POLICY BRIEF NO. 4

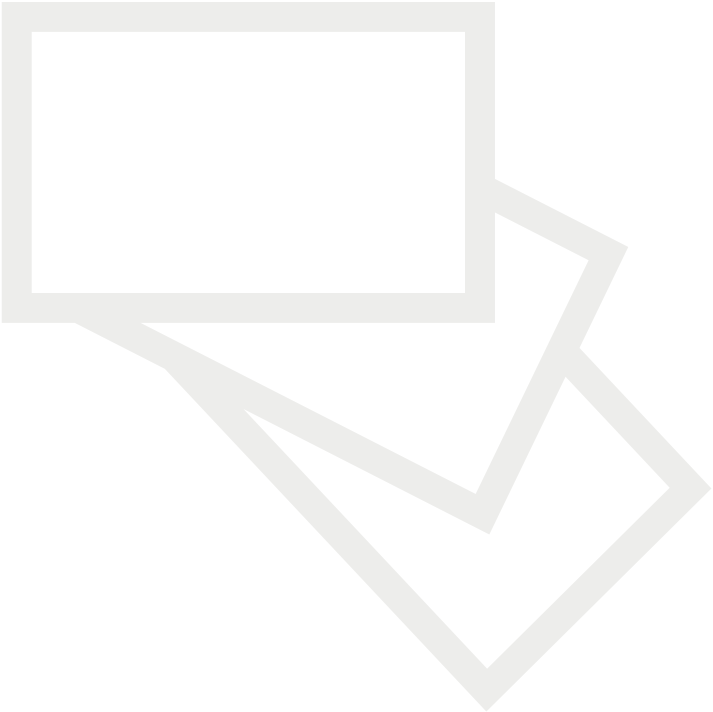
ACHIEVING COMPREHENSIVE AND CONSISTENT EU CYBERSECURITY POLICIES

The challenge: Building coherent EU cybersecurity policies

There is a lack of consistency in EU cybersecurity policies and regulations, leading to a multitude of overlapping, but also conflicting obligations.

Over the past few years, numerous policies and regulatory measures concerning cybersecurity have been adopted on EU level. So far, they focused predominately on the areas of internal market and criminal justice in order to strengthen the security of citizens, businesses, and public administrations in the digital environment.

However, these **policy efforts often lack consistency and a sufficiently coherent view on issues** tied to cybersecurity policies. This is something that should be addressed.



Direct cooperation between EU Member States can weaken fundamental rights protection

When shaping cybersecurity related policies, care must be taken not to cause unintended and negative side effects, especially with regard to the protection of EU citizen's fundamental rights. This can under circumstances provide for a challenging task. A recent example of this is the European Commission's proposal for law enforcement authorities to have cross-border access to data (so-called e-Evidence).

A study by the European Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE) analysed this proposal. It found that the increased cooperation regime allowing swift access of EU Member States to provider data would obstruct these states 'from taking responsibility for an effective protection of fundamental rights within its territory'. This would cause legal uncertainty for both service providers and individual users.

This is mostly caused by the proposal foreseeing a re-allocation of protective functions from EU Member States towards service providers and/or the competent authority, which effectively weakens fundamental rights protection of individuals. It seems advisable that the further legislative process should address this concern.

The concept of ‘cybersecurity’ is still evolving

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

It is often suggested that it is hard to attain consistency in policies concerning cybersecurity due to the existting different ways to understand cybersecurity and its scope.

Numerous definitions of ‘cybersecurity’ are currently used, at EU level, as well as on national level through EU institutions, stakeholders, and in Member States.

These definitions of cybersecurity vary and depend on the addressee, context, and policy area in which they are employed.

EU cybersecurity, discussions may include various aspects with further own, specific, and complex issues, like cyber resilience, cybercrime, cyberdefense, cybersecurity in the narrower sense, and other global cyberspace issues.

The different meanings of the term ‘cybersecurity’ can have both advantages and disadvantages.

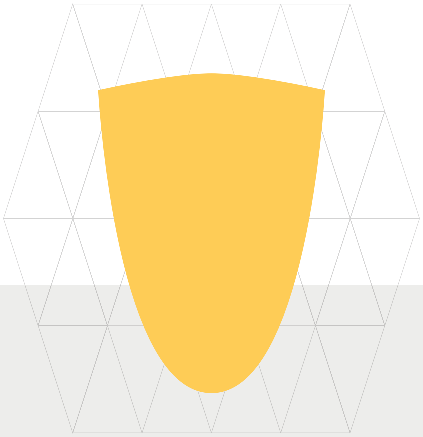
- It has **flexibility** to adapt to changing circumstances, but…
- …it is also **causing friction** between the EU and Member States‘ power, especially in the national security domain…
- Moreover, when such a term is constantly evolving, the **scope remains unclear**. It can become overly inclusive or broad, obstructing and hampering coherent regulation in this area.
- **The ambiguity of the term ‘cybersecurity’ should be addressed** to clarify regulatory fragmentation as well as the institutional responsibilities.

Cybersecurity is multi-faceted, affecting many areas

Some exemplary aspects of cybersecurity policy areas are cybercrime, network and information security measures, as well as electronic communications. Many of them have also impact on the European data protection framework.

Health

Business



Police and National Security

Attempts of conceptualising cybersecurity have been further complicated by the **blurring boundaries between different** cybersecurity domains, which are linked to the factual professional expertise required, such as for instance security engineering, operational security and vulnerability management, or IT security frameworks and standards.

The EU and its Member States define ‘cybersecurity’ differently

Other countries have widely varying definitions in their policy documents as well, ranging from very limited scopes to globally encompassing ones.

