ANALYSIS OF THE EU CYBERSECURITY ACT UNDER THE THEORY OF NEOLIBERAL INSTITUTIONALISM

Safrida Alivia Sri Ananda, Ika Riswanti Putranti, Andi Akhmad Basith Dir

The Faculty of Social and Political Sciences Universitas Diponegoro
Jalan Professor Soedarto SH, Kota Semarang
Email: safridasriyono@gmail.com

Disubmit: 24-03-2021 | Diterima: 19-04-2022

Abstract

Wannacry Ransomware epidemics have attacked several high-profile companies in European Union creating an EU-wide cybersecurity crisis in the digital economy and social order. In response, European Union established an appropriate regulation in cybercrime namely The Cybersecurity Act. The Act as an international regime does not only gives a permanent mandate that strengthens European Union Agency for Network and Information Security (ENISA) but also establishes The EU Cybersecurity Certification Scheme in order to increase cybersecurity and build cyber resilience in the European Union Digital Single Market. This paper investigates how does the Cybersecurity Act as a business law in maintaining cybersecurity aspect on the European Union Digital Single Market through the theory of neoliberal institutionalism as a framework of thinking. After a series of conduction of literature reviews, this research argues that The Cybersecurity Act would be an appropriate regulation in dealing with the cybersecurity crisis in the digitalized market order. The standardization in The EU Cybersecurity Certification Scheme regulated by The Cybersecurity Act would improve cybersecurity and build cyber resilience in the European Union Digital Single Market.

Key words: *European Union Digital Single Market, Cybercrime, The Cybersecurity Act, International Regime.*

Abstrak

Wabah *Ransomware Wannacry* telah menyerang berbagai perusahaan terkemuka di Uni Eropa yang menciptakan suatu kondisi krisis keamanan siber di seluruh Uni Eropa yang telah melekat dengan sistem ekonomi dan sosial yang telah terdigitalisasi. Menanggapi hal tersebut, Uni Eropa menetapkan regulasi yang tepat dalam menangani kejahatan siber yaitu melalui pembentukan *The Cybersecurity Act*. *The Act* sebagai rezim internasional tidak hanya memberikan mandat permanen yang memperkuat lembaga *European Union Agency for Network and Information Security* (ENISA) tetapi juga menetapkan *The EU Cybersecurity Certification Scheme* untuk meningkatkan keamanan siber serta membangun ketahanan siber di dalam tatanan *European Union Digital Single Market.* Tulisan ini mengkaji bagaimana peran *The Cybersecurity Act* sebagai hukum bisnis dalam menjaga aspek keamanan siber dalam *European Union Digital Single Market* dengan menggunakan teori neoliberal institusional sebagai kerangka berpikir. Setelah melalui serangkaian kajian pustaka, penelitian berpendapat bahwa *The Cybersecurity Act* akan menjadi regulasi yang tepat untuk menangani krisis keamanan siber di dalam tatanan pasar yang telah terdigitalisasi. Hal ini dikarenakan standardisasi pada *The EU Cybersecurity Certification Scheme* yang diatur oleh *The Cybersecurity Act* akan meningkatkan keamana siber dan membangun ketahanan siber pada *European Union Digital Single Market*.

Kata kunci: *European Union Digital Single Market,* Kejahatan Siber, *The Cybersecurity Act,* Rezim Internasional.

 DOI: https://doi.org/10.21776/ub.arenahukum.2022.01501.9

Introduction

The Fourth Industrial Revolution has brought advancement in every sector of modern society through the mass adoption of digitalization and smart automation. In the economic sector, the adoption of cutting-edge technologies does not only affecting the performance of a particular business but also affect the economic function in general. Many researchers from many respected companies, such as BCG, IMF, and World Economic Forum shows that whenever companies cut back on technology investments aiming to shore up profits, the results is the opposite, as profits sink significantly, and, as a side effect, GDP also falls dramatically, then a chain reaction starts with the fall of labor productivity after a few years.[1] Therefore, governments around the world are investing heavily in their digital economy to enhance value creation and prosperity.[2]

European Union Single Market is one of the biggest economies in the world. The single market refers to the EU as one territory without any internal borders or other regulatory obstacles to the free movement of goods and services.[3] In order to strive as the world leader in the economic sector, the European Union has adopted a digitalization strategy in its internal market order by introducing the European Union Digital Single Market on 6th May 2015 as one of the European Commission's political priorities. This digitalization strategy aims to create an internal market order that fits the modern digital world that attached to the interconnected cyber system. Therefore, it will create the most extensive and valuable form of digital market in the world for various online-based businesses. According to European Commission (2017), a fully functional Digital Single Market could contribute €415 billion per year to the economy and create hundreds of thousands of new jobs.

The existence of technological advances through the digitized information system has brought many opportunities for the economic sector of the European Union. But at the same time, the use of cutting-edge technologies also posing a massive threat to the security of the Digital Single Market and greatly affect the security of the European Union in general. The adoption of computer technology and the internet of things in the business sector has challenged all the stakeholders to solve the evolving cyber threats that spill over in cross-border trading operations and rising conflicts from the misuse of cyberspace. Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data, and other cyber incidents have

1 Marco Antonio Cavallo, "The Growing Importance of the Technology Economy", https://www.cio.com/article/3152568/the-growing-importance-of-the-technology-economy.html#:~:text=Technology%20has%20deeply%20affected%20the,and%20more%20robust%20international%20trade, accessed 21 December 2020.

2 IMD, "IMD World Digital Competitiveness Ranking 2019", https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/, accessed 12 December 2020.

3 European Commission, "The European Single Market", https://ec.europa.eu/growth/single-market_en, accessed 22 December 2020.

become commonplace.[4] The UK Government Information Security Breaches Survey indicates that among the survey participants, 90% of large organizations reported that they had suffered a security breach in 2015, with this figure standing at 74% for small organizations.[5] A 2014 study estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013; with Germany being the most affected Member States (1.6% of GDP).[6]

Cyber incidents have rapidly grown up to the occurrence of the European cyber crisis that mainly targeted multiple high profile companies operating in the Digital Single Market. The cyber crisis is a serious threat to the basic structures or the fundamental values and norms of a system (in cyberspace), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions.[7] The EU cyber crisis occurred in 2017 through the attack of "WannaCry" Ransomware Epidemics targeted several large companies in Europe that provide vital services such as Britain's National Health Service (NHS), Spain's telecommunications company Telefonica, and French's automaker company Renault. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.[8] The attack is carried out by sending emails designed to trick recipients into clicking on attachments or visiting certain websites. After the execution, the WannaCry ransomware will replicate itself and spread rapidly across computer networks, and infect other vulnerable machines. After infecting the machine, the ransomware will encrypt files and data targeted at the system. Then the hacker will ask for a ransom payment in the form of cryptocurrency to restore files and data that have been encrypted.

