CSS | ISSUE BRIEF

THE EU’S JOINT CYBER UNIT

A move towards a collective digital future

Palak Minda *

Edited by: Akshata Satluri

INTRODUCTION

This paper centers around the Joint Cyber Unit (JCU) recommendation made by the European Commission on the 23rd of June 2021. It traces the trajectory of events leading to the 2020 strategy of the commission. It briefly discusses the said EU Cybersecurity Strategy for the Digital Decade brought forth by the commission in 2020 which first introduced this idea of establishing the joint unit and also addresses other facets which were introduced whose efficient functionality would be dependent on the working of the JCU. It goes on to elaborately discuss the recommendation and the contingencies the unit shall be based on.

1.The 2013 EU Cybersecurity Strategy and the pandemic

Prior to 2020, the ‘EU Cybersecurity Strategy’ of 2013 had three pillars upon which the legal framework of cybersecurity was built, namely, cyber defence, the law enforcement and the network and information security (NIS). Law enforcement – being the first pillar – had the Directive on Attacks against Information Systems (2013) which controlled illicit ventures including access to data, interference with the same etc. NIS being the second pillar primarily encompassed legal instruments such as the Cybersecurity Act of 2019, the 2016 NIS Directive, etc. The third pillar of cyber defence however remained to be undeveloped in this progressive digital world, leaving the EU vulnerable to cyber-attacks and crimes.[2]

Cyber-attacks and crimes are a threat to the national security of a region. In the European Union, such attacks escalated to 756 in 2020 from 432 in 2019 during the COVID pandemic.[3] The situation was grave as sensitive data regarding two covid vaccines was released after an attack

**** The author is a student of Jindal Global Law School and Research Assistant at the Centre for Security Studies, JSIA.***

[2] Crossroads Europe, . “Cybersecurity and the EU: Lessons from the Covid-19 Crisis.” Crossroads Europe, October 6, 2020. https://crossroads.ideasoneurope.eu/2020/10/06/cybersecurity-and-the-eu-lessons-from-the-covid-19-crisis/.

[3] Tidy, Joe. “EU Wants Emergency Team for 'Nightmare' Cyber-Attacks.” BBC News. BBC, June 23, 2021. https://www.bbc.com/news/technology-57583158.

on the European Medicines Agency.[4] It further escalated when disinformation regarding Covid-19, the vaccines and other data with respect to the disease was spread.[5] Additionally, the violation of the Solar Winds had a large scale affect involving numerous stakeholders including the public administrations, government across nations as well as several businesses from different sectors.[6] Further, a group of cyber criminals called the Darkside attacked the Colonial pipelines and set them offline for a week in May 2021. This caused mass panic and shortages of fuel supply. Furthermore, ransomware attacks had increased tremendously over the course of the last year. Such hackers started stealing and manipulating sensitive data from the system of the organisations, asking for hefty amounts simply to revert the damage they have caused. One such grave incident of ransomware included the attack on Ireland’s health care system. The pandemic has weakened the health care system as is, such an attack would not just affect an individual nation but the world at large. It would not just have large financial impact but also have a massive “human cost”.[7] This led to a shift towards introducing more elaborate and stringent policies. Rather than having a significant alteration, it made the European Commission reinforce ‘existing ideas and attitudes, albeit with a renewed impetus and an acceleration of action’ in the field of cyber security.[8]

Consequently, on 16 December 2020, as a part of the European Union’s idea of establishing a green, resilient and digital Europe, the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission together brought forth the new EU Cybersecurity Strategy for the Digital Decade. The Covid-19 situation tested the previous strategy of 2013 as the expansion of the digital world due to work from home for most business and government sectors had left nations vulnerable. Owing to failure of the previous strategy, the new 2020 strategy was introduced with a focus on enabling a cyber connectivity across Europe and strengthening the existing security measures and digital tools to combat cyber-attacks and crimes. This was a part of the Union’s broader aim of turning Europe into a global leader for digital economy.[9]

[4] Declerck, Thomas. “New Eu Cybersecurity Strategy: European Commission Accelerates Push for EU to Lead in Cybersecurity Regulation.” JD Supra, December 24, 2020. https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/.

