the Cybersecurity Network Foundation implements the 'Cyber Hero' educational program and organizes the national cybersecurity competition 'Serbian Cybersecurity Challenge'. Efforts are currently underway to secure more sustainable sources of funding, including at national and regional (EU) level.

Monitoring and oversight

The growing focus on the importance of cybersecurity-related public-private partnerships and other such arrangements to national interests and national security, and growing investment in these mechanisms requires greater focus on regularly measuring and reviewing their performance.

Monitoring entails the continuous and systematic assessment of a given project or initiative based on the goals that have been agreed, the activities that have been planned and how they are implemented, and the information that is collected along the way. It enables effort to assess in a systematic and objective manner, the relevance, performance, impact, success, or lack there-of, and sustainability of the project or initiative in accordance with stated objectives. Oversight is particularly important when public funds are involved in the collaboration.

For some OSCE participating States, monitoring and evaluation are often part of their national cybersecurity strategy implementation plan and entail detailed reporting requirements. Efforts in this area continue to mature.

Other, looser forms of engagement may not be so rigorous, but being able to articulate their value in contributing to agreed goals is nonetheless important. Regardless of the type of collaboration and whether it stems from a national cybersecurity strategy, some participating States have noted that they often face challenges in assessing the value of their engagements with the private sector, and they may not always have a complete picture of what they entail and how they are contributing to the goals set out in their national cybersecurity strategy. Due to increasing requirements and the need to prioritize effort and resources, some participating States are currently reviewing their existing public-private collaborations, including through an extensive review of memorandums of understanding or agreements with private sector entities.

For traditional, contract-based infrastructure public-private collaboration, numerous tools and mechanisms are used for monitoring and oversight purposes. Lessons from these can be drawn for cybersecurity-related public-private partnerships and other such arrangements, particularly in the absence of formal reporting obligations. They include tools such as proactive disclosure, a process through which non-sensitive data is disclosed throughout the lifecycle of a given partnership or collaboration so that content, scope, and progress of the collaboration (not the content of what is discussed) is accessible and available to everyone. This kind of structured access to data can help enhance confidence in the project, by providing a means for government, industry and other non-government actors to monitor performance, analyze cost-benefit ratios, identify new opportunities for collaboration, as well as prevent fraud and corruption.

Other developments in this area involve collaborative approaches to supporting and overseeing government national cybersecurity strategy implementation. The **Austrian Cyber Security Platform** plays such a role. The body acts as an umbrella for the permanent exchange of information between public administration and representatives of the economy, science and research with all stakeholders taking part on an equal footing. It consists of some 100 individuals from across critical sectors that voluntarily self-organize into different sub-groups to assist and advise different projects, such as drafting the national cybersecurity strategy or providing input to Austria's position ahead of relevant international meetings and negotiating processes. In addition, the Platform has the remit to advise and support the national **Cyber Security Steering Group**. It also meets with the government at regular intervals to report on the implementation of the national cybersecurity strategy from the perspective of the private sector.

People

Cybersecurity-related PPPs and other such arrangements require clarity about who should be involved and for what purpose. This involves clear articulation of:

- The stakeholders involved and their roles and responsibilities within the arrangement.
- Whether the arrangement is open to all interested parties or restricted to a smaller or targeted group.
- How those involved are expected to contribute to meeting the goals of the arrangement.
- Whether specific expertise or dedicated functions may be required to facilitate relationship building between the public and private sector actors involved.

Participation or membership in a public-private partnership or other such arrangement will always be contingent on the purpose and aim of the actual arrangement. In OSCE participating States, they can involve just one public authority (e.g., a National Cyber Security Centre) or several. These 'several' tend to be ministries of (or agencies under) Justice, Interior, Defense, Education, Digital Transformation, Treasury/Finance, Emergency/Disaster Planning and Recovery. On the private side, key stakeholders can include multinational technology companies, telecommunications companies, internet service providers, cybersecurity companies, owners and operators of critical infrastructure and other essential assets and services, SMEs, individual experts and even individuals acting in their personal capacity.

It is important to note that some participating States take an even broader approach to such arrangements. Relevant initiatives may include academia, technical institutes or bodies, specialized civil society organizations or the entire population of a country. This tends to be the case where education and capacity-building are concerned. For example, in **Italy**, in line with specific provisions laid out in the National Recovery and Resilience Plan, the National Cyber Security Strategy and a recently approved law on post-secondary education, efforts are underway to develop a **Co-ordination Network of Higher Technological Institutes (ITS - Istituti Tecnologici Superiori)** for the development of a digital transition and of a national ecosystem to train new digital skills. The collaboration will involve several institutions, both at the national and at the regional level, and aim to develop the ITS, which represent a tertiary education segment run as a result of co-operation between local administrations, schools and industry, with the participation of universities. The ITS system, created a decade ago, is still small in size and the initiative has the goal of promoting its growth, especially in cybersecurity.

