CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

JANUARY 2024

Cyber Resilience in the EU

Vaibhavi Katal

Edited by: D Sakshi

About the Author

Vaibhavi Katal is a under student at the Jindal School of International Affairs and is Research Assistant at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof. Dr. Pankaj K. Jha. Researchers at CSS explore both regional and thematic topics in the broader field of international security studies to write issue briefs, policy briefs, defence white papers, and dialogue session reports on contemporary issues. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource-related security issues; the proliferation of weapons of mass destruction; defence economics and the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:


www.linkedin.com/company/jindal-centre-for-security-studies/


www.instagram.com/css_jsia/


https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

IB2401007

Introduction

In a world driven by ubiquitous digital connections, the need for strong cyber resilience has become critical. The increasing dependence of communities and economies on networked technology, increases the susceptibility to cybercrime . This paper examines the critical need for cyber resilience, a comprehensive and adaptable approach for navigating the complex web of emerging cyber hazards. As we investigate the ever-changing nature of digital threats, it becomes clear that traditional cyber security paradigms are insufficient for fortifying nations, organisations, and individuals against the persistent and complex challenges that characterise the cyber realm.

Cyber resilience, as I understand it, is the ability to predict, tolerate, recover from, and adapt to unfavorable cyber circumstances. It entails a comprehensive strategy for safeguarding digital systems, that emphasises preventive measures, effective incident response, and continual adaptation to evolving threats. To achieve cyber resilience, a combination of technological solutions, risk management strategies, and organisational preparedness is required to ensure the ability to maintain essential functions, protect sensitive data, and quickly recover from cyber incidents, thereby minimising potential damage and ensuring operational continuity in the face of evolving cyber threats.

Cyber security employs encryption and firewalls among other technologies to safeguard one against attacks.. Resilience facilitates prompt recovery in the aftermath of an attack through the implementation of contingency plans and backups. To match plans with organisational objectives and legal requirements, governance sets up policies and monitoring.

What Led to the Need for Cyber Resilience?

The paradigm shifts of the 21st century ushered in a more globalized world where technology played a critical role fostering deeper connections between nations, cultures, and individuals.[1] Traditional boundaries have been dissolved by technological breakthroughs, notably in communication and information transmission, promoting unprecedented levels of interconnectedness and interdependence. The proliferation of mobile phones and the emergence of the internet has altered how we interact, share ideas, and do business on a global scale.

In this networked ecosystem, information flows effortlessly across boundaries, enabling real-time collaboration and the quick diffusion of knowledge.[2] Social media platforms, online collaboration tools, and digital communication channels have become essential components of our everyday lives, allowing us to interact beyond geographical boundaries. This interconnection has revolutionised not just the way people interact but also industries, economies, and societal institutions.

Furthermore, technology has accelerated the expansion of e-commerce, eliminating market barriers and giving customers access to items and services from all across the world.[3] Digital globalisation has created new opportunities for individuals and organizations to access a worldwide audience, stimulating international innovation and competitiveness. However, these potentials are accompanied by disadvantages, since growing connectedness exposes communities and people to new risks, notably in the field of cyber security.[4]

---

[1]Jamesr.faulconbridgeandjonathanv.beaverstock - Sage Publications Inc. (n.d.-b). https://www.sagepub.com/sites/default/files/upm-binaries/24132_19_Hollway_Ch_19.pdf

[2] *How smart, Connected Products Are Transforming Competition*. Harvard Business Review. (2020, September 10). https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

[3]Chaudhary, A. (2022, July 25). *Metaverse has potential to revolutionize e-commerce*. mint. https://www.livemint.com/opinion/online-views/metaverse-has-potential-to-revolutionize-ecommerce-11658743775928.html

[4](2014, February 10). *A survey of emerging threats in cybersecurity*. Journal of Computer and System Sciences. https://www.sciencedirect.com/science/article/pii/S0022000014000178

As the globe becomes more intertwined through technology, the necessity for a strong cyber security framework has become critical. In this hyper-connected world, dangers ranging from data breaches to ransom ware attacks pose risks to individuals, corporations, and even national security. Protecting digital infrastructure and guaranteeing safe information flow have become key imperatives for governments, corporations, and individuals alike. The task now is to find a balance between capitalising on the benefits of technology connections and strengthening our digital landscapes against increasing cyber threats. In managing this delicate balance, the value of international cooperation, agreed cyber security standards, and proactive cyber resilience measures becomes increasingly clear.