[5] Carracipo, Helena, and Benjamin Farrand. “Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy.” Taylor & Francis, August 30, 2020. https://www.tandfonline.com/doi/full/10.1080/07036337.2020.1853122.

[6] Declerck, Thomas. “New Eu Cybersecurity Strategy: European Commission Accelerates Push for EU to Lead in Cybersecurity Regulation.” JD Supra, December 24, 2020. https://www.jdsupra.com/legalnews/new-eu-cybersecurity-strategy-european-47823/.

[7] Tidy, Joe. “EU Wants Emergency Team for 'Nightmare' Cyber-Attacks.” BBC News. BBC, June 23, 2021. https://www.bbc.com/news/technology-57583158.

[8] Carracipo, Helena, and Benjamin Farrand. “Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy.” Taylor & Francis, August 30, 2020. https://www.tandfonline.com/doi/full/10.1080/07036337.2020.1853122.

[9] Ștefura, Flavia, and Cristina Crețu. “European Union's New Cybersecurity Strategy.” Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

2.The 2020 Cybersecurity Strategy

The new document divided Cybersecurity into three sects: (2.1) cyber resilience (2.2) establishing operational capacity through a Joint Cyber Unit and (2.3) promoting an open and global cyberspace.[10] For the purposes of this paper, we shall focus on the Joint Cyber Unit while briefly discussing the topic of cyber resilience so as to get a clarity about the functionality of the Unit and the European Commission's intention regarding the same.

2.1. Cyber Resilience

This subset deals with the critical infrastructure (CI) and the essential services of the European Union. This idea was to ensure that the public as well as the private sectors are given the option of selecting amongst the most secure services and infrastructures.[11]
For the promotion of such resilience for the cybersecurity of single market, two legislative proposals were introduced with the said Strategy, namely, the Critical Entities Resilience Directive (CER) and NIS2. Moreover, the European Cyber Shield" was promoted with these proposals.[12]

2.1.1. NIS Directive 2020

As stated above, the NIS Directive was central to the resilience of the single market for cybersecurity. Previously, the directive helped facilitate the cybersecurity capabilities of the EU and increased it. It mandated the Member states to have detailed National Cybersecurity Strategy, build Computer Security Incident Response Teams (CSIRTs) and employ competent national NIS authorities to handle cyber-attack incidents and in turn increasing cyber resilience across digital services as well as in important sectors from the public and private entities. However, owing to such disintegration across different levels, it became exceptionally difficult to execute the directive practically across the internal market.[13]

Therefore, in light of the pandemic and the failure of the previously established systems and policies, it was extremely important for such cyber resilience to be reviewed and in turn improved. This would provide a drastic reduction of inconsistencies that existed in the internal

[10] Ibid.

[11] Ibid.

[12] Noyan, Oliver. "The New EU Cyber Security Strategy – Exploring Ways to Shape Europe's Digital Future." You are being redirected... Accessed September 24, 2021. https://finabel.org/the-new-eu-cyber-security-strategy-exploring-ways-to-shape-europes-digital-future/.

[13] "Legislative Train Schedule." European Parliament, n.d.. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive/05-2021.

market, making the relevant sectors more regulated through rules. Such increase in resilience is paramount in all relevant sectors like, health, transport, finance, energy and such other sectors which lie at the core of the society and the economy at large.[14]

Hence, on 7th July 2020, the European Commission conducted a public consultation for the revision of the 2016 NIS Directive, wherein it invited views on the implementation and in turn the impact of the same if changes were made to it. They shut this consultation on 2nd October 2020 and introduced the new directive with the 2020 EU Cybersecurity Strategy.[15]