The devastating cyber attack through "WannaCry" Ransomware Epidemics in 2017 has caused great destruction in the European digital economic and social order. The hack caused more than 19,000 appointments to be canceled, costing the NHS £20m between 12 May and 19 May and £72m in the subsequent cleanup and upgrades to its IT systems.[9] In the Telefonica case, Kroustek said in a statement provided to International Business Times that the financial impact of the attack on Telefonica

4 Deloitte, "Cyber Crisis Management", https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/cyber-crisis-management.html, accessed 21 December 2020.

5 PWC, "Information Security Breaches Survey 2015"*,* in *ISBS Technical Report Blue*, (London: HM Government, 2015).

6 COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and C.

7 Arjen Boin, *The Politics of Crisis Management: Public Leadership Under Pressure,* (Cambridge: Cambridge University Press, 2005).

8 Alert (TA16-091A), "Ransomware and Recent Variants", https://us-cert.cisa.gov/ncas/alerts/TA16-091A, accessed 20 December 2020.

9 Matthew Field, "WannaCry Cyber Attack Cost the NHS £92 m as 19,000 Appointments Cancelled"*, The Telengraph,* (11 October 2018): 1.

should be significant, and goes far beyond the ransom being demanded, noting that about 85 percent of the company's computers have been infected and employees have been sent home.[10] Among the highest-profile corporate victims was French automaker Renault SA, which was forced to shut down factories across Europe.[11] A recent report, in the aftermath of the "wannacry" attack $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy.[12]

Despite the devastating consequences, the benefit brought by the adoption of computer technology and the internet of things is undeniable. Therefore, the digitalization strategy constantly developed by the European Union until it reached an "omnipresent connectivity", meaning that the connectivity to the internet in Europe can be accessed comprehensively. In 2019, some 77% of the EU-27's adult population reported having used the internet on a daily basis during three months preceding the survey; this figure was 3 percentage points higher than in 2018 and 31 points higher than a decade before (46% in 2009).[13] In the Digital Single Market system, all business actors both large companies and small and medium enterprises (SMEs) constantly maximize the use of the hyper-connected system (cyberspace) in their business activities.

Businesses have switched from the conventional trading system into the modern trading system using cyberspace through e-commerce marketing strategy. Ecommerce sales in Europe grew to 621 billion euros in 2019 and are set to be worth 717 billion euros in 2020.[14] Various leading e-commerce in Europe is included Otto GmbH (a retail company based in Germany) with total revenue reached 14.3 billion euro in 2019/2020, Groupe Casino (a retail company based in French) with total revenue reached 37.822 billion euro in 2017, and Zalando (a fashion and lifestyle company based in Germany) with net income reached 99.7 million euro in 2019. In addition, according to the 2020 Digital Economy and Society Index Report (DESI), the European Commission has explained that companies in the European Union have become increasingly digitalized lead by large companies. 38.5% of large companies relied on advanced cloud services and 32.7% were using big data analytics.[15] The adoption of cloud technology and big data analytics will contribute positively to customer relationship

10 A Dellinger, "Tellefonica WannaCry Ransomware: One of Spain's Largest Telecom Companies Hit By Cyberattack"*, IB Times,* (5 December 2017): 1.

11 N Kostov, "WannaCry Attack hits Renault, 200.000-plus victims", https://www.marketwatch.com/story/wannacry-attack-hits-renault-200000-plus-victims-2017-05-15, accessed 22 December 2020.

12 Proposal For A Regulation of the Uropean Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ('Cybersecurity Act').

13 European Commission, "The EU Cybersecurity Certification Framework", https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework, accessed 21 Janury 2021.

14 Ecommerce News, "Ecommerce in Europe"*, Ecommerce News,* (November 2021): 1.

15 European Commission, "Cloud Computing", https://digital-strategy.ec.europa.eu/en/policies/cloud-computing, accessed 22 December 2020.

management (CRM), marketing of company operations, quality assurance, and company project management.

The increasing reliance upon digitalized information systems in the modern economic sector makes every stakeholder vulnerable to the evolving nature of cyber threats. Although this technology has allowed for many advances in global terms, the openness and philosophy of freedom that underpins the use of the network, also have negative consequences and challenge the global authorities to think of new ways to solve the damages experienced because of the use of cyberspace for bad purposes.[16] It leads to a dilemma that urges dialogue and research about the transition of global economic order to a new era of the modern economy that embedded with a hyper-connected ecosystem.

From the international point of view, the misuse of cyberspace has to gain consideration about how to regulate the problematic cyber nature. Cyber incidents have rapidly grown in the unbounded territorial boundaries of cyberspace that potentially threaten every stakeholder from different countries that operating in a hyper-connected system. Therefore, cooperation between nations is increasingly necessary to give traction to discussions on global cyber governance, aiming at the conclusion of international agreements capable of establishing mutual assistance to guarantee digital inclusion, for the sharing of information and collaboration in investigations of cybercrimes, as well as for the harmonization and guarantee of enforcement regardless of territorial limits imposed by traditional regulatory models.[17]

According to the theory of neoliberal institutionalism, Robert O Keohane emphasizes the importance of the establishment of institutions in international cooperation. This is in line with the basic assumption of the theory of neoliberalism that absolute gains would be achieved from cooperation. Cooperation is not an easy feat and can lead to tension, but states could potentially benefit from cooperative strategies.[18] Institutions provide a coordinating mechanism to help states capture potential gains from cooperation; this "constructed focal point" increases the opportunity for cooperative outcomes.[19] The form of institutions according to Keohane involved; organization, set of rules, and convention.

The theory of neoliberal institutionalism is one of the school in the theory of neoliberalism. The theory of neoliberalism itself is the continuation of the clasic liberalism theory in the clasification of politic

16 Fabio R Bechara and Samara B Schuch, "Cybersecurity and Global Regulatory Challenges", *Journal of Financial Crime Vol.8, No. 2*, (November 2020): 359-374, accessed 12 December 2020, doi: https://doi.org/10.1108/JFC-07-2020-0149.

17 *Ibid.*

18 Robert O Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy,* (New Jersey: Princeton University Press, 1984).

19 Robert O Keohane and Lisa L Martin, "The Promise of Insitutionalist Theory", *International Security Vol. 20, No. 2* , (Summer 1995): 39-51.

liberalism phylosophy. Liberalism is an ideology, philosophical view, and political tradition which based on the comprehension that liberty and equality of right is the main political value.[20] In general, liberalism point of view dismiss every restriction mainly every restriction conducted by the government and religion. The purpose of the liberalism theory is to create a liberal social structure. This independent structure characterized by the liberty of thinking for all individual. In the international structure, liberalism belive that every democratic country would not engage in war towards each other.

