Unveiling the significance of cyber resilience in the European Union

Eleni Kapsokoli
Μέλος ΑΛΛΗΛΟΝ
Post-doctoral Candidate, Department of International and European Studies of the University of Piraeus. Researcher, Laboratory of Intelligence and Cyber-security at the Department of International and European Studies of the University of Piraeus.
Eleni Kapsokoli | LinkedIn

Περίληψη

In an increasingly digitalized world, cyber resilience is a critical component of defence against the ever-evolving security landscape. While technological advancements play an essential role in enhancing and safeguarding the national digital infrastructure, promoting digitalization and interconnectivity in our society, cyberattacks have grown in both complexity and frequency. These threats demonstrate security vulnerabilities and emphasize the need for cyber resilience at national and international levels. By adopting a proactive and holistic approach to cybersecurity, states, entities, and users can enhance their ability to endure, respond to, and recover from cyber incidents, ensuring the continuity of their operations and safeguarding the integrity of sensitive data. This paper analyzes the reasons why cyber resilience has become paramount in the EU.

The digital transformation and interconnectedness of our society allow for greater flexibility and growth but reveal numerous cyber-threats that must be addressed swiftly and effectively. Almost all activities are based on information communication technologies and the exploitation of data which created unprecedented opportunities but also vulnerabilities. The emergence of new technologies (artificial intelligence, machine learning, big data, augmented reality, etc.) gradually transforms the society from a physical to a digital one. The only certain thing is that no matter how prepared a state or non-state actor is, there is always the possibility that they will be the target of a cyberattack. There is no immunity in cyberspace. When everything has become digital, such cyber-threats will have more serious consequences.

The reason for the above is that the toolbox and modus operandi of perpetrators are constantly evolving in sophistication and effectiveness. Cyber-threats have evolved from simple malware attacks to sophisticated and targeted cyber-espionage campaigns and Distributed Denial of Service (DDOS) attacks. The rise of ransomware, nation-state attacks, and supply chain vulnerabilities highlights the dynamic nature of cyber-threats.

The word 'resilience' in the field of cybersecurity has been carefully chosen by experts. Resilience is defined as the ability to (re)act in any condition, to recover quickly and effectively from a difficult situation, to be familiar with the environment in which one operates, and to review, adopt or develop new techniques to ensure the continuity of business or information environment. Cyber resilience refers to an organization's ability to anticipate, prepare for, respond to, and recover from malicious cyber activities while maintaining the continuous delivery of its essential services. This principle has become a

major strategic challenge for all actors.

In the last decades, significant cyber incidents have triggered the adoption or revision of existing policies and strategies from state and non-state actors to address these new security challenges and mitigate their impact. These cyberattacks unveiled the security vulnerabilities of critical national infrastructures and information systems and emphasized the development of the principle of cyber resilience. The COVID-19 pandemic significantly increased these threats and highlighted the critical importance of cyber resilience. With the sudden shift to remote work due to lockdowns and social distancing measures, organizations had to rapidly digitalize their activities. Cybercriminals took advantage of the fear and uncertainty surrounding the pandemic by conducting such attacks. The rapid adoption of new technologies and digital platforms during the pandemic often outpaced users' understanding of cybersecurity best practices. Many of them were not adequately prepared to defend against emerging cyber-threats. The consequences of such an incident can be disastrous, from loss of sensitive data to loss of customer trust and destruction of the organization's reputation. A puzzle piece filling in the cyber malicious landscape is the war in Ukraine (2022- till now) proved to be multidimensional since it is materialized not only on the physical battlefield but also in cyberspace by weaponing technology and information.

Cybersecurity remains a key factor, but cyber resilience is also pivotal and should be included in every relevant strategy, and crisis management plan. Achieving all the above requires preparation with training and simulations of human resources, recognition of threats, effective protection, adaptability according to circumstances, and assumption of responsibilities. Organizations should embrace resilience by developing a common mindset and culture. There is a need for multi-stakeholder collaboration (a range of international and national actors) through joint actions on enhancing cyber resilience through technical, financial, diplomatic, and legal ways. Adopting such an ever-increasing approach to risk also means that actors are aware of what is currently happening in cyberspace.