This new directive has a wider scope with more stringent rules and implications. It 'aims to strengthen the security requirements imposed, addressing security of supply chains, streamlining reporting obligations, introducing more stringent supervisory measures and stricter enforcement requirements including harmonised sanctions across Member states'.[16] The directive further introduced proposals for sharing data as well as increased cooperation at a national and EU level with regard to crisis management of such crimes-attacks. In Cybersecurity matters, the mandate of this directive would apply to numerous entities and sectors, leading to an increment in the level of security and the scope of the proposal.[17] It enforces new obligations on the important and the essential service providers in the critical sectors, by binding them to report such cyber-attack cases, 'implementing security policies, scrutinizing the security of suppliers and the use of encryption technology'. In case of non-compliance, it provides national authorities with the power to enforce the law to the extent that they can make the CEOs of such firms step down temporarily or even stop the activities of such firms.[18]

2.1.2. Cyber Shield

Another part of the resilience building strategy of the European Commission was the Cyber Shield. This mechanism was introduced to facilitate a speedy exchange of threat intelligence among the public, private, as well as the security authorities.[19] This was to help ensure that

[14] Ștefura, Flavia, and Cristina Crețu. "European Union's New Cybersecurity Strategy." Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

[15] "Legislative Train Schedule." European Parliament, n.d.. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive/05-2021.

[16] Ibid.

[17] "Legislative Train Schedule." European Parliament, n.d.. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive/05-2021.

[18] Cerulus, Laurens. "Europe's Gambit to Fight off Cyberattacks." Politico. Politico, December 17, 2020. https://www.politico.eu/article/europe-gambit-fight-off-cyberattacks/.

[19] Ibid.

through an effective mechanism, potential threats are detected and an adequate response is taken by the EU players before any actual damage has been caused[20].

Julia Schuetze, researcher at the Stiftung Neue Verantwortung in Berlin, stated that the EU Cybersecurity strategy could only have an impact, if the EU defined “when to share the right information, in time to make a difference". In line with what Ms. Schuetze has said, new mandates would be provided to the agencies and institutions by the EU to ensure a safe exchange of confidential data and information.[21]

Further, as a part of the resilience policy as well as broader aim of achieving global leadership in the digital economy, the 2020 plan aims to target the “authoritarian regimes’ restrictions on the internet”. The idea is to impose sanctions on such hacking teams which have the backing of the state. This is to ensure that stricter rules are followed globally. Therefore, within their foreign intelligence service (INTCEN), EU would have to establish a “ cyber intelligence working group” to meet their goal. [22]

Improvement in the resilience capacity of the EU would not be enough to combat the wide scale cyber-attacks its members have been subjected to. Having an effective response team with the requisite digital tools and skills and the backing of enforcement authorities would be necessity for the efficient functioning of the 2020 strategy. In today’s world, most relevant sectors including energy, health, transport, space, defence, finance, telecommunications are primarily dependent on the information systems, exchange of data and interconnected network . With technological advancement, this dependency would exponentially increase, thereby increasing the data vulnerability. Therefore, in order to keep such threat at bay, it is necessary for the EU to ensure that all digital investments are merged with cybersecurity and the overall operational capacity of the EU is improved.[23]

2.2. Joint Cyber Unit

Building cyber resilience would not be fruitful unless the EU has the operational capacity to effectively combat cyber-attacks.[24] Previously, the national security of each nation was under

[20] Noyan, Oliver. “The New EU Cyber Security Strategy – Exploring Ways to Shape Europe’s Digital Future.” You are being redirected... Accessed September 24, 2021. https://finabel.org/the-new-eu-cyber-security-strategy-exploring-ways-to-shape-europes-digital-future/.

[21] Cerulus, Laurens. “Europe's Gambit to Fight off Cyberattacks.” Politico. Politico, December 17, 2020. https://www.politico.eu/article/europe-gambit-fight-off-cyberattacks/.

[22] Ibid.