Why Has the Demand for Cyber Resilience Grown?

Nations across the globe have tapped into the need for cyber resilience as cyber threats have skyrocketed, especially in today's time. One of the recent examples is the hacker group 'Anonymous' that declared a 'cyber war' against Russian President Vladimir Putin after Russia invaded Ukraine.[5] As a result, the need for cyber resilience is widely recognised across the world, and several states outside of the European Union (EU) have taken efforts to address the expanding cyber threat scenario.[6] Countries like United States, Singapore, Australia, Canada, and others are seeing the significance of establishing a strong cyber resilience framework to protect key infrastructure, national security, and individual privacy.

[5] Jr., T. H. (2022, March 25). *What is anonymous? how the infamous "hacktivist" group went from 4chan trolling to launching cyberattacks on Russia*. CNBC. https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

[6] *Cybersecurity policies*. Shaping Europe's digital future. (n.d.-a). https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

After seven years since the first European Union strategy was published, the EU saw it as essential to take another step towards developing a stricter and stronger plan by issuing a new strategy act.[7] According to the opening paragraph of the new plan, "Cyber security is an integral part of Europeans' security. Whether it is connected devices, electricity grids, or banks, aircrafts, public administrations or hospitals they use or frequent, people deserve to do so within the assurance that they will be shielded from cyber threats. The EU's economy, democracy and society depend more than ever on secure and reliable digital tools and connectivity. Cyber security is therefore essential for building a resilient, green, and digital Europe."[8]

The growing need for cyber resilience in the European Union (EU) shows a growing understanding of the essential role cyber security plays in protecting the region's digital environment. As the EU faces a rise in digital transformation across industries, the frequency and sophistication of cyber-attacks are increasing.[9] As a result, comprehensive measures to maintain the resilience of digital systems, secure sensitive data, and reduce the effects of cyber disasters are now more relevant than ever before. "Thousands of cyber-attacks have inundated Europe's energy grid since Russia's invasion of Ukraine, and a top industry leader is calling for help as officials and researchers fret that not nearly enough is being done." Said Brussels.[10]

[7] Ibid

[8] Cybersecurity in the EU: An introduction - universidad nacional de ... (n.d.). https://blogs.uned.es/digitaleconomy/wp-content/uploads/sites/253/2022/01/Cybersecurity-in-the-EU-an-introduction.pdf

[9] A trusted and Cyber Secure Europe - enisa. (n.d.-a). https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

[10] Jack, V. (2023, November 26). *Europe's grid is under a cyberattack deluge, industry warns*. POLITICO. https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/

What Have the EU Government and Other Organisations Done?

Ever since Russia's renowned hacking organisation Fancy Bear has been targeting European countries with cyber-attacks, the EU's cyber emergency response team has alerted policymakers in a memo seen in POLITICO.[11] As a result, the EU introduced the Network and Information Systems Directive (NIS Directive), which went into force in 2018.[12] The NIS Directive mandates that critical infrastructure operators and digital service providers across the EU have a common degree of cyber security preparation.[13] These organisations are required to conform to risk management strategies, communicate significant events, and uphold a minimum level of security.

Furthermore, the EU has also been actively striving to improve collaboration and information sharing across member states through bodies such as the European Union Agency for cyber security (ENISA).[14] ENISA is critical to promoting collaboration and exchanging best practices to

[11] Roussi, A. (2023, November 27). *Russian hackers pose "high" threat level to EU, Bloc's Cyber Team warns*. POLITICO. https://www.politico.eu/article/threat-eu-high-russia-hackers-launch-cyberattacks-fancy-bear-election/#:~:text=Moscow's%20Fancy%20Bear%20group%20is,EU%20cyber%20response%20team%20warns.&text=Russia's%20notorious%20hacking%20group%20Fancy,a%20note%20seen%20by%20POLITIO