Facing these new challenges, the European Union (EU) has adapted to the new technological imperatives and challenges. The EU is becoming a global regulatory power and has recognized the growing threats arising from the nature of cyberspace. On the one hand, it adopted several measures and obligations, and on the other hand, it established institutions responsible for assisting member states in the field of cybersecurity, data protection and cyber-defence by strengthening internal cyber resilience. Even if member states have developed national cyber strategies, they adopted different approaches and capabilities regarding 'cyber-security', 'cyber resilience' and 'cyber defence'. So, there is an absence of a coherent approach among the member states (Kapsokoli, 2020, 378).

The EU Cybersecurity Strategy of 2017 stated that "We need a Europe that is resilient, which can protect its people effectively by anticipating possible cybersecurity incidents, by building strong protection in its structures and behaviour, by recovering quickly from any cyberattacks, and by deterring those responsible". This phrase underscores the main goal of the Union, which is the existence of multilayered resilience in cybersecurity (European Commission, 2017).

European institutions like ENISA (European Union Agency for Cybersecurity) further enhance the resilience of information systems and national critical infrastructures by developing the cyber-capabilities, know-how and technological autonomy of the Union (European Commission, 2020). NIS2 (Directive on Security of Network and Information Systems) aims to harmonize the European cybersecurity requirements, strengthen cyber resilience measures and capabilities for member states and effectively protect critical infrastructure (Official Journal of the European Union, 2022). The Resilience of Critical Entities (RCE) Directive mirrors NIS2 and necessitates a national strategy to increase the resilience of critical entities that provide state services (Official Journal of the European Union, 2022). Digital Operational Resilience Act (DORA) specifically points to the financial sector, aiming to establish a robust security framework at a European level and focus on addressing the critical aspects of cyber resilience (Official Journal of the European Union, 2022). The Cyber-diplomacy toolbox (2017) is the EU's joint international diplomatic response to malicious cyber activities and behaviour with the Union's key strategic partners (NATO, etc.). The cherry on top was the adoption of the new Cyber Resilience Act in September 2022, which will ensure that digital products which are on the European market have sufficient cybersecurity requirements and vulnerabilities can be dealt with more efficiently (European Commission, 2022). The Cyber Solidarity Act (2023) complements the EU's digital quiver which has as a main goal the strengthening of harmonization to mitigate the growing vulnerabilities by identifying, preparing for, and responding to cyber-threats within the EU. To do so, it is important to develop the capabilities of its member states based on resilience and exchanging best practices and information.

The EU is taking pivotal steps to foster cyber resilience and to establish close international cooperation and alignment of the actors with cybersecurity measures. All the above regulatory and policy efforts are commendable and demonstrate the strive for a more resilient Union. However, many member states are struggling to advance their digitalization and face challenges such as the lack of cyber professionals and non-developed cyber capabilities. This situation leaves small and medium-sized enterprises (SMEs) and less fortified public sector entities especially susceptible to cyber-threats. Often lacking the needed knowledge and technology, they struggle to mitigate the complexity of cyber risks. Brussels is committed to aiding member states in adopting the updated measures outlined in NIS2, DORA and CRA, but also by empowering ENISA's authorities to determine the most effective practices under the regulations and policies outlined in the NIS1.

To sum up, the essential role of cyber resilience in the modern digital landscape cannot be overpassed. Enhancing this principle across Europe and beyond demands a unified, continent-wide push to safeguard critical assets, alongside a globally coordinated strategy for response. Pan-European cyber resilience relies on the technical and organizational precautions of states, the available well-educated human resources, and effective cooperation mechanisms. Moreover, it focuses on the active engagement of the private sector, which must entirely embrace collaboration rather than avoid it. As cyberattacks continue to evolve in sophistication and frequency, organizations, states, private-public sector, and society must prioritize building resilience into their cybersecurity strategies, ensuring the continuity of their operations and safeguarding the confidentiality, integrity, and availability of sensitive data.

Bibliography

European Commission. (13 September 2017). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels.

European Commission. (16 December 2020). Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade.

European Commission. (15 September 2022). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.

European Commission. (18 April 2023). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

Kapsokoli, E. (2020). "European Union and Cybersecurity: Institutions and Strategies", in Daskalakis, I. (ed.) The Defence Integration of the European Union, Athens, Infognomon, (in Greek), pp.357-382.

Official Journal of the European Union. (27 December 2022). DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).