[23] Ștefura, Flavia, and Cristina Crețu. “European Union's New Cybersecurity Strategy.” Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

[24] Ibid.

the supervision of its government. However, in light of the cyber-attacks and invasion in Europe in 2020, EU's plan of creating a Joint Cyber Unit (JCU) has been urgently put forth through a recommendation on 23rd June, 2021. The previous issues regarding giving powers over such sensitive area to a pan European body was overcome owing to the cyber crisis that the European nations went through.[25]

Although the previous strategies and policies regarding cybersecurity did delve into subjects of cooperation between several EU institutions and the Member States yet, they failed to establish a common forum for exchange of information and data between states. Moreover, there was no mechanism for accumulation of mutual resources so as to combat such attacks in a coordinated and a joint manner.[26]

Therefore, to bridge these gaps, the European Commission recommended the idea of having a Joint Cyber Unit as a common platform for all cross-border cyber threats in the EU. This unit would exist in physical as well as the virtual manner. It is supposed to facilitate a well-planned, faster and coordinated response of the EU as a whole against cyber invasion[27] through exchange of information and data about such attacks in real time by the Member states.[28] The said unit would have an advanced preparedness to deal with cybersecurity crisis situations. The forum would further facilitate a 'structured cooperation between civilian, diplomatic, law enforcement and defence cybersecurity communities'.[29]With greater awareness,[30] constant cross-border monitoring,[31] combined resources, expertise, more stakeholders involving private parties, systematic organisation and preparedness, the unit aims to efficiently prevent, deter

[25] Leyden, John. "EU Pushes Plans for Joint Cyber Unit in Fight against Increased Cyber-Attacks." The Daily Swig | Cybersecurity news and views. The Daily Swig, June 23, 2021. https://portswigger.net/daily-swig/eu-pushes-plans-for-joint-cyber-unit-in-fight-against-increased-cyber-attacks.

[26] Ștefura, Flavia, and Cristina Crețu. "European Union's New Cybersecurity Strategy." Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

[27] Pingen, Anna. "Commission Recommends Joint Cyber Unit." eucrim, July 9, 2021. https://eucrim.eu/news/commission-recommends-joint-cyber-unit/.

[28] E&T editorial. "EU Announces Joint Cyber Unit to Tackle Escalating Online Crime." RSS, June 23, 2021. https://eandt.theiet.org/content/articles/2021/06/eu-announces-joint-cyber-unit-to-tackle-escalating-online-crime/.

[29] Noyan, Oliver. "Commission Proposes 'Operational Arm' of European Cyber Shield." www.euractiv.com, June 23, 2021. https://www.euractiv.com/section/cybersecurity/news/commission-proposes-operational-arm-of-european-cyber-shield/.

[30] Ștefura, Flavia, and Cristina Crețu. "European Union's New Cybersecurity Strategy." Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

[31] "EU Cybersecurity: Commission Proposes a Joint Cyber Unit to Step up Response to Large-Scale Security Incidents." The European Sting - Critical News & Insights on European Politics, Economy, Foreign Affairs, Business & Technology - europeansting.com, June 23, 2021. https://europeansting.com/2021/06/23/eu-cybersecurity-commission-proposes-a-joint-cyber-unit-to-step-up-response-to-large-scale-security-incidents/.

and respond to all cyber-crime matters[32] as well as have a speedy recovery from the same.[33] Moreover, this unit would serve as the "operational arm of the European Cyber Shield,"[34] and other policies introduced by the European Commission for promotion of cyber resilience in the EU. Furthermore, as claimed by Raghu Nandakumara, the field CTO at cybersecurity vendor Illumio, this unit would be a "logical progression from the 2016 NIS Directive which required individual member states to be appropriately equipped, facilitated strategic cooperation and information exchange, and imbibed a culture of security in sectors critical to the economy and security." Even Andrey Yakovlev, a security researcher at Intsights, commented that combating cyber invasion and attacks is "multi-state operation" which would essentially require a coordinated response from several International stakeholders together rather than having each member state have separate legislations, policies and mechanism.[35]