The purpose of the arrangement will also determine whether it is open to all interested parties, or closed, requiring participating entities or individuals to meet certain criteria. Sometimes the character of the private entity – whether it is multinational or foreign – may dictate whether its personnel can participate in a given national arrangement or not. National security-related considerations – and, increasingly, national legislation – tend to inform such decisions. Again, non-disclosure agreements and similar arrangements are viewed as important tools for enabling this form of co-operation.

The shifting threat and regulatory environments are propelling several participating States to enhance co-ordination amongst government authorities and review existing memorandums of understanding and associated partnerships and arrangements with the private sector to ensure better prioritization and use of resources. In some instances, dedicated positions have been established within the government to specifically co-ordinate a government's co-operation with the private sector on cybersecurity-related issues. This is the case, for instance, of the **Czech Republic** and **the Netherlands**, where preparations are underway for working with a much broader body of private sector entities under the NIS2 Directive.

Concluding remarks

A starting point of OSCE engagement on cybersecurity-related PPPs was the outcome of the report of the CBM 14 group in 2021. This report on emerging practices serves as a follow-up. Its recommendations are organized under the rubrics of **purpose**, **policy**, **process** and **people**. These represent recommended baselines for how government entities, together with the private sector, can determine the purpose of the relationship (the *why*); what it will focus on (the *what*); the modalities or structure of the arrangement (the *how*) and who should be involved (the *who*).

The report demonstrates how engagement with the private sector is becoming a prominent feature of strengthening cybersecurity and resilience across OSCE participating States. The sheer number of collaborative arrangements presented by participating States throughout the development of the report demonstrates how such relations are both normalizing and maturing, as well as building confidence within and across different communities.

At the same time, participating States interviewed throughout the process were candid about the scope and scale of cybersecurity and resilience challenges they face. They have signaled significant interest in learning more about how other participating States and other regions collaborate with the private sector to overcome challenges such as working collaboratively with SMEs, research institutes or specific critical infrastructure sectors; on establishing and maintaining trusted and secure platforms for information exchange; on capacities for rapid response; on incentive-accountability structures in cybersecurity-related public-private partnerships; and on monitoring and oversight of such arrangements. Importantly, participating States are also interested in hearing the views of private sector partners in such arrangements. In this regard, the examples submitted by participating States to inform this report are a treasure trove for future exchanges at the bi-lateral, regional and international levels across a number of different areas.

ANNEX I:

Purpose, Policy, Process, People

Purpose (general)

Cybersecurity-related public-private partnerships (PPPs) and other such arrangements should have a clearly defined purpose. This requires:

- A clear understanding of the national cybersecurity ecosystem.
- A clear understanding of the strengths and weaknesses of relevant public and private sector entities in the country vis-à-vis the cybersecurity and resilience challenges that need to be addressed.
- Identifying areas in which public-private co-operation could address identified challenges.
- Identifying how to incentivize engagement of relevant private sector and other actors.
- Identifying whether a dedicated government position for facilitating or co-ordinating relations between the public and private sector needs to be established.

Policy

Cybersecurity-related PPPs and other such arrangements should be clearly outlined in national policy and/or legislation. This requires:

- Acknowledgement of the importance of public-private arrangements in national cybersecurity policy and strategy, including through the articulation of how the arrangement will contribute to attaining national security, economic and social development goals, details of which can be included in related action plans.
- Consultation with relevant private entities in policy, legislative and regulatory decisions that will affect them.
- A commitment to establishing transparency and oversight mechanisms for public-private arrangements and related activities.

Process

Cybersecurity-related PPPs and other such arrangements require clear implementation modalities or governance structures to help ensure that goals are met and that appropriate incentive-accountability structures are considered from the outset. This includes joint confirmation by the public and private actors involved on:

- The specific goals of the arrangement and the specific problems it is setting out to solve.
- The activities that the arrangement will undertake to attain the agreed goals.
- Lifespan and funding sources.
- Security or non-disclosure requirements and protocols that need to be put in place and the cyber hygiene practices that need to be promoted amongst participants.
- Mechanisms for monitoring and oversight of activities undertaken.
- Mechanisms for reviewing and updating implementation modalities or governance structures of the overall PPP/arrangement.
- Communications/outreach strategy.

People

Cybersecurity-related PPPs and other such arrangements require clarity about who should be involved and for what purpose. This involves clear articulation of:

- The stakeholders involved and their roles and responsibilities within the arrangement.
- Whether the arrangement is open to all interested parties or restricted to a smaller or targeted group.
- How those involved are expected to contribute to meeting the goals of the arrangement.
- Whether specific expertise or dedicated functions may be required to facilitate relationship building between the public and private sector actors involved.

ANNEX II:

OSCE Permanent Council Decision No. 1202

PC.DEC/1202
10 March 2016

Organization for Security and Co-operation in Europe Permanent Council

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202

OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs.

The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

1. Participating States will voluntarily provide their national views on various aspects of national and transnational threats to and in the use of ICTs. The extent of such information will be determined by the providing Parties.

PCOEW6464

2. Participating States will voluntarily facilitate co-operation among the competent national bodies and exchange of information in relation with security of and in the use of ICTs.

