POLICY BRIEF NO. 4

ACHIEVING COMPREHENSIVE AND CONSISTENT EU CYBERSECURITY POLICIES

The challenge: Building coherent EU cybersecurity policies

Over the past few years, numerous policies and regulatory measures concerning cybersecurity have been adopted on EU level. They focused predominately on the areas of internal market and criminal justice in order to advance the security of citizens, businesses, and public administrations in the digital environment. However, there is lack of consistency in these policies and regulations, leading to a multitude of overlapping, but also conflicting obligations. A recent example for this lack of consistency is the European Commission's proposal for law enforcement authorities to have cross-border access to data (e-Evidence). The study analysing this proposal found that the increased cooperation regime allowing swift access of EU member States to provider data would obstruct Member States (MS) 'from taking responsibility for an effective protection of fundamental rights within its territory', and would cause legal uncertainty for both service providers and individual users.

Policy documents and legislative measures often concern only certain aspects of the cybersecurity domain and are adopted without considering them in the overarching legal framework.

Evolving 'cybersecurity' concept

It is often suggested that it is hard to attain consistency in policies concerning cybersecurity due to the existing different ways to understand cybersecurity and its scope. Numerous definitions of 'cybersecurity' are used at EU and national level by EU institutions, stakeholders, and EU Member States. The definitions of cybersecurity vary and depend on the addressee, context, and policy area in which they are employed. In EU cybersecurity, discussions may include various aspects like cyber resilience, cybercrime, cyberdefence, cybersecurity in the narrower sense, and other global cyberspace issues.

However, policy documents and legislative measures often concern only certain aspects of the cybersecurity area and are adopted without considering them in the overarching legal framework. Examples of such chunks include areas of cybercrime, network and information security measures (targeting operators of

THE EU AND ITS MEMBER STATES DEFINE CYBERSECURITY DIFFERENTLY

For example, the Cybersecurity Strategy of the European Union of 2013 gives the following definition: 'Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.' In contrast, the EU Member States developed cybersecurity definitions at national level that capture domestic approaches to address cybersecurity challenges and threats. For instance, the Czech Republic Cybersecurity Strategy for the period of 2015-2020 states that 'Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace [...]'. The Luxembourg National Cybersecurity Strategy III 2018 states that cybersecurity 'is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets.', while focusing on the protection goals availability, integrity and confidentiality. Other countries have widely varying definitions in their policy documents as well, ranging from very limited scopes to globally encompassing ones.

essential services, or providers of critical and digital infrastructures), and electronic communication, which includes matters of privacy and data protection. Attempts of conceptualising cybersecurity have been further complicated by blurring boundaries between different cybersecurity domains. The different meanings of the term 'cybersecurity' can have both advantages and disadvantages. The term has flexibility to adapt to changing circumstances. At the same time, an ever-evolving term can become overly inclusive or broad, obstructing and hampering coherent regulation in this area. It also causes friction between EU and Member States power, especially in the national security domain. Therefore, the ambiguity of the term 'cybersecurity' in the EU should be addressed to clarify regulatory institutional responsibilities.

Lack of EU competence for cybersecurity regulation

The challenge of creating comprehensive and consistent cybersecurity policies is furthered by uncertain EU competence to legislate on cybersecurity matters. The EU only has the competence conferred on it by the Member States in the Treaties. It may have exclusive competence, shared competence, or competence to take supporting, coordinating, or supplementary action. Since cybersecurity is not mentioned as part of any existing field, the EU seeks for permissible legal justification for cybersecurity regulatory measures in established policy areas. For example, the European Commission proposal for 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 (NIS Directive) argued that that the diverse Member States' practices with regards to cybersecurity measures hinder the protection awarded to consumers and business, thus reducing 'the overall level of security of network and information systems'. In other words, it suggested that additional (cyber) security measures are necessary. This ambiguous usage of the term 'cybersecurity' in several EU policies and measures is not accidental. It may suggest that there is a 'competence problem', which is pivotal to the relationship between the EU and its Member States. The recognition of internal, external, and also defence dimensions of cybersecurity requires careful consideration of the EU competence allocation by EU Member States, as well as the interpretation of the EU competence by the institutions.

Promoting cooperation between stakeholders

Combating cybersecurity threats must be recognized as a matter that requires the expertise and cooperation of stakeholders within different domains, such as IT, psychology, law, education, business, and policy. The EU already embraces such a multi-stakeholder approach with initial involvement of public and private sectors, including national governments, internet providers, technology and security firms, businesses, and civil society in order to tackle cybersecurity threats. However, such cooperation could be furthered.