2.2.1. Further details regarding the JCU

The aforementioned unit would comprise of a variety of stakeholders and experts including members from the Defence Agency of Europe, the European External Action Service (EEAS), Agency of Cybersecurity of the EU (ENISA) as well as the Europol's European Cybercrime Centre.[36] During the initial phase of preparation, ENISA hopes to work as the secretariat of the unit. It aims to help the unit with its tasks of sharing information, coordinating, organising and preparing for response. Owing to this, the JCU would be set-up close to ENISA's Brussels office and at a close proximity with the office of Computer Emergency Response Team for the European Union's agencies, business and corporations (CERT-EU).[37]

[32] Pingen, Anna. "Commission Recommends Joint Cyber Unit." eucrim, July 9, 2021. https://eucrim.eu/news/commission-recommends-joint-cyber-unit/.

[33] Ștefura, Flavia, and Cristina Crețu. "European Union's New Cybersecurity Strategy." Lexology. MPR Partners, February 9, 2021. https://www.lexology.com/library/detail.aspx?g=ad1630cc-5172-4600-9a53-985fb6c845db.

[34] Noyan, Oliver. "Commission Proposes 'Operational Arm' of European Cyber Shield." www.euractiv.com, June 23, 2021. https://www.euractiv.com/section/cybersecurity/news/commission-proposes-operational-arm-of-european-cyber-shield/.

[35] Leyden, John. "EU Pushes Plans for Joint Cyber Unit in Fight against Increased Cyber-Attacks." The Daily Swig | Cybersecurity news and views. The Daily Swig, June 23, 2021. https://portswigger.net/daily-swig/eu-pushes-plans-for-joint-cyber-unit-in-fight-against-increased-cyber-attacks.

[36] E&T editorial. "EU Announces Joint Cyber Unit to Tackle Escalating Online Crime." RSS, June 23, 2021. https://eandt.theiet.org/content/articles/2021/06/eu-announces-joint-cyber-unit-to-tackle-escalating-online-crime/.

[37] Leyden, John. "EU Pushes Plans for Joint Cyber Unit in Fight against Increased Cyber-Attacks." The Daily Swig | Cybersecurity news and views. The Daily Swig, June 23, 2021. https://portswigger.net/daily-swig/eu-pushes-plans-for-joint-cyber-unit-in-fight-against-increased-cyber-attacks.

The Digital Europe Programme would be funding the establishment and systematic functioning of the JCU.[38] Some financial support to help build the cyber-defence capacity of the member states might also be provided by the European Defence Fund.[39]

2.2.2. Steps to establish an effective JCU

The European Commission has proposed four main steps to create the JCU in a gradual manner.[40]

First is the assessment phase. This phase lasts till December 31, 2021. By then the commission aims to identify the operational capabilities of the unit.[41]
Second is the planning phase. This phase ends on June 30, 2022. Till them the commission wishes to develop the Cybersecurity Incident and Crisis Response Plan of the EU to fight such cyber invasions.[42]

Third is the operational phase. This phase shall end on December 31, 2022. By then the commission aims for the unit to be completely functional to fulfil its operational responsibilities.[43]

Fourth is the cooperation expansion phase. By the end of this phase on June 20, 2023, a progress report is to be submitted by the members of the JCU and provide incident, crisis response services to the private entities as well as share information with them.[44]

2.2.3. Potential drawbacks of the Joint Cybersecurity Unit

[38] Stefura, Flavia. “The EU Commission Presents next Steps in the Setting up of the Joint Cyber Unit - Technology - European Union.” Welcome to Mondaq. MPR Partners, July 13, 2021. https://www.mondaq.com/security/1090722/the-eu-commission-presents-next-steps-in-the-setting-up-of-the-joint-cyber-unit-.

