Challenges of Universal Adoption of The Budapest Convention on Cybercrime

Agus Nilmada Azmi[1], Syarah Shabrina[2]
[1]FISIP UIN Syarif Hidayatullah, Jl. Kertamukti , Ciputat, Banten, Indonesia
[2]FISIP UIN Syarif Hidayatullah, Jl. Kertamukti , Ciputat, Banten, Indonesia

E-mail Coresponding-author: agus.nilmada.azmi@uinjkt.ac.id

Abstract

This research analyses the challenges of universal adoption of the Budapest Convention on Cybercrime. The development of science and technology has experienced a very rapid movement that cannot be separated from its negative implications. One of them is the emergence of cybercrime attacks, or cybercrimes that utilize all loopholes and tricks on the sidelines of technological advances. Cybercrime has evolved into a transnational or international crime. The Budapest Convention on Cybercrime is an international treaty that governs matters related to cybercrime. Most countries in the world have adopted and ratified it, but some countries, such as Russia, India, and Brazil, have chosen not to. This study seeks to identify the challenges faced in adopting the universal Budapest Convention. This study used qualitative-descriptive methods using observational data, literature, and documents related to the challenges faced in the universal adoption of the Budapest Convention. This challenge is faced by the Council of Europe as the initiator of this convention by creating an agenda to realize the universal adoption of the Budapest Convention in order to take it into account and overcome it, especially related to combating cybercrime.

Keyword: Budapest Convention; Cybercrime; Adoption

A. Introduction

The development of science and technology in the present can be said to have experienced a very rapid movement. The telegraph and radio technologies that emerged in the 20th century were remarkable achievements. It is inconceivable that both have been replaced by the internet world with their giant sea cable connections today. Information that exists in one corner of the world can be received and accessed by others in another corner of the world.

Borders, both geographical (such as mountains and seas) and political (such as countries), no longer exist. However, all the advantages and advances obtained from the development of science and technology will certainly not be separated from ugliness and setbacks. It's can be seen in the emergence of cybercrime attacks or crimes in the cyber world.

Technological advances, through the existence of the internet, make various types of crimes today possible to carry out across national borders. Cybercriminals take advantage of loopholes and tricks in between technological advances to carry out their crimes. Cyberattacks began to be discovered in 1999, when the Melissa computer virus spread the world via email (Katie, 2020). It takes more than US$80 billion to clean and repair computer systems affected by the virus (FBI, 2019).

There is also a distributed denial of service (DDoS) attack on the world's largest websites, such as CNN, Amazon, Yahoo, and eBay, launched in 2000 by a hacker named Michael Calse, who was 15 years old at the time. It caused the collapse of several websites over several hours, resulting in millions of dollars in losses (Wolf, 2022). These attacks show that cybercrime can not only cause huge financial losses, but it can also be carried out by anyone, against anyone, and wherever they are. In other words, cybercrime is a crime that is transnational.

With the cross-border nature and rise of cybercrime, law enforcement efforts are increasingly becoming a priority for every country in the world, one of which is the use of international legal instruments. Although the situation is urgent and on the agenda around the world, so far there is only one cross-border legal instrument that explicitly regulates cybercrime, namely the Budapest Convention on Cybercrime. The Budapest Convention on Cybercrime was established in 2001 by the Council of Europe with the active participation of observer states from international organizations.

For more than 20 years, the Budapest Convention has been signed and ratified by 67 countries in the world, consisting of 46 member states of the Council of Europe and 21 non-member states (Chart of Signatures and Ratification of Treaty 185, 2001). The Budapest Convention is considered the only international treaty that governs cybercrime. Many countries feel that they have various reasons not to ratify the treaty because it is important for their security. They also consider that there is no other international agreement whose member states cover most countries in the world.

Although most countries in the world have adopted and ratified the Budapest Convention, others, such as Russia, India, and Brazil, have chosen not to. Thus, the study seeks to identify the challenges faced in the universal adoption of the Budapest Convention around the world.

B. Research Method

The research uses qualitative-descriptive methods to answer the challenges faced in the universal adoption of the Budapest Convention. Qualitative research is research that can produce descriptive data, both written and oral, from people and their observable behaviour. Qualitative research aims to understand and explore a problem both for individuals and groups in the social environment. Qualitative research is applied in a descriptive form (qualitative-descriptive) to explain and describe problems related to the challenges of universal adoption of the Budapest Convention in the international realm in the face of cybercrime. The use of qualitative-descriptive methods requires the identification and collection of data through observation, interviews, literature, and documents related to research. From these data, the author can then explain, describe, compile, explain, and analyze them so that they can produce the information you want to seek through the research (Creswell, 2013).