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 own 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 […]’.

As another national example serves the **Luxembourg National Cybersecurity Strategy III 2018,** which 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.

Uncertainty over the 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. Depending on context and interpretation, it may have exclusive competence, shared competence, or competence to take supporting, coordinating, or supplementary action.

Since cybersecurity cannot be exclusively allocated to one specific policy area, the EU should continuously seek **clarification of legal justifications for cybersecurity regulatory measures** in established policy areas.

Who is regulating all matters of cybersecurity?

A careful consideration of competence questions is required to effectively address the internal, external, and also defence dimensions of cybersecurity.

The EU has come to use the term 'cybersecurity' very carefully. An example is the European Commission's proposal for the NIS Directive (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). This proposal argued that that the diverse Member States' practices with regard to cybersecurity measures hinder the protection awarded to consumers and business, thus reducing 'the overall level of security of network and information systems'. With these words, the EC practically suggested that additional (cyber) security measures are necessary.

This suggests that the EU recognized that there may be a **'competence problem'**, which is pivotal to the relationship between the EU and its Member States.

Promoting cooperation between stakeholders

The struggle against severe cybersecurity threats must be recognized as a matter that requires the expertise and cooperation of stakeholders within different expert domains, for instance professionals from information technology, psychology, law, education, business, and policy areas.

The EU already embraces such a multi-stakeholder approach with initial involvement of public and private sectors.

This includes governmental institutions, 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).

Due to the 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.

But while some efforts have already been made to establish cooperation between the relevant DGs and different units within, these are often still informal practices. There is a **lack of formal policies governing cooperation and exchange** between these institutions.

Examples for current attempts to cultivate cooperation through both formal and informal ways are networks of specialised experts, conferences and multi-stakeholder gatherings. But still, with regard to the establishment of better institutional cooperation, efforts have been so far inconsistent, incomplete, and not particularly efficient.

Future **policy initiatives should differentiate between roles, competences, and mission goals of involved domains and actors clearly**. This is especially important with respect to the decision whether to pursue rather offensive or rather defensive cybersecurity strategies.

Institutional cooperation on national level

Various cooperation groups exist, such as the European Data Protection Board, or the Body of European Regulators for Electronic Communications (BEREC), exist. Know-how and information exchange practices between CERTs and law enforcement authorities on national as well as on international level exist, but these are not yet optimally established. Consequently, **action is needed to address understaffing and inefficiency of institutions** in order to involve all relevant actors sufficiently.

The 2013 and 2017 EU Cybersecurity Strategies have both called for a comprehensive approach towards cybersecurity protection. This involves national approaches to cybersecurity as well, which relates not only to the solely national level, but also to the interactions between the EU and its Member States.

Well-balanced strategic decisions are needed

Some examples for often quite controversially discussed topics in the context of offensive vs. defensive cybersecurity strategies are the debates around the use of so-called lawful access, meaningful encryption without backdoors, or zero-day exploits.

While these measures and tools can be deployed by security agencies to combat crime, they can have serious **negative collateral side effects**, such as general weakening the security of ICT systems for everyone.

When dealing with these issues, 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.

To advance coherent and value-driven cybersecurity policies, security experts, data protection authorities, human rights advocates and the general public should be involved. There is a need to **shape a more refined balance between the needs of law enforcement and citizens' rights**.

A positive example is the recently adopted Cybersecurity Act since it at least clarifies the governance structure by spelling out different roles of the ENISA. The ENISA consults the EC on cybersecurity matters, provides a focal point of know-how, thereby facilitating cooperation and coordination among different stakeholders.

Aim for value-driven cybersecurity

The highest standards of the rule of law and the protection of fundamental rights should be followed.

This is especially crucial for the areas of law enforcement and criminal procedure, as well as for cooperation and information exchange cases, where **a careful balance needs to be struck between interests of citizens, societies, and Member States**.

While most Member States developed their first cybersecurity strategies before the adoption of the NIS Directive, it may already help in detailing the governance framework on national level by defining roles and responsibilities of stakeholders in the public and private sectors. Thus, a careful eye should be kept on how well such legislative measures fit within the bigger picture.

Consequently, policy makers need to **develop a clear understanding of limitations to cooperation on the basis of legality and judicial principles**, and try to preserve coherence across several legislative frameworks.

Starting points for advanced cybersecurity policies

Recommended steps to mitigate inconsistencies in European cybersecurity policies:

Ensure that EU Member States always provide for the sufficient protection of the fundamental rights of individuals, especially with regard to the balance between security and personal data protection.

Agree EU-wide on a well defined common understanding of what 'cybersecurity' means and which expertise domains should be addressed when initiating new policy regulations.

Unambiguously resolve regulation competence uncertainties.

When allocating tasks and imposing obligations on institutions via policy, differentiate between roles, competences, and mission goals of involved domains and actors clearly.

Evaluate and improve information exchange practices.

Clarify the interrelations between state CERTs and private ones, and ensure that all of them follow data protection rules and ethical guidelines.

More information can be found

The slides are based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity).

The objective of CANVAS is 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.

In particular, we provide the following CANVAS resources:

- Briefing packages
- CANVAS Reference Curriculum
- CANVAS MOOC
- Open Access Book
  ‘The Ethics of Cybersecurity’

The following slide directly points to those of our White Papers which address in detail the challenges of cybersecurity.

Bibliography: cybersecurity challenges (CANVAS White Papers)

Ethical challenges

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Legal challenges

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technological challenges

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Project facts

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

Slidedocs version:
Version 2.0 October 2019

Project duration:
Sept. 2016 – Oct. 2019

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

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.

Funding notice for CANVAS

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 EU and the Swiss Government