Cybersecurity in the European Union:

Possibilities and perspectives

Aron James Miszlivetz

Catching up and stocktaking: The previous financial framework

The EU's previous 2014-2020 long-term financing framework (MFF) had little mention of the development of digital programs and lacked any specific mention of enhancing the cyber capabilities within the European Union. The Connecting Europe Facility in Heading 1 focused mainly on infrastructure and telecommunications development, high-speed optical internet. To close regional development gaps for digital infrastructure and accessibility, Cohesion Funds could also be used. What was lacking were clearly defined goals and programs regarding future technologies (the use of AI, 5G networks, quantum computing, defense against cyber threats), as well as facing the challenges that arrive from using such tools. Moreover, other international players such as the United States, Russia and China were more conscious of such technologies as the European Union was lagging behind in the last decade. Naturally, coordinating such efforts among 28, and recently with 27 members proved difficult, but not impossible. As we near a new post-Covid era, the challenges the Union is facing also shape its future, especially when one looks at the developments in the field of digital- and cyberspace.

The new 2021-2027 MFF was a real breakthrough, not only for brushing together national interests, but regarding the themes and scope of main strategic priorities the EU and its Member States wanted to develop for the future. The two parallel and converging roads the EU sought out are green and digital. To use sustainable technologies while also contributing to competitiveness and increased security within its borders, the former which further declined during the Covid-19 pandemic.

The main headings of the new financial framework are more streamlined and integrated. Previously *Competitiveness for Growth and Jobs* was renamed to *Single Market, Innovation and Digital*. As part of this new heading in the new budgetary cycle the Digital Europe program focuses extensively towards pursuing the digital transformation of public services and businesses through high-performance computing, artificial intelligence, improving digital skills and establishing cybersecurity. The latter, which remains at the core of EU policy, is not only part of the Commission's priorities in but is also part of the new recovery plan for Europe, the Next Generation EU , mentioned several times in the European Security Union Strategy, and is an integral part of Horizon Europe (FP9) for innovation.

What is new in the EU'S cyber landscape?

While the new recovery plan provides additional investments in cybersecurity due to an increase in disinformation and attacks on social systems mainly for SMEs, the Security Union Strategy focuses on establishing hard defense capabilities including establishing active evasive tools to counter cyber threats. Multiple legislative proposals are on the table soon to be adopted. The revision of the Network and Information Security Directive (NIS2) and the new Directive on the Resilience for Critical Entities (CER) constitute the legal bases for action.

Establishing trust is the first step towards any relationship. This is equally true for the EU institutions/agencies and the Member States. A network of Security Operation Centers to protect SMEs using AI capabilities as well as protecting the health, financial, infrastructural and energy sectors is one of these trust-building projects. Next to this, Digital Innovation Hubs would lead in the field of researching evolving and future threats. Joint Cyber Units would help establish trust in an early warning system to notify other EU Member States and the institutions in the event of an attack and step up in a coordinated way. In the military field, EU Member States are already working closely as part of the Permanent Structured Cooperation in the cyber landscape.

Interestingly, the Commission also proposed to enhance global cooperation with international partners regarding cyber threats to create new norms and standards through dialogues and diplomacy. In short, while the NIS2 will provide security to entities big and small, establishing uniform requirements and a sanctions regime across Member States. The CER will cover ten unique sectors and introduce regular risk assessments to shed light on deficiencies (involving a cross-sectorial approach).

The new Strategy also involves the issues of establishing secure and safe 5G networks in order to become technologically less dependent on third-party actors (e.g. China) in this field. This is the first step towards creating telecommunication networks that are secure and financially accessible for citizens across the Union.

Towards a new, global cyber diplomacy?

While the EU is physically present with around 140 delegations worldwide, its virtual presence is not all-encompassing. Therefore, the creation of a Cyber Diplomacy Network through dialogues with third countries, especially the EU Neighborhood remains an important step. It is necessary to create a common understanding of threat perception and create stronger regional cooperation in the cyber field. The Cyber Diplomacy Network aims to create such a forum. Last but not least, the establishment of an EU Domain Name System for individuals, businesses and enterprises (DNS4EU) would create more oversight in case of a malicious cyber-incident (e.g. denial-of-service attack). To put it in simple terms, it is aimed at creating a "European window" towards the internet, so one can see what happens outside and be informed of any intrusions.

The EU's cyberfuture

As the EU Cybersecurity Strategy was presented last December, during the March 2021 Council meeting, EU ministers adopted conclusions on this strategy. The Network of Security Operations Centers were agreed upon, as well as the definition of a Joint Cyber Unit and ensuring the use of stronger encryption channels. The visible impact for citizens would be a new EU cybersecurity certification framework in which digital and IT product (online and offline) would be certified as safe by the EU. For example a "smart appliance"

1083 Budapest, Ludovika tér 2. | +36 1 432 9150
POSTACÍM 1441 Budapest, Pf. 60. | rektor@uni-nke.hu, uni-nke.hu

would be certified only of it complied with the strictest privacy and anti-breach measures (privacy & security by design), reiterating the importance of the Budapest Convention on Cybercrime. In training the cyber experts of the future, the recently established European Cybersecurity Network and Competence Center in Romania will coordinate EUMS cyber centers as well as conduct research. Training skills will be offered as part of a Master course funded by the Commission.

While there is a lot of work to be done in the coming years, the EU is hopefully taking matters of its security seriously. Catching up to the international stage will take time and effort from Member States too. The result means that citizens will be better protected from foreign influence and can use secure channels of communication across the Union. Shaping cyberspace by "European design" is one step closer in becoming a serious partner to count with. While the level of fragmentation between Member States makes it difficult for attacks to affect all members equally, a secure technological and cyberspace will make it easier to evade such risks. This may also contribute to a swift adoption of digital technologies for companies that are not as equipped, thus increasing the economic competitiveness and citizens' well-being in the European Union.

20.04.2021

1083 Budapest, Ludovika tér 2. | +36 1 432 9150
POSTACÍM 1441 Budapest, Pf. 60. | rektor@uni-nke.hu, uni-nke.hu