3. Participating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity.

4. Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

5. The participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.

6. Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

7. Participating States will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

8. Participating States will nominate a contact point to facilitate pertinent communications and dialogue on security of and in the use of ICTs. Participating States will voluntarily provide contact data of existing official national structures that manage ICT-related incidents and co-ordinate responses to enable a direct dialogue and to facilitate interaction among responsible national bodies and experts. Participating States will update contact information annually and notify changes no later than thirty days after a change has occurred. Participating States will voluntarily establish measures to ensure rapid communication at policy levels of authority, to permit concerns to be raised at the national security level.

9. In order to reduce the risk of misunderstandings in the absence of agreed terminology and to further a continuing dialogue, participating States will, as a first step,

voluntarily provide a list of national terminology related to security of and in the use of ICTs accompanied by an explanation or definition of each term. Each participating State will voluntarily select those terms it deems most relevant for sharing. In the longer term, participating States will endeavour to produce a consensus glossary.

10. Participating States will voluntarily exchange views using OSCE platforms and mechanisms inter alia, the OSCE Communications Network, maintained by the OSCE Secretariat's Conflict Prevention Centre, subject to the relevant OSCE decision, to facilitate communications regarding the CBMs.

11. Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals from the Consolidated List circulated by the Chairmanship of the IWG under PC.DEL/682/12 on 9 July 2012, subject to discussion and consensus agreement prior to adoption.

The following CBMs were first adopted through Permanent Council Decision No. 1202 on 10 March 2016:

12. Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or subregional level; this is to investigate the spectrum of co-operative measures as well as other processes and mechanisms that could enable participating States to reduce the risk of conflict stemming from the use of ICTs. Such activities should be aimed at preventing conflicts stemming from the use of ICTs and at maintaining peaceful use of ICTs.

With respect to such activities participating States are encouraged, inter alia, to:

– Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;

– Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and

– Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.

PCOEW6464

13. Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.

14. Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.

15. Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures to discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies.

Collaboration may, inter alia, include:

– Sharing information on ICT threats;

– Exchanging best practices;

– Developing, where appropriate, shared responses to common challenges including crisis management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure;

– Adopting voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident;

– Sharing national views of categories of ICT-enabled infrastructure States consider critical;

– Improving the security of national and transnational ICT-enabled critical infrastructure including their integrity at the regional and subregional levels; and

– Raising awareness about the importance of protecting industrial control systems and about issues related to their ICT-related security, and the necessity of developing processes and mechanisms to respond to those issues.

16. Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated

information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region. OSCE participating States agree that such information exchange, when occurring between States, should use appropriately authorized and protected communication channels, including the contact points designated in line with CBM 8 of Permanent Council Decision No. 1106, with a view to avoiding duplication.

Practical Considerations[1]

The provisions of these Practical Considerations do not affect the voluntary basis for the activities related to the aforementioned CBMs.

Participating States intend to conduct the first exchange by October 31, 2014, and thereafter the exchange of information described in the aforementioned CBMs shall occur annually. In order to create synergies, the date of the annual exchanges may be synchronized with related initiatives participating States are pursuing in the UN and other fora.

The information exchanged by participating States should be compiled by each of them into one consolidated input before submission. Submissions should be prepared in a manner that maximizes transparency and utility.

Information may be submitted by the participating States in any of the official OSCE languages, accompanied by a translation in English, or only in the English language.

Information will be circulated to participating States using the OSCE Documents Distribution system.

Should a participating State wish to inquire about individual submissions, they are invited to do so during meetings of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039 or by direct dialogue with the submitting State making use of established contact mechanisms, including the email contact list and the POLIS discussion forum.

The participating States will pursue the activities in points 9 and 10 above through existing OSCE bodies and mechanisms.

The Transnational Threats Department will, upon request and within available resources, assist participating States in implementing the CBMs set out above.

1 First adopted as part of Permanent Council Decision No. 1106 on 3 December 2013

In implementing the CBMs, participating States may wish to avail themselves of discussions and expertise in other relevant international organizations working on issues related to ICTs.

Considerations[2]

Participating States will, at the level of designated national experts, meet at least three times each year, within the framework of the Security Committee and its Informal Working Group established by Permanent Council Decision No. 1039, to discuss information exchanged and explore appropriate development of CBMs. Candidates for future consideration by the IWG may include inter alia proposals for CBMs aimed at increasing transparency, co-operation, and stability among States in the use of ICTs. Such efforts should, to the extent that they relate to the mandate of the IWG, take into account and seek to complement the expert-level consensus reports of the 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including their recommendations on voluntary CBMs, and the Group's work in support of voluntary non-binding norms, rules and principles of responsible State behaviour in the use of ICTs.

The Transnational Threats Department of the OSCE Secretariat, through its Cyber Security Officer will, upon request and within available resources, assist participating States in implementing the CBMs set out above, and in developing potential future CBMs.

2 First adopted as part of Permanent Council Decision No. 1202 on 10 March 2016.

Follow OSCE

OSCE Secretariat
Transnational Threats Department
Wallnerstrasse 6
1010 Vienna, Austria

Organization for Security and Co-operation in Europe

cybersec@osce.org
www.osce.org/secretariat/cyber-ict-security