As a critic towards the theory of neorealism, neoliberal institutionalism does not contradict the basic assumption of neorealism that the condition of international system is anarchy. Nonetheless, neoliberal institutionalism tend to be optimistic rather than the theory of neorealism in viewed the anarchic international system. According to the institutionalist, in an anarchic international system, cooperation would be established through the formation of an international regime. More recently, a collective defition, worked out at a conference on the subject, defined international regimes as "sets of implicit or explicit principles, norms, rules and decision-making procedures around which actrors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice".[21]

From the above definition, it can be concluded that the establishment of an appropriate regulation is crucial in order to tackle the cybersecurity risk in the masive technological adoption in the European Union Digital Single Market. Therefore, this research paper attempt to discuss on The Cybersecurity Act as a business law in the digital market order and how does the impact of this regulation towards the cybersecurity aspect of European Union Digital Single Market. The nature of this research is qualitative research conducted through a series of literature review using the theory of neoliberal institutionalism as a framework of thinking. This research paper employ the normative juridical approach in order to obtain multiple research data. Furthermore, the normative juridical approach used in this analysis is the statute approach which carried out by reviewing the regulation related to the legal issues being handled. This research paper uses credible sources from books, credible websites, and journals. This research paper aim to provide knowledge about the role of international regimes in solving international issues specifically in the misuse of cyberspace.

20 Moh Suardi, *Ideologi Politik Pendidikan Kontemporer*, (Yogyakarta: Deepublish, 2015).

21 Robert O Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy,* (New Jersey: Princeton University Press, 1984).

Discussion

The Cybersecurity Act enacted through The Regulation (EU) 2019/881. The establishment of The Cybersecurity Act as international regime would bring positive impact towards the European Union Digital Single Market. The international regime would be able to increase security of the European Union Digital Single Market through the implementation of The EU Cybersecurity Certification Scheme that would evaluate and guarantee the cybersecurity of digital products, services, and processes involved in the Digital Single Market structure.

A. The European Union Digital Single Market

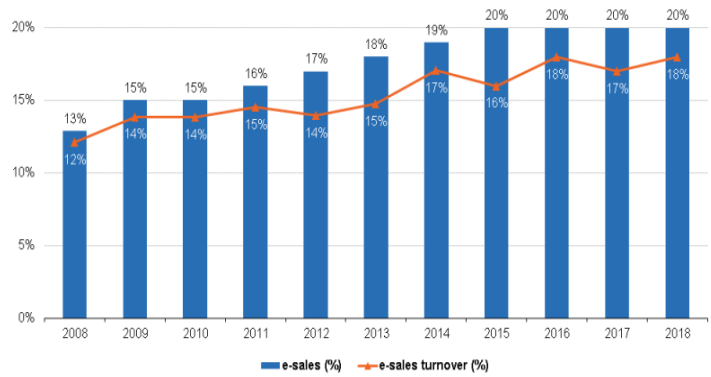
Digital Single Market as one of the European Commission's political priorities built on three pilars. The first pilar is "improving access to digital goods and services", according to this pilar the fully functionate Digital Single Market would facilitate goods and services to be available online in the cross border Europe in order to expand the access of consumen and e-comerce without any obstacle (erase geo-blocking). The second pilar is "an environment where digital networks and services can prosper", according to this pilar the Digital Single Market aim to create an appropriate environment for digital network and services by providing infrastructure and services that are high-speed, secure, and trustworthy, and supported by appropriate regulations that priotize cybersecurity, data protection/privacy, and fairness and transparency in online media (including cybersecurity regulations, data protection, and fairness and transparency of online media). The third pilar is "digital as a driver for growth", according to this pilar Digital Single Market aim to maximize the European digital economy growth in order to give maximum benefit towards the European society.

Every organization around the world competing to adopt digital transformation startegies to improve their performance. Digital transformation, in essence, means the application and use of modern technology in an organizations's business processes to achive its goals and increase efficiency.[22] E-commerce refers here to the trading of goods or services over computer networks such as the internet by methods specifically designed for the purpose of receiving or placing orders.[23] It aims to reach more customers for company and to provide more diverse options for customers. According to the data obtained from E-commerce Statistics (Graphic 1), if accumulated in ll Member States of the European Union (EU-28) there has been an increase in e-sales by 7% accompanied by an increase in revenue of 6% from e-sales activities in the period 2008-2018.

22 A I.V and K A.I, "Model Management Trends and the Digital Economy: from Regional Development to Global Economic Growth", In *Digital Maturity: Definition and Model,* (Amsterdam: Atlantis Press, 2020).

23 Eurostat, "E-commerce statistics", https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Esales_remain_stable_over_recent_years, accessed 13 February 2021.

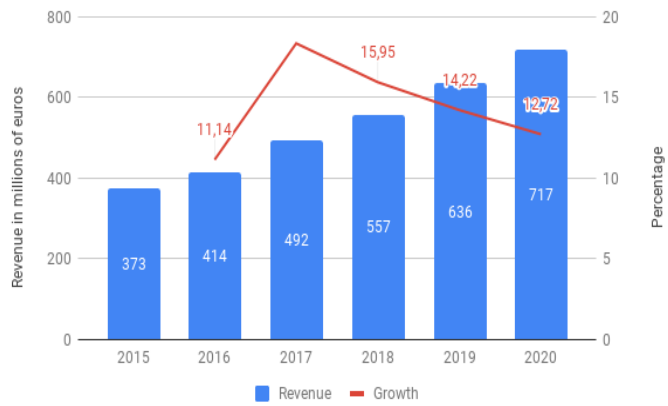
Graphic 1. E-sales and turnover from e-sales, EU-27, 2010 to 2019



Source : Secondary Data, processed, 2020

In the Digital Single Market, the most widely used media for e-commerce is website or application, either developed by each company or through the e-commerce marketplace. As shown in Graphic 2, various companies in EU Member States prefer to develop their own company-owned websites or applications rather than using e-commerce marketplace websites or applications. The highest usage rates of company-owned websites or apps are in Slovakia (98%), Estonia and Romania (97% each). However, in several Western European countries the use of e-commerce marketplace websites is also quite high, at 61% in Italy, 51% in Germany, and 50% in Austria.

Graphic 2. E-sales broken down by web sales and EDI-type sales, 2019

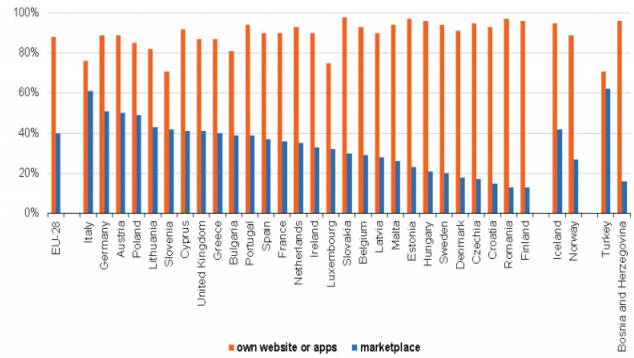


Source : Secondary Data, processed, 2020

In its development, Ecommerce sales in Europe grew to 621 billion euros in 2019 and are set to be worth 717 billion euros in 2020.[24] This shows an increase in income of 12.7% in 2020 when compared to the previous year (See Graphic 3). The largest online stores in the European Union that are currently actively conducting e-sales activities include; Otto (Germany), Groupe Casino (France), and Zalando (Germany).