[39] “EU Cybersecurity: Commission Proposes a Joint Cyber Unit to Step up Response to Large-Scale Security Incidents.” The European Sting - Critical News & Insights on European Politics, Economy, Foreign Affairs, Business & Technology - europeansting.com, June 23, 2021. https://europeansting.com/2021/06/23/eu-cybersecurity-commission-proposes-a-joint-cyber-unit-to-step-up-response-to-large-scale-security-incidents/.

[40] Ibid.

[41] Stefura, Flavia. “The EU Commission Presents next Steps in the Setting up of the Joint Cyber Unit - Technology - European Union.” Welcome to Mondaq. MPR Partners, July 13, 2021. https://www.mondaq.com/security/1090722/the-eu-commission-presents-next-steps-in-the-setting-up-of-the-joint-cyber-unit-.

[42] Ibid.

[43] Ibid.

[44] Ibid.

The Joint Cybersecurity Unit recommendation is not full proof in nature. There seem to be certain gaps which need to be met for the EU's plan to effectively work.[45]

Firstly, as claimed by Mr. Rajesh Muru, principal analyst in digital transformation and cybersecurity at Global Data Technology, it might be easy to convince governments of different nations that this joint unit would secure their data however, the real struggle would be to make them consensually work with the private sector businesses. Moreover, the infrastructure for such technology would need the EU to bring the service providers into the picture. It would be extremely difficult to convince security companies to work with their rivals, each having their own cyber defences, footprints and initiatives.[46]

Secondly, the issue of transparency would arise. There is bound to be some reluctancy among the Member States with regard to a transparent sharing of data and information. It would a task to bring the nations together in a way that there is an easy exchange of information between them.[47]

Thirdly, as stated by Ilia Kolochenko, member of Europol's data protection experts network, such a unit would not be completely effective unless there is global cooperation. The issue of foreign jurisdiction might arise when the non-EU nation refuses to deport its citizen for a cyber-crime they have committed abroad. Further, with such developed technology, some nation-state hackers are capable of hacking the system of others (their rivals) and proxying their attacks through such violated system. This could lead to the risk of innocent parties being vulnerable to counter attacks, further breaching international laws and escalating crime.[48]

Conclusion

"I think, the best way to protect EU countries from digital threats is to invest in national cyber resilience capacities, promote cyber security awareness among organisations of all sizes, and implement mandatory cyber education in schools and universities." These are the words of Ilia Kolochenko, a member of Europol's data protection experts network. [49] It is seen that she believes that the potential drawbacks of establishing a Joint Cyber Unit are greater than its benefits to the point that the EU must depend on other mechanism and institutions to combat cyber-crimes rather than trying to find ways to bridge the gap the recommendation leaves. On

[45] Glover, Claudia. "The New EU Joint Cybercrime Unit Faces Significant Hurdles." Tech Monitor, June 24, 2021. https://techmonitor.ai/technology/cybersecurity/eu-joint-cybercrime-unit.

[46] Ibid.

[47] Ibid.

[48] Scroxton, Alex. "European Union to Set up New Cyber Response Unit." ComputerWeekly.com. ComputerWeekly.com, June 23, 2021. https://www.computerweekly.com/news/252502897/European-Union-to-set-up-new-cyber-response-unit.

[49] Ibid.

the contrary, I believe that the introduction of this proposal could be a milestone in achieving cybersecurity at a global level. Previously, nations had reservations regarding giving away their power to a pan European body however, when urgency arose post the pandemic they were comparatively more willing. Similarly, with the expansion of the digital world, cyber-crime would keep increasing exponentially as more players get access to resources and information. Therefore, rather than shutting down the idea of having such a unit altogether, it is believed that taking small steps towards achieving the goal would be a better plan of action. Establishing this joint unit in accordance with the steps recommended and crossing the hurdles one-by-one could help achieve Europe's broader goal of being the global leader in the digital economy.