[12] *Press corner*. European Commission - European Commission. (n.d.). https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3651

[13] *Directive on measures for a high common level of cybersecurity across the Union (NIS2 directive)*. Shaping Europe's digital future. (n.d.). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive#:~:text=The%20Directive%20on%20measures%20for,them%20to%20be%20appropriately%20equipped

[14] *International strategy - enisa*. ENISA. (2021, November). https://www.enisa.europa.eu/publications/corporate-documents/enisa-international-strategy

improve the EU's overall cyber resilience.[15] The EU has also established a cyber security Competence Centre to encourage research and innovation in the field, ensuring that the region remains at the cutting edge of technical breakthroughs and security measures.[16] The European Union's council president and the European Parliament reached a provisional agreement on proposed cyber security legislation and later agreed to the EU's Cyber Resilience Act.[17]

The General Data Protection Regulation (GDPR) is considered the most rigorous privacy and security policy globally.[18] This regulation, stemming from the European Union (EU), imposes obligations on any organization that gathersdata about EU citizens.[19] On May 25, 2018, the regulation went into force.[20] The GDPR will impose severe penalties on anyone who breaks its privacy and security regulations, with fines exceeding tens of millions of euros.[21]

The GDPR reflects Europe's adoption of a rigorous approach concerning data privacy and security coincides with the growing prevalence of cloud storage for personal information and the escalating frequency of breaches. GDPR compliance is a scary proposition for small and medium-sized organisations (SMEs) since the law is vast, broad, and lacking in specificity.[22]

---

[15] *CISA and ENISA enhance their cooperation*. ENISA. (2023, December 12). https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

[16] *Eu gets Cybersecurity Competence Centre*. eucrim. (n.d.). https://eucrim.eu/news/eu-gets-cybersecurity-competence-centre/#:~:text=In%20order%20to%20pool%20expertise,relevant%20resources%20in%20the%20EU

[17] Mark Young, A. A. (2023, December 1). *The EU's Cyber Resilience Act has now been agreed*. Inside Privacy. https://www.insideprivacy.com/cybersecurity-2/the-eus-cyber-resilience-act-has-now-been-agreed/

[18] *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. (2023, September 14). https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU

[19] Ibid

[20] Ibid

[21] Ibid.

[22] Ibid.

The GDPR includes regulations for personal data security.[23] It necessitates the implementation of suitable technological and organisational safeguards to ensure the protection of personal data.[24] The Network and Information Systems Directive (NIS Directive) focuses on network and information system security in essential areas such as energy, transportation, healthcare, and digital infrastructure.[25] It necessitates the implementation of security measures and the reporting of important cyber security events by operators of essential services (OES) and digital service providers (DPS)[26].

The EU actively promotes cyber security innovation through a variety of measures.[27] Innovation techniques and technologies that improve digital security are supported by research and development programmes, public-private collaborations, and financing possibilities.[28] The EU fosters the creation of cutting-edge solutions by encouraging collaboration between business, academia, and government.[29]

---

[23] Castagna, R., & Lavery, T. (2021, January 29). *What is GDPR? an overview of GDPR compliance and conditions*. WhatIs. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

[24] Ibid

[25] Castagna, R., & Lavery, T. (2021, January 29). *What is GDPR? an overview of GDPR compliance and conditions*. WhatIs. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR

[26] Ibid

[27] *Cybersecurity policies*. Shaping Europe's digital future. (n.d.-a). https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[28] *Home*. The Digitalisation of Science, Technology and Innovation : Key Developments and Policies | OECD iLibrary. (n.d.). https://www.oecd-ilibrary.org/sites/b9e4a2c0-en/index.html?itemId=%2Fcontent%2Fpublication%2Fb9e4a2c0-en

[29] *IAC 2023 and GDA: Cutting-edge collaborative space solutions for a shared future*. GLOBAL DEVELOPMENT ASSISTANCE. (2023, October 24). https://gda.esa.int/2023/10/iac-2023-and-gda-cutting-edge-collaborative-space-solutions-for-a-shared-future/

The European Union uses state-of-the-art technologies to guarantee the safety of its citizens while accessing the internet..[30] Advances in artificial intelligence, machine learning, and secure communication protocols are examples of this. Embracing these technologies enables powerful security against emerging cyber threats, resulting in a safer online environment for both individuals and organisations.