24 Ecommerce News, "Ecommerce in Europe", *Ecommerce News*, (November 2021): 1.

Graphic 3. Growth of ecommerce revenue in Europe



Source : Secondary Data, processed, 2020

In the digital economy, apart from using e-commerce in their sales strategy, business people also involve other advanced technologies to manage their business more effectively and efficiently. Through the Digital Economy and Society Index Report 2020, the European Commission has explained that companies in the European Union are now increasingly digitized. Dimana 38,5% perusahaan besar sangat bergantung pada penggunaan teknologi canggih seperti layanan awan (cloud services) dan 32.7% perusahaan besar telah menggunakan analitik big data.[25]

Companies in the European Union are now making significant use of cloud technology. The availability of both edge and cloud computing is essential in a computing continuum to ensure that data is processed in the most efficient manner.[26] Through cloud computing technology, companies can take advantage of computer technology that is connected to an internet network so that they can run programs or applications through a centralized network. The use of cloud technology can have a positive impact on customer relationship management (CRM), corporate operational marketing, quality assurance, and enterprise project management.

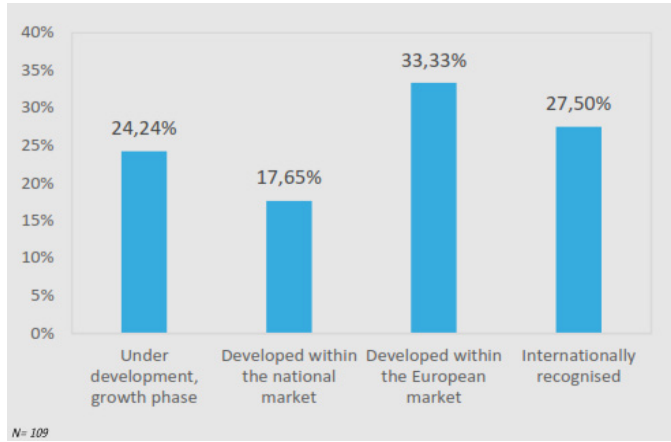
In addition to cloud service technology (cloud services) used in the company, the use of technology will result in very large and varied data flows (big data) in cyberspace. These data can be in the form of data created by humans or generated by machines such as sensors, satellite images, digital images and videos, purchase transaction records, GPS signals, and others that are very valuable for the sustainability of a company, especially those involved in market order. digital. Thus, data has now become a new asset that is vital for economic growth. Therefore, data analytics capabilities are needed for companies involved in the Digital Single Market to make the right business decisions through the extraction of their big data. Big data has now started to be used by businesses that are developed in the

25 European Commission, "Integration of DIgital Technology by Enterprises", https://ec.europa.eu/digital-single-market/en/integration-digital-technology-enterprises, accessed 13 April 2021.

26 European Commission, "Cloud Computing", https://digital-strategy.ec.europa.eu/en/policies/cloud-computing, accessed 22 December 2020.

European market (by 33%) and by businesses that have been recognized internationally (27.5%) (See Graphic 4). The Commission has highlighted the value of the EU data economy, which was estimated to be worth €272 billion in 2015, or around two per cent of EU GDP.[27] It has grown rapidly in recent yeras, External estimates suggest that its value could rise to €643 billion by 2020, more than three percent of GDP, as long as policy and legal frameworks for the data economy are put in place.[28]

Graphic 4. Adoption of big data and data analytics by company development stage



Source : Secondary Data, processed, 2018

Through the use of big data, companies can improve competitiveness, sales, and analyze information related to products, services and employees. 86% of respondents who adopted big data and data analytics consider digital technologies to have generated positive outcome.[29] According to an Accenture study, 79% of enterprise excecutives say that companies that do not adopt Big Data will fall behind the competition.[30] This is because big data analysis capabilities can enable companies to improve three main business functions, namely operational marketing, customer relationship management (CRM), project management, and quality assurance. Thus, various companies can grow rapidly by utilizing big data analysis generated from digital business activities.

The use of advanced technology in the Digital Single Market brings many advantages and conveniences for both business people and customers. This is evidenced by the continued increase in e-commerce within the European Union's Digital Single Market

27 HM Government, "The exchange and protection of personal data", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf, accessed 17 April 2021.

28 *Ibid.*

29 European Commission, "Digital Transformation Scoreboard 2018 EU business go digital: Opportunities, outcome, and uptake", https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018_0.pdf , accessed 22 December 2020.

30 Tetiana Boichenko, "How to choose a reliable big data enterprise analytics provider?", https://www.n-ix.com/how-choose-big-data-enterprise-analytics-provider/ , accessed 22 December 2020

and accompanied by an increase in income (turnover) generated through e-sales to the EU's GDP. And there are various benefits by adopting other advanced technologies such as big data and cloud services that can be utilized by business people in managing companies in an increasingly competitive digital economy. Thus, it can be concluded that the Digital Single Market strategy launched by the European Union has been able to increase economic growth through effectiveness and efficiency in cross-border trade in the European Union, expand markets and tighten competition, and provide convenience for customers throughout the European Union to access products. and services needed.

B. The EU Cyber Crisis

The existence of technological advances has brought many opportunities for the economy in the European Union. The internet has made the world smaller in many ways but it has also opened us up to influences that have never been so varied and so challenging.[31] But at the same time the use of advanced technology also brings a malicious threat to the security of the Digital Single Market which involves cyberspace in cross-border trading operations. In a few decade, cybersecurity issues have risen from being mainly the concern of IT-security experts to become national security priority of modern states, with a considerable impact on contemporary diplomatic, financial and political affairs.[32]

Both small and large-scale businesses that use information and telecommunications technology have the potential to become targets of cyber threats. The UK Government Information Security Breaches Survey indicates that, among the survey participants, 90% of large organizations suffered a security breach in 2015, with this figure standing at 74% for small organization.[33]

The use of information systems and networks is certainly accompanied by risks to the security and privacy of information owned by the company. Therefore, the adoption of advanced technologies such as cloud services and big data within the company also brings no less threat to various actors involved in digital markets that operate in cross-border area. The threat of cyber crime that most threatens the current digital economy is data theft (data theft). Data theft (data theft) or commonly called data breach (data breach) is a form of security breach of information owned by an individual, an entity, or a particular organization. In general, a data breach is an event that an individual's Personally Identifiable Information (PII) is released without the individual's consent or

31 P.S.Semma, et al., "Overview of Cyber Security", International Journal of Advanced Research in Computer and Communication Enginering, Vol. 7, No.11, (November 2018): 125-128, accessed 13 April 2022, doi: https://doi.org/10.17148/IJARCCE.2018.71127.

32 Sarah Backman, "Conceptualizing cyber crises", Journal of Contingencies and Crisis Management, (December 2020): 429-438, accessed 13 April 2022, doi: https://doi.org/10.1111/1468-5973.12347.

33 ENISA, "Information security and privacy standards for SMEs", https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport, accessed 22 December 2020.

knowledge.[34] This security breach is usually carried out by misusing someone's personal information such as name, social security number, email address, password, debit/ credit card, financial account information, medical records, driver's license, etc in order to conduct fraud.

The threat of cyber crime in the form of data theft is now very massive in all industries, including finance, manufacturing, retail, telecommunications, hospitality, and various other services including health facilities, government, education, etc. The Privacy Rights Clearinghouse methodology has classified the types of data breaches into several categories.[35] The first category is the unintentional disclosure of data by abusing sensitive information that is publicly posted on a website and then sent to the wrong party via email, fax, or mail.