Institutional cooperation on EU level

On EU level, a number of EU institutions, agencies and services are already focused on cybersecurity issues, such as the EC Directorate Generals (e.g., DG CONNECT, DG for Mobility and Transport, and DG Joint Research Centre). While some efforts have been made already to establish cooperation between those DG and different units within, some of these are informal practices only, while those already governed by formal policies have not yet unfolded their full potential. Moreover, due to the ever-increasing importance and reliance of societies on ICT, it is to be expected that the number of DGs concerned with cybersecurity matters will grow continuously. The EU institutions and bodies working on different aspects of cybersecurity policy already aim to cultivate their cooperation through both formal and informal ways, such as networks of specialised experts, conferences and multi-stakeholder gatherings. Yet, for the success of any multi-stakeholder approach, a more comprehensive governance structure is prerequisite. So far, efforts to establish institutional cooperation have been mostly inconsistent, incomplete and not efficient enough. Therefore, future policy initiatives should differentiate roles, competences, and mission goals of involved domains and actors in a clear manner. This is especially important with respect to the decision whether to pursue rather offensive or rather defensive cybersecurity strategies. An example for such a decision would be the debates around the use of so-called lawful access, meaningful encryption without backdoors, or zero-day exploits. Thereby, the European Union should try to earnestly address concerns with respect to potential weakening of the whole IT security landscape, privacy and data protection as well as Human Rights in general. The advice would be to involve security experts, data protection authorities, human rights advocates and the general public when shaping a more refined balance between the needs of law enforcement and citizens' rights. The recently adopted Cybersecurity Act is positive development, as it at least clarifies the governance structure by spelling out different roles of the ENISA - it consults the EC on cybersecurity matters, provides a focal point of know-how, thereby facilitating cooperation and coordination among different stakeholders.

Institutional cooperation on national level

The 2013 and 2017 EU Cybersecurity Strategies call for a comprehensive approach towards cybersecurity protection. This also concerns national approaches to cybersecurity. The cooperation mechanisms extending from the EU level to the Member States' institutions could be further improved. While various cooperation groups, such as the European Data Protection Board, the Body of European Regulators for Electronic Communications (BEREC) exist, some of them are seriously understaffed, or lack the full potential of their efficiency due to difficulties in involving all relevant actors sufficiently. In some cases, entities and regulators having responsibilities over different areas of cybersecurity within a country do not have effective communication practices. For instance, the know-how and information exchange between CERTs and law enforcement authorities on national level could still be improved. Yet when addressing this issue, Member States should be encouraged to establish more coherent information exchange rules and mechanisms in accordance with EU values and citizen's fundamental rights. While most Member States developed their first cybersecurity strategies before the adoption of the NIS Directive, it may further help in detailing the governance framework on national level by defining roles and responsibilities of stakeholders in the public and private sectors. When considering changes needed to facilitate effective cooperation in cybersecurity matters, the highest standards of the rule of law and

protection of fundamental rights should be followed. This is especially crucial for the areas of law enforcement and criminal procedure, where a careful balance needs to be struck between interests of states, societies and individuals. Consequently, policy makers should develop a clear understanding of limitations to cooperation concerning cybersecurity matters on the basis of legality and judicial principles, and try to preserve coherence across several legislative frameworks.

Where more info can be found

This Policy Brief is based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity). Detailed reports of this work have been published in four main White Papers:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Opinions Regarding Cybersecurity
4. Technological Challenges in Cybersecurity

All White Papers can be found on our website, along with all of our (downloadable and printable) Policy Briefs, short online explanations of the key cybersecurity issues, and commented literature lists for further reading:

canvas-project.eu

Moreover, you can find even more CANVAS project material on our website:

CANVAS Reference Curriculum
(integrating the value perspective into cybersecurity training and education)

CANVAS MOOC
(Massive Open Online Course)

Open Access Book
"The Ethics of Cybersecurity"

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Objective of CANVAS:
To bring together stakeholders from key areas of the European Digital Agenda to approach the challenge how cybersecurity can be aligned with European values and fundamental rights.

Partners:
The CANVAS Consortium consists of 11 partners (9 academic institutions and 2 partners outside academia) located in 7 European countries.

Version and date of publication:
Version 2.0, October 2019

Funding:
1.57 Mio. €, of which 1 Mio. € is funded by the European Commission and the remaining part emerges from the Swiss State Secretariat for Education, Research and Innovation.

Project coordination and contact:
PD Dr. sc. ETH Markus Christen, University of Zurich (UZH), Digital Society Initiative, Rämistrasse 66, 8001 Zürich

Project duration:
September 2016 – October 2019