Businesses and the EU work to improve cyber security through public-private partnerships. These programmes frequently involve collaborative research, information exchange, and the establishment of best practices.[31] These collaborations help to create a more resilient digital environment by pooling resources and knowledge.[32]Threat intelligence sharing forums are one example of public-private cyber security collaboration, in which government agencies and private sector organizations exchange information on emerging cyber threats.[33] Another example is collaborative public awareness campaigns aimed at educating the public about internet safety, in which corporations and government organisations collaborate to promote cyber security best practices.[34] Such collaborations highlight the responsibility for cyber security and show how collaborative efforts lead to a safer digital environment.[35]

---

[30]Cybersecurity: How the EU tackles Cyber Threats - consilium. (n.d.). https://www.consilium.europa.eu/en/policies/cybersecurity/

[31] *Public Private Partnerships (ppps)*. ENISA. (2022, November 11). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps

[32] *Cybersecurity policies*. Shaping Europe's digital future. (n.d.). https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[33] EU space policy and the involvement of Civil Society. (n.d.-b). https://www.eesc.europa.eu/sites/default/files/files/qe-04-23-899-en-n.pdf

[34] The role of awareness in adoption of government cyber security ... - diva. (n.d.-c). https://www.diva-portal.org/smash/get/diva2:1127292/FULLTEXT01.pdf

[35] *Who is responsible for cyber security?*. International Security Journal. (2023, August 9). https://internationalsecurityjournal.com/who-is-responsible-for-cyber-security/

Furthermore, awareness regarding cyber security was raised through various channels. Educational institutions provide formal cyber security training through courses and programmes.[36] Individuals can also educate themselves by using internet resources, workshops, and industry certifications. Awareness initiatives and outreach programmes also contribute to the general public's understanding of cyber security. Through extensive initiatives, the EU actively helps to make everyone secure online. Initiatives such as awareness campaigns to educate individuals about cyber risks and best practices fall under this category. The EU also funds cyber security education and research in order to create a more educated and resilient digital society. The EU aims to make the internet a safer place for everyone by developing a culture of cyber security awareness and expertise.[37]

How is the EU Creating Cyber Security Awareness?

The European Union (EU) takes a multifaceted approach to increasing public awareness of cybersecurity. First, it runs public awareness campaigns to inform people about common threats such as malware and phishing and provides helpful advice for safe online practices.[38] Second, it incorporates cybersecurity into formal education to raise awareness at different levels, such as

[36] (2021, June 16). *Cybersecurity awareness for children: A systematic literature review*. International Journal of Child-Computer Interaction. https://www.sciencedirect.com/science/article/pii/S2212868921000581

[37] *The importance of cyber security awareness in Education*. Cyber Security Awareness. (2023, September 12). https://terranovasecurity.com/blog/cyber-security-awareness-in-education/

[38] Apps, S. C. (2023, February 21). *Cybersecurity awareness: Definition, Importance & More*. Spanning. https://spanning.com/blog/cybersecurity-awareness/

schools and universities.[39] Finally, it offers online resources with information on password security and identifying cyber threats.[40]

Public-private partnerships promote collaborative efforts to solve cybersecurity concerns collectively, fostering information exchange and cooperative research. Legislative initiatives, such as the Network and Information Systems Directive (NIS Directive), require critical infrastructure operators to implement security measures, improving both cybersecurity and awareness.[41] Furthermore, EU research and innovation funding assures cutting-edge technology for consumers and enterprises, emphasising a shared responsibility for online security.

Conclusion

To summarise, the European Union (EU) has demonstrated an enduring dedication to promoting cyber resilience among its member states. The EU has worked to build a safe digital environment for citizens and companies alike through a complex strategy that includes legislation, awareness campaigns, education, and joint activities. The need to secure vital infrastructure such as the General Data Protection Regulation (GDPR), the Cyber Security Act, and the Network and Information Systems Directive (NIS Directive).