The second category is Hacking/Malware where a cyber criminal enters through an electronic device and commits a data breach. The third category is payment card fraud involving debit and credit cards which is not carried out through hacking but through device searches at service point terminals. The fourth category is through insiders who have legal access but intentionally violate information, this is usually done by employees or contractors.

The fifth category is the physical loss of various non-electronic documents that are lost, discarded, or stolen. This can occur with the loss of paper documents or documents contained in portable devices such as laptops, PDAs, smartphones, portable memory devices, CDs, hard drives, data tapes, and others that are lost, discarded, or stolen. The sixth category is through lost, discarded, or stolen stationary devices such as computers or servers. And the sixth category is unknown. This security threat can be fatal to the company because it can disrupt business continuity, the company's monetary reputation and cause various other losses. Thus, a cross-border security strategy is needed to overcome the enormous threat to massive data flows within the European Union's Digital Single Market which includes cross-border online trading activities throughout the European Union.

In fact, the cybersecurity threat in the form of data theft has occurred in the cybersecurity crisis that attacked the European Union's Digital Single Market in 2017 through the "WannaCry" Ransomware Epidemics attack on various high profiles in the European Union such as Britain's National Health Service, a Spanish telecommunications company, namely Telefonica, and the multinational car company Renault. These attacks are carried out by sending emails designed to trick recipients into clicking attachments or visiting certain websites. Then after execution, the WannaCry ransomware will replicate itself and spread rapidly across computer networks and infect

34 E.F. Goodman, "Your Duty If You Discover a Data Breach", *American Bar Association*, (2008): 16-19.

35 R.E. Holtfreter and A Harrington, "Data breach trends in the United States", *Journal of Financial Crime Vol. 22, No. 2*, (2015): 242-260, doi: https://doi.org/10.1108/JFC-09-2013-0055.

other vulnerable machines. After infecting the machine, the ransomware will encrypt files and data targeted at the system. Then the hacker will ask for a ransom payment (ransom) in the form of bitcoin (crypto currency) to restore encrypted files and data.

These ransomware epidemics are the latest and largest in a series of attacks in the cybersecurity crisis that hit the European Union in 2016-2017. More than 4,000 ransomware attacks have occurred every day since the beginning of 2016, a 300% increase over 2015.[36] A 2016 study by PwC revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years, while at least 80% of European companies have experienced at least one cybersecurity incident.[37]

Cyber incidents certainly have a negative impact on businesses in Europe, where the level of trust of stakeholders such as the public and businesses in the digital economic order has decreased. A 2014 study estimated that the economic impact of cybercrime in the Union amounted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013; with Gremany being the most affected Member States (1.6% of GDP).[38] The services most affected are various main services such as financial services, energy, technology, industry, etc.

The ransomware epidemic in 2017, had a devastating impact on the European Union. The hack caused more than 19,000 appointments to be cancelled, costing the NHS £20m between 12 May and 19 May and £72m in the subsequent cleanup and upgrades to its IT systems.[39] The damages were also experienced by the Spanish telecommunications company Telefonica. The ransomware demands $300 paid in bitcoin before it will decrypt the files it holds hostage.[40] In addition, the loss was also felt by the multinational automobile company Renault, where the company was forced to close factories throughout Europe.[41] A recent report, in the aftermath of the "wannacry" attack, estimated that a serious cyber-attack could cost the global economy more than $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy.[42]

C. The Concept of The Cybersecurity Act

36 COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and C.

37 *Ibid.*

38 *Ibid*, p. 2.

39 Matthew Field, "WannaCry Cyber Attack Cost the NHS £92 m as 19,000 Appointments Cancelled"*, The Telegraph*, (11 October 2018): 1.

40 A Dellinger, "Tellefonica WannaCry Ransomware: One of Spain's Largest Telecom Companies Hit By Cyberattack", *IB Times,* (5 December 201): 1.

41 N Kostov, "WannaCry Attack hits Renault, 200.000-plus victims", https://www.marketwatch.com/story/wannacry-attack-hits-renault-200000-plus-victims-2017-05-15 , accessed 22 December 2020.

42 COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on

The Cybersecurity Act is a set of rules established through The Regulation (EU) 2019/881 in order to increase the cybersecurity of the European Union through a permanent mandate given to the European Union Agency for Network and Information Security (ENISA). In addition, The Cybersecurity Act also regulates the establishment of the first Cybersecurity Certification Framework agreed at the European level in order to evaluate and ensure the security of ICT products, ICT services, and ICT processes in the Digital Single Market at a certain level applicable in all EU Member States. Certification plays a critical role in increasing the trust and security of products and services that are crucial for the Digital Single Market.[43] The establishment of an EU-wide cyber certification scheme will be a strategic effort to secure the internal market order which has been attached to the hyper-connected system. In addition, the establishment of the EU-wide certification scheme will overcome the fragmentation and obstacles in securing the EU Digital Single Market through a harmonized approach at the Union level by discontinuing every cybersecurity certification scheme that has been established in the various Member States.

The establishment of the European Cybersecurity Certification Framework has been regulated in the Regulation (EU) 2019/881 in article 46 :

> "The European cybersecurity certification framework shall be established in order to improve the condition for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonized approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services, and ICT processes."

The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards, and procedures.[44] According to article 2 of The Cybersecurity Act, an ICT product means an element or group of elements from a network and information system. ICT service means a service that consists entirely or primarily in the transmission, storage, retrieval, or process of infomation via networks and information systems. In addition, the ICT process is a series of activities carried out to design, develop, deliver, or maintain ICT products or ICT services. Thematic application areas likely to be affected by the cybersecurity certification provisions of the CSA may include specific ICT products (e.g. semiconductors), services (e.g. cloud services), and processes (e.g. information security-related methods).[45]

ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and C.

43 European Commission, "The EU Cybersecurity Certification Framework", https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework , accessed 21 January 2021.

44 *Ibid*, p. 2.

45 ENISA, "Bolstering ENISA in The EU Cybersecurity Certification Framework", https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework , accessed 22 December 2020.

Another example of ICT products, services, and processes applications for the certification schemes are :

1. ICT products such as applications and software, for example, e-book, video games, digital contents, etc.
2. ICT services such as cloud services and big data analytics.
3. ICT processes such as digital trade through e-commerce marketing strategy both developed by each company or through e-commerce marketplace.

D. The Cybersecurity Act as a Business Law

According to the theory of neoliberal institutionalism, Robert O Keohane emphasizes the importance of the establishment of institutions in international cooperation. The form of institutions according to Keohane involved; organization, set of rules, and convention. Business law is the body of law which governs business and commerce and is often considered to be a branch of civil law and deals both with issues of private and public laws.[46] Business law falls into two distinctive areas: (1) the regulation of commercial entities by the laws of company, partnership, agency, and bankruptcy and (2) the regulation of commercial transactions by the laws of contract and related fields.[47]

The European Union has officially adopted a digitalization strategy in its internal market order by introducing the European Union Digital Single Market on 6th May 2015 as one of the European Commission's political priorities. The existence of technological advances through the digitized information system has brought many opportunities for the economic sector of the European Union. Nowadays, business activities are carried out electronically rather than by traditional means. On the other hand, the mass adoption of technological advances in the business sector would potentially bring the misuse of cybercrime as a hybrid form of obstacle in the Digital Single Market order. All these being said, although we speak about unprecedented context, the European Union, over the last two decades, has enacted more directives and regulations in order to keep up with this market's unique and high innovation rate with the goal to ensure the customer's protection.[48]

Following the evolving nature of cyber threat that potentially threaten the European Union Digital Single Market by the masive adoption of digitalization aspect in business sector, European Union has make an appropriate business law that adapted to and embraced the fast developing world of the digitalization and internet of things. The Cybersecurity Act enacted through The Regulation (EU) 2019/881 would be considered as part of

46 Ahmed Umar Abubakar, *Business Law*, (Honolulu: Atlantic International University, 2006).

47 Britannica, "Business Law. Encyclopedia Britannica". https://www.britannica.com/topic/business-law.

48 Ovikdiu Loan Dumitru and Andrei Viorel Tomescu, "European Consumer Law in The Digital Single Market". *Juridical Tribune Vol. 10, No. 2*, (June 2020): 1-17, accessed 7 August 2020, doi; https://ssrn.com/abstract=3641921.

business law in regulating the European Union Digital Single Market on the cybersecurity aspect. The Cybersecurity Act would provide protection for all the stakeholder that actively involved in the European Union Digital Single Market. Furthermore, through the adoption of The Cybersecurity Certification Scheeme regulated on The Cybersecurity Act, European Union would establish standards for the cybersecure business concerns. Therefore, The Cybersecurity Act is a vital business law regulating unified cyber secure business practice in European Union.

E. European Union Competence in The Cybersecurity Act

According to the theory of neoliberal institutionalism, Robert O Keohane emphasizes the importance of the establishment of institutions in international cooperation. Cooperation is not an easy feat and can lead to tension, but states could potentially benefit from cooperative strategies.[49] Institutions provide a coordinating mechanism to help states capture potential gains from cooperation; this "constructed focal point" increases the opportunity for cooperative outcomes.[50] As explained in the previous section, the Digital Single Market strategy has been complemented by the regulations of The Cybersecurity Act as an international regime. A set of rules stipulated in The Cybersecurity Act will contribute to forging stronger cooperation at the supranational level to maintain EU cybersecurity especially in the economic sector which attached to the digital transformation strategy.

In Article 28 of the Treaty of the Functioning of the European Union (TFEU) has been explained that :

> "To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations, and opinions".

In order to determine the classification of competences, it must determine the type of legal action to be taken first. The type of legal action in the European Union constitutions is consists of legally binding acts and non-binding acts. Legally binding acts can take the form of regulations, directives, and decisions. In another hand, non-binding acts can be in the form of recommendations or opinions. The Cybersecurity Act has been enacted through the enforcement of The Regulation (EU) 2019/881 on 27 June 2019. As regulated in Article 288 of the Treaty on the Functioning of the European Union (TFEU), a regulation shall have general application. Therefore, the regulation codified in The Cybersecurity Act not only grants a permanent mandate to ENISA but also shall be binding in its entirety and directly applicable in all Member States.

The division of competence in the European Union has been stipulated in

49 Robert O Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy,* (New Jersey: Princeton University Press, 1984).

50 Robert O Keohane and Lisa L Martin, "*The Promise of Insitutionalist Theory"*, *International Security Vol. 20, No. 1*, (Summer 1995): 39-51.

the Treaty of Lisbon which consists of executive competence, shared competence, and supporting competence. Exclusive competences (Article 3 of the Treaty on the Functioning of the European Union – TFEU) areas in which the EU alone is able to legislate and adopt binding acts.[51] Shared competences (Article 4 of the TFEU) mean EU and EU countries are able to legislate and adopt legally binding acts.[52] Whereas, supporting competences (Article 6 of the TFEU) means the EU can only intervene to support, coordinate or complement the action of EU countries.[53]

The Digital Single Market strategy is not formally categorized into a particular area of competence due to there is no specific area related to digitalization in the division of competence regulated in the Treaty of the Functioning of the European Union (TFEU). However, according to the strategic objective of the Digital Single Market to encourage economic growth in the European Union, the Digital Single Market can be categorized as an extension of the common commercial policy area under exclusive competence and the internal market area under shared competence. Furthermore, considering the scope of the Digital Single Market involves complex nature of cyber ecosystem that spill over borders, the roles of different actors in all level of the society are needed.

The enactment of The Cybersecurity Act through The Regulation (EU) 2018/881 would lead to the enforcement and obligation of the instituted law in every Member States. It will overcome the disparity in various Member States with relatively different cybersecurity levels in carrying out activities in the digitalized internal market. Therefore, the regulation codified in The Cybersecurity Act is under the exclusive competence of the European Union in order to have a harmonized approach in dealing with cyber issues all over Europe. Due to the establishment of The EU Cybersecurity Certification schemes as an EU-wide Cybersecurity Framework, every national cybersecurity certification schemes that have been developed in various Member States such as the Cyber Essentials scheme, the Dutch scheme for the Baseline Security Product Assessment (BSPA), and the Certification Sécuritaire de Premier Niveau must be dismissed if it covers the same procedure. In addition, it is prohibited to develop another certification scheme that includes the same procedures as The EU Cybersecurity Certification scheme.

In order to comprehensively implement the EU Cybersecurity Certification scheme, the National Cybersecurity Certification Authority should be established in each Member States. The establishment of the National Cybersecurity Certification Authority must be informed to the European Commission.

51 European Union, "Division of Competences within the European Union", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:ai0020#:~:text=The%20EU%20has%20only%20the,attain%20the%20objectives%20provided%20therein , accessed 21 Janury 2021.

52 *Ibid.*

53 *Ibid.*

It is an independent authority tasked with enforcing the regulations in The Cybersecurity Act precisely in The EU Cybersecurity Certification Scheme. In addition, the authority also tasked with observing the compliance of various companies operating in the Digital Single Market towards the regulations under The Cybersecurity Act.

F. The Positive Contribution Brought by The Cybersecurity Act

Cybercrime is a global, transantional serious problem that needs strong technical and legal responses.[54] The increasing expansion and diversification in the strategies and practices of cybercrime has become a difficult obstacle in order to understand the extent of embedded risks and to define efficient policies of prevention for corporations, institutions, and agencies.[55] Therefore, the misuse of the technology has created the need of the enactment and implementation of the cyber laws.[56]

The enactment of The Cybersecurity Act will contribute positively to the European Union Digital Single Market. Through The EU Cybersecurity Certification scheme established under The Regulation (EU) 2018/881 (The Cybersecurity Act), every company involved in the Digital Single Market will be guaranteed to have implemented best practices in digital-based business activities. Therefore, The Cybersecurity Act will contribute positively to the second pillar of the European Union Digital Single Market, "an environment where digital network and services can prosper" which includes the need for adequate cybersecurity in the digitalized internal market order. It is necessary to increase the trust of various stakeholders actively involved in the Digital Single Market. The Cybersecurity Act becomes the first international regime regulating the internal market in responding to challenges related to the security of ICT products, ICT services, and ICT processes in the Digital Single Market. This is in line with the basic assumption of the theory of neoliberal institutionalism which tends to be optimistic that the establishment of cooperation would be strengthened through the formation of an international regime.