Notably, the EU acknowledges the significance of proactive measures, placing particular emphasis on the need for individuals to possess adequate knowledge and skills to securely navigate the evolving realm of cyberspace.Public awareness initiatives, instructional programmes, and the

[39] Ibid

[40] *Raising awareness of cybersecurity*. ENISA. (2021, December 14). https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity

[41] Information sharing cover indexed 0611 - combatting cybercrime. (n.d.-b). https://www.combattingcybercrime.org/files/virtual-library/national-laws/information-sharing-public-private-partnerships,-perspectives-and-proposals.pdf

incorporation of cyber security into formal education all demonstrate the EU's commitment to providing its citizens with the information and skills they need to engage in safe online behaviour. As the digital world evolves, the EU's will to adapt and expand its cyber resilience framework places it at the forefront of global efforts to resist cyber-attacks. The continued collaboration, legislative measures, and research expenditures demonstrate the EU's commitment to ensuring a safe and resilient digital future for its citizens.

BIBLIOGRAPHY

1. (2014, February 10). *A survey of emerging threats in cybersecurity*. Journal of Computer and System Sciences. https://www.sciencedirect.com/science/article/pii/S0022000014000178
2. Castagna, R., & Lavery, T. (2021, January 29). *What is GDPR? an overview of GDPR compliance and conditions*. WhatIs. https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR
3. Chaudhary, A. (2022, July 25). *Metaverse has potential to revolutionize e-commerce*. mint. https://www.livemint.com/opinion/online-views/metaverse-has-potential-to-revolutionize-ecommerce-11658743775928.html
4. Cybersecurity in the EU: An introduction - universidad nacional de ... (n.d.). https://blogs.uned.es/digitaleconomy/wp-content/uploads/sites/253/2022/01/Cybersecurity-in-the-EU-an-introduction.pdf
5. *Cybersecurity policies*. Shaping Europe's digital future. (n.d.). https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
6. *How smart, Connected Products Are Transforming Competition*. Harvard Business Review. (2020, September 10). https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition
7. Information sharing cover indexed 0611 - combatting cybercrime. (n.d.-b). https://www.combattingcybercrime.org/files/virtual-library/national-laws/information-sharing-public-private-partnerships,-perspectives-and-proposals.pdf
8. *International strategy - enisa*. ENISA. (2021, November). https://www.enisa.europa.eu/publications/corporate-documents/enisa-international-strategy
9. Jack, V. (2023, November 26). *Europe's grid is under a cyberattack deluge, industry warns*. POLITICO. https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/
10. Jamesr.faulconbridgeandjonathanv.beaverstock - Sage Publications Inc. (n.d.-b). https://www.sagepub.com/sites/default/files/upm-binaries/24132_19_Hollway_Ch_19.pdf
11. Jr., T. H. (2022, March 25). *What is anonymous? how the infamous "hacktivist" group went from 4chan trolling to launching cyberattacks on Russia*. CNBC.

https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

12. Mark Young, A. A. (2023, December 1). *The EU's Cyber Resilience Act has now been agreed*. Inside Privacy. https://www.insideprivacy.com/cybersecurity-2/the-eus-cyber-resilience-act-has-now-been-agreed/
13. *Raising awareness of cybersecurity*. ENISA. (2021, December 14). https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity
14. Roussi, A. (2023, November 27). *Russian hackers pose "high" threat level to EU, Bloc's Cyber Team warns*. POLITICO. https://www.politico.eu/article/threat-eu-high-russia-hackers-launch-cyberattacks-fancy-bear-election/#:~:text=Moscow's%20Fancy%20Bear%20group%20is,EU%20cyber%20response%20team%20warns.&text=Russia's%20notorious%20hacking%20group%20Fancy,a%20note%20seen%20by%20POLITIO
15. *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. (2023, September 14). https://gdpr.eu/what-is-gdpr/
16. *Who is responsible for cyber security?*. International Security Journal. (2023, August 9). https://internationalsecurityjournal.com/who-is-responsible-for-cyber-security/