The importance of The Cybersecurity Act towards the Digital Single Market has been strengthened through an assertive statement of the Vice President of European Union Digital Single Market Andrus Ansip, "Europe's Digital Single Market can only be a reality if it includes robust cybersecurity commitments. This Commission has pushed forward in making sure Europe has the necessary capabilities, including by proposing

54 Victoria Stanciu and Andrei Tinca, "Exploring cybercrime – realities and challenges", Journal of Accounting and Management Information System, Vol. 16, No. 4, (2017): 610-632, accessed 13 April 2022, doi: http://dx.doi.org/10.24818/jamis.2017.04009.

55 Regner Sabillon, *et al*., "Cybercrime and Cybercriminals: A Comprehensive Study". *International Journal of Computer Networks and Communcations Security, Vol. 4, No. 6,* (June 2016): 165-176, accessed 13 April 2022, E-ISSN 2308-9830.

56 R. M. Kamble, "Cyber Law and Information Technology", *International Journal of Scientific and Engineering Research, Vol. 4, No. 5,* (May 2013): 789-794, accessed 13 April 2022, ISSN 229-5528.

a European certification framework and having financing for cybersecurity research and development under the next long-term EU budget. Work on 5G security is a particular priority, as it has the potential to impact every aspect of our future.".[57] Commissioner for Digital Economy and Society Mariya Gabriel added that "The EU Cybersecurity Act has demonstrated the need for an EU approach to responding to all challenges, protect our citizens, and stay competitive. In order to achieve this goal, Europe has granted a permanent mandate to the EU Agency for Cybersecurity. The Cybersecurity Act also enables EU-wide cybersecurity certification. With the Cybersecurity Act, the Directive on the security of networks and information systems and the proposed European Cybersecurity Competence Centre we have put forward a strong EU pattern, based on our democratic values and safeguarding our citizen's interest.".[58]

In dealing with the evolving nature of cyber threats that previously able to harm European society just as hazardous as catastrophic events through the massive incidents of the EU cyber crisis is proven that a strategy based on cybersecurity is no longer provides adequate protection in the more digitalized environment. Therefore, the ability to react to these attacks and to design and implement a more robust organization recalls the concept of resilience, known in physics as the assumption of sustaining crashes without breaking.[59] Cyber resilience refers to "the ability to recover or regenerate its performance to a sufficient level after an unexpected impact procedure a degradation of its performance. It is characterized by [four] abilities: to plan/prepare, absorb, recover from, and adapt to known and unknown threats".[60] Since the threats existed in the cross-border cyber ecosystem, the foremost action must be taken at the cross-border level through the establishment of cooperation.

According to the Article 52 Regulation (EU) 2019/881, The Cybersecurity Act regulates the evaluation and level of assurance of various ICT products, service, and process that involved in the Digital Single Market. To express the cybersecurity risk, a certificate may refer to three assurance levels (basic, substantial, high) that are commensurate with the level of the risk associated with the intended use of the product, service, or process, in terms of the probability and impact of an incident.[61] The "basic" level assure that the ICT product, service, and process meet the security

57 European Commission, "The EU Cybersecurity Act Brings a Strong Agency for Cybersecurity and EU-Wide Rules on Cybersecurity Certification", https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity , accessed 17 January 2021.

58 *Ibid.*

59 Alesandro Annarelli et al., "Understanding the Management of Cyber Resilience Systems", Elsavier Ltd, (September 2020), accessed 20 November 2020, doi: https://doi.org/10.1016/j.cie.2020.106829.

60 Rick Cassleman, "Expanding Cyber Resilience Beyond Convention Resiliency and Nuclear Command, Control, and Communications", In *On the Horizon: A Collection of Papers from the Next Generation,* (Maryland: Rowman & Littlefield, 2020).

61 European Commission, "The EU Cybersecurity Certification Framework", https://ec.europa.eu/digital-

requirements and have been evaluated to minimize the underlying risk of cyber incidents. The evaluation conducted by technical documentation review. The "substantial" level of assurance assure that ICT product, service, and process meet security requirements and have been evaluated to minimize the risk of cyber incidents conducted by actors with limited skills and resources. The evaluation includes a review that shows the absence of any known vulnerabilities to the public and properly implements the necessary security functions. Meanwhile, the 'high' level of assurance assure that the ICT product, service, and process meet security requirements and have been evaluated to minimize the risk of sophisticated cyber incidents conducted by actors with significant skills and resources. The evaluation includes a review to show the absence of vulnerability known by public and implemented advanced security functions, cyber resilience assessment, and penetration testing.

Through the implementation of the standardization in The EU Cybersecurity Certification Scheme under The Cybersecurity Act, the European Union Digital Single Market will be a digitally mature market that continuously leads the global digital economy order supported not only with cybersecurity strategy but also cyber resilience strategy. Every business operating in the Digital Single Market will make sure to have the ability to prepare, absorb, adapt and recover quickly from unforeseen events targeting them in the ever-changing cyber ecosystem through the evaluation and assessment under The EU Cybersecurity Certification Scheme. Therefore, according to Article 51 Regulation (EU) 2019/881, the certification would achieve various cybersecurity objectives. A number of cybersecurity objectives include information security, access control, vulnerability assessment, user activity monitoring, cyber resilience, security by design, and patch management.[62]

Conclusion

The Cybersecurity Act is the first international regime that regulating the internal market in responding to challenges related to the security of ICT products, ICT services, and ICT processes in the Digital Single Market. Through the establishment of The EU Cybersecurity Certification Scheme, The European Union would have a harmonized approach in dealing with the evolving cyberthreats that previously harm the society just as hazardous as catastrophic events. The implementation of the standardization in the EU-wide certification scheme would potentially increase cybersecurity and build cyber resilience that contributes positively to the Digital Single Market into a more digitally mature digital market. This is in line with the basic assumption of the theory of neoliberal

single-market/en/eu-cybersecurity-certification-framework , accessed 21 January 2021.

62 IT Governance. "The EU Cybersecurity Act", https://www.itgovernance.co.uk/eu-cybersecurity-act, accessed 21 January 2021.

institutionalism that emphasizes the necessity of institutions in strengthening cooperation in dealing with international issues.

BIBLIOGRAPHY

Book

Boin, Arjen. The Politics of Crisis Management: Public Leadership Under Pressure. Cambridge: Cambridge University Press, 2005.

Cassleman, Rick. "Expanding Cyber Resilience Beyond Convention Resiliency and Nuclear Command, Control, and Communications". In On the Horizon: A Collection of Papers from the Next Generation, Maryland: Rowman & Littlefield, 2020.

Keohane, Robert O. After Hegemony: Cooperation and Discord in the World Political Economy. New Jersey: Princeton University Press, 1984.

PWC. "Information Security Breaches Survey 2015". In ISBS Technical Report Blue. London: HM Government, 2015.

Suardi, Moh. Ideologi Politik Pendidikan Kontemporer. Yogyakarta: Deepublish, 2015.

I.V, A, and K A.I. "Model Management Trends and the Digital Economy: from Regional Development to Global Economic Growth." In Digital Maturity: Definition and Model. 2nd International Scientific and Practical Conference. Amsterdam: Atlantis Press, 2020.

Journals

Annarelli, Alessandro. et al. "Understanding the Management of Cyber Resilience Systems". Elsavier Ltd, (September 2020). Accessed 20 November 2020, doi: https://doi.org/10.1016/j.cie.2020.106829.

Backman, Sarah. "Conceptualizing Cyber Crises". Journal of Contingencies and Crisis Management, (December 2020): 429-438. Accessed 13 April 2022, doi: https://doi.org/10/1111/1468-5973.12347.

Bechara, Fabio R, and Samara B Schuch. "Cybersecurity and Global Regulatory Challenges". Journal of Financial Crime Vol. 28, No. 2, (November 2020): 359-374. Accessed 12 December 2020, doi: https://doi.org/10.1108/JFC-07-2020-0149.

Dumitru, Ovidiu Loan and Andrei Viorel Tomescu. European Consumer Law in The Digital Single Market. Juridical Tribune Vol. 10, No. 2, (June 2020): 1-17. Accessed 7 August 2020, doi: https://ssrn.com/abstract=3641921.

Goodman, E.F. "Your Duty If You Discover a Data Breach." American Bar Association, (2008): 16-19.

Holtfreter, R.E., and A Harrington. "Data breach trends in the United States." Journal of Financial Crime Vol. 22, No. 2, (2015): 242-260. Accessed 5 June 2020, doi: https://doi.org/10.1108/JFC-09-2013-0055.

Kamble, R.M. "Cyber Law and Information Technology". International Journal of Scientific and Engineering Research, Vol. 4, No. 5. Accessed 13 April 2022, ISSN 2229-5518.

Keohane, Robert O and Lisa L Martin. "The Promise of Insitutionalist Theory." International Security, Vol. 20, No. 1. (Summer 1995): 39-51.

Sabillon, Regner. et al. "Cybercrime and Cybercriminals: A Comprehensive Study". International Journal of Computer Networkds and Communications Security, Vol. 4, No. 6, (June 2016): 165-176, accessed 13 April 2022, E-ISSN 2308-9830.

Semma, P.S. et al. "Overview of Cyber Security". International Journal of Advanced Research in Computer and Communication Enginering. Vol. 7, No. 11, (November 2018): 125-128, accessed 13 April 2022, doi: https://doi.org/10.17148/IJARCCE.2018.71127.

Stanciu, Victoria and Andrei Tinca. "Exploring Cybercrime – Realities and Challenges". Journal Accounting and Management Information System. Vol. 16, No. 4, (2017): 610-632, accessed 13 April 2022, doi: http://dx.doi.org/10/24818/jamis.2017.04009.

News

Dellinger, A. "Tellefonica WannaCry Ransomware: One of Spain's Largest Telecom Companies Hit By Cyberattack". IB Times, (5 December 2017): 1.

Ecommerce News. "Ecommerce in Europe". Ecommerce News, (November 2021): 1.

Field, Matthew. "WannaCry Cyber Attack Cost the NHS £92 m as 19,000 Appointments Cancelled". The Telegraph, (11 October 2018): 1.

Paper

Abubakar, Ahmed Umar. Business Law. Honolulu: Atlantic International University. 2006.

Internet Script

Alert (TA16-091A). "Ransomware and Recent Variants". https://us-cert.cisa.gov/ncas/alerts/TA16-091A. Accessed 20 December 2020.

Boichenko, Tetiana. "How to choose a reliable big data enterprise analytics provider?". https://www.n-ix.com/how-choose-big-data-enterprise-analytics-provider/. Accessed 22 December 2022.

Britannica, T. "Business Law". https://www.britannica.com/topic/business-law.

Accessed 21 December 2020

Cavallo, Marco Antonio. "The Growing Importance of the Technology Economy". https://www.cio.com/article/3152568/the-growing-importance-of-the-technology-economy.html#:~:text=Technology%20has%20deeply%20affected%20the,and%20more%20robust%20international%20trade. Accessed 21 December 2020

Deloitte. "Cyber Crisis Management". https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/cyber-crisis-management.html. Accessed 21 December 2020.

ENISA. "Bolstering ENISA in The EU Cybersecurity Certification Framework". https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework. Accessed 22 December 2020.

ENISA. "Information security and privacy standards for SMEs". https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport. Accessed 22 December 2020.

European Commission. "Cloud Computing". https://digital-strategy.ec.europa.eu/en/policies/cloud-computing. Accessed 22 December 2020.

European Commission. "Digital Economy and Digital Society Statistics at Regional Level". https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_digital_society_statistics_at_regional_level. Accessed 22 December 2020.

European Commission. "Digital Transformation Scoreboard 2018 EU business go digital: Opportunities, outcome, and uptake". https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Digital%20Transformation%20Scoreboard%202018_0.pdf. Accessed 22 December 2020.

European Commission. "Integration of Digital Technology by Enterprises". https://ec.europa.eu/digital-single-market/en/integration-digital-technology-enterprises. Accessed 13 April 2021.

European Commission. "The EU Cybersecurity Act Brings a Strong Agency for Cybersecurity and EU-Wide Rules on Cybersecurity Certification". https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity. Accessed 17 January 2021.

European Commission. "The EU Cybersecurity Certification Framework". https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework..Accessed 21 Janury 2021.

European Commission. "The European Single Market". https://ec.europa.eu/

growth/single-market_en. Accessed 22 December 2020.

European Union. "Division of Competences within the European Union". https://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=legissum:ai0020#:~:text=The%20EU%20has%20only%20the,attain%20the%20objectives%20provided%20therein. Accessed 21 January 2021.

Eurostat. "E-commerce statistics". https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Esales_remain_stable_over_recent_years. Accessed 13 February 2021.

HM Government. "The exchange and protection of personal data.". https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf. Accessed 17 April 2021.

IMD. "IMD World Digital Competitiveness Ranking 2019". https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019/. Accessed 12 December 2020.

IT Governance. "The EU Cybersecurity Act". https://www.itgovernance.co.uk/eu-cybersecurity-act. Accessed 21 Janury 2021.

Kostov, N. "WannaCry Attack hits Renault, 200.000-plus victims". https://www.marketwatch.com/story/wannacry-attack-hits-renault-200000-plus-victims-2017-05-15. Accessed 22 December 2020.

Regulation

COMMISSION STAFF WORKING DOCUMENTIMPACTASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and C".

Proposal For A Regulation of The European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification ('Cybersecurity Act').