C. Results and Discussion

Cybercrime is a crime committed using the internet, such as stealing someone else's personal information or introducing a malicious program to someone else's computer (MacMillan Dictionary, n.d.). In another definition, cybercrime is defined as the use of computers as a tool to do illegal things such as committing fraud, distributing child pornography and intellectual property, identity theft, or invasion of privacy (Britannica, 2022). In addition, cybercrime is also said to be an umbrella term that includes crimes formed by computers, where computers and technology are used as auxiliary roles for the crime (Bossler & Berenblum, 2019, p. 495). So, briefly, the term cybercrime refers to a type of crime committed through computers that occurs in cyberspace or through internet media.

The Budapest Convention on Cybercrime

The Budapest Convention, also known as the Convention on Cybercrime, is an international treaty convention that aims to improve the process of investigation and cooperation between countries in dealing with and preventing cybercrime. The Budapest Convention is an international cooperation mechanism in the face of Internet-based

challenges to investigate crimes that do not fall into international connections, where countries that have adopted or ratified the convention contribute to each other to think of easier and more efficient ways of international cooperation in criminal investigations of cybercrime (The Budapest Convention on Cybercrime (ETS No. 185) and its Protocols, 2001).

The Budapest Convention became a key instrument for harmonizing cybercrime laws and developing a common judicial area for cyberspace more generally. In addition, the convention has also become the world's first international treaty aimed at cybercrime and encourages the regulation of cybercrime in accordance with human rights and the rule of law. The Convention was adopted by the Council of Europe Committee of Ministers on November 8, 2001, and opened on November 23, 2001, in Budapest, Hungary. The opening of the convention was also attended by countries outside the members of the European Council and the European Union (EU), such as the United States, Canada, Argentina, Japan, and South Africa (Parashar, 2019, p. 131). It can be said that the convention is an open treaty for third countries outside the European Council and the EU.

The main priority of the agreement is to encourage international cooperation in achieving a common policy in terms of public protection against cybercrime by adopting appropriate regulations. In addition to facilitating operational cooperation, the convention has also established guidelines for developing and harmonizing different national legal frameworks. It is shown there is general agreement in Europe that the convention has represented major progress in creating a common judicial area to deal with cyber problems (Renard, 2018, p. 333).

The Convention has been supplemented by laws or treaties that are used as harmonization to provide approaches that can facilitate effective cooperation between states participating in the Convention and global law enforcement agencies. In fact, it shows that all the instruments contained in it are also to promote European global norms. The broad acceptance of the convention has been seen by the EU as an important condition for providing financial support for cyber capacity building in third countries or countries other than the Council of Europe or the EU. Thus, after the Convention took place, many of the states that had signed and ratified it to be applied to their respective national laws.

All results of the Budapest Convention have been contained in European Treaty Series No. 185, also known as the Convention on Telematics Crimes. As for the treaty, there are three main objectives of the Budapest Convention, including:

1. Articles 2–11, namely the alignment of the national framework through the integration of cybercrime lists the scope of the convention not only covers crimes against computer systems and data but also covers other electronic means such as fraud, dissemination of child sexual abuse material, and copyright infringement.
2. Articles 16–22, namely, to improve cybercrime investigation techniques Each country that adopts it must also foresee new search and seizure powers for local law enforcement authorities and force internet access providers to store user data to monitor online activity in real time.
3. Articles 23–35 promote and expand international cooperation, whereby each adopting state shall assist the law enforcement authorities of other States Parties to the widest extent possible. Despite originating in Europe, the agreement eventually caught the attention of non-European countries and thus became a global benchmark. Since 2001, 66 major non-European countries such as the US, Canada, Argentina, Japan and South Africa have ratified the treaty providing a consistent and technically neutral approach to cybercrime.

Regulations and Forms of Cybercrime in the European Convention on Cybercrime

The following are the rules contained in the European Convention on Cybercrime:

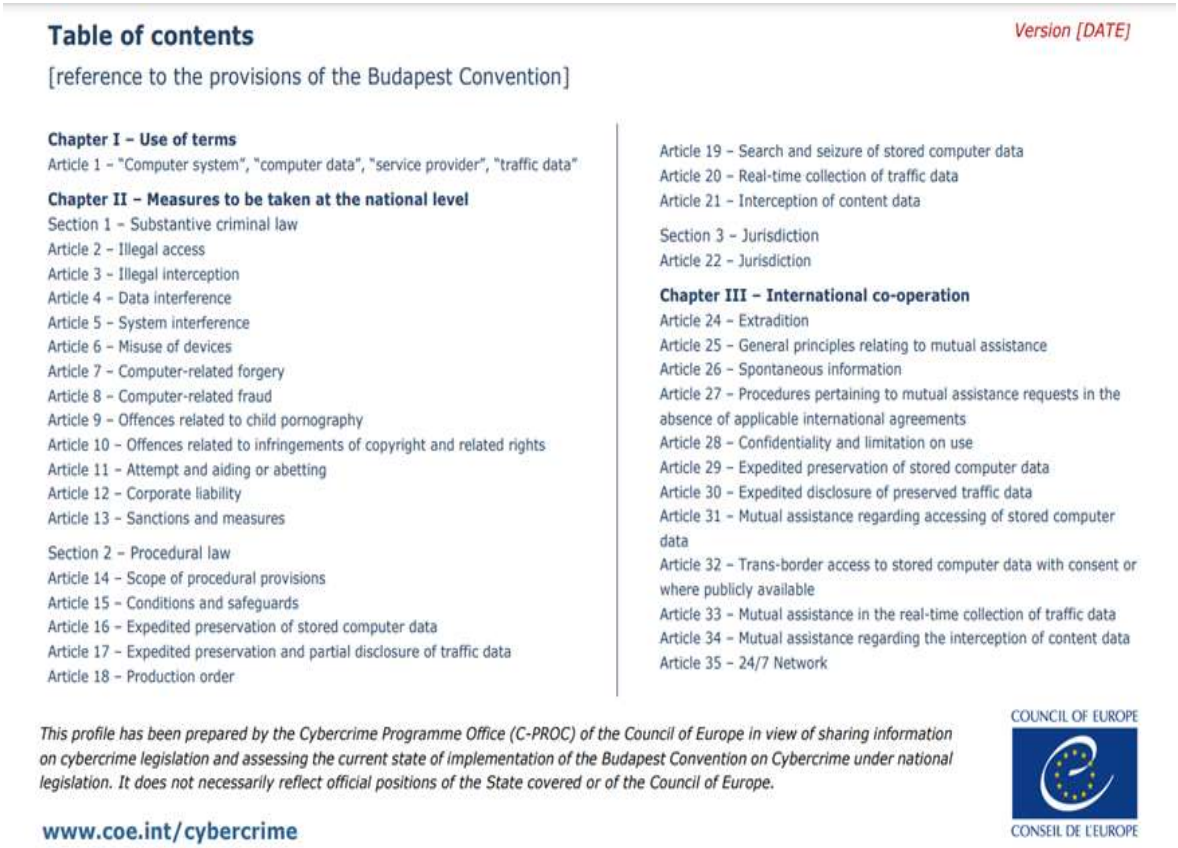

Table of contents

Version [DATE]

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Source: Council of Europe. Cybercrime Legislation. Domestic Equivalent to the Provisions of the Budapest Convention. (https://rm.coe.int/octocom-legal-profile-kosovo/16809e5451)

In the regulations of the European Convention on Cybercrime, there are also several forms of cybercrime, among others (The Budapest Convention on Cybercrime (ETS No.185) and its Protocols, 2001):

1. Illegal Content, is the entry of data and information that contains elements that are not good, violate the law, and disturb public order.
2. Illegal Access, is accessing computer systems without permission, which includes threats and attacks that are dangerous so that they can disrupt the security of data and computer systems.
3. Illegal Interception, is a technical interception, transmitting computer data, and emitting electromagnetic that carries data from the computer.
4. Data Interference, is the destruction, deletion, alteration, and hiding of computer data intentionally and without permission such as inserting malicious codes, viruses, and so on.
5. System Interference, is inserting, transmitting, damaging, deleting, aggravating, altering, and hiding computer data so that it can interfere with other data systems.
6. Misuse of Device, is the misuse of equipment both software and hardware that has been modified to gain access from a computer or computer network.

7. Computer Related Offences, Forgery, and Fraud, is an activity that commits forgery and fraud through computer networks.
8. Offences Related and Child Pornography, is an activity related to child pornography content.
9. Offences Related to Infringements, are activities related to infringement of copyright and related rights

Therefore, the convention has played a useful role in setting international standards on key issues that, by definition, have involved and affected actors in different jurisdictions. The existence of the convention is enough to attract worldwide attention because the fight against cybercrime and the maintenance of cyber security have become important concerns for companies, public administrations, and all individuals associated with them.

Challenges to Universal Adoption of the Budapest Convention (Russia, India, and Brazil's Rejection of the Budapest Convention)

1. Russia

Over the past few decades, Russia has wanted to advocate a new cybercrime treaty despite the Budapest Convention. Although Russia has become a member of the Council of Europe, it has been reluctant to join the Budapest Convention, claiming that it violates state sovereignty by allowing cross-border cybercrime operations. Russia is the only member state of the Council of Europe that has not signed the Budapest Convention. According to him, the convention is outdated and no longer efficient due to new types of cybercrime and threats that have emerged in recent years (TASS, 2021).

It's makes Russia more struggling to form a cybercrime agreement with an international scope. Russia began its efforts by submitting a resolution to the UN General Assembly to create a new mechanism to combat cybercrime called the International Technical Commission. The resolution was strongly challenged by many countries, such as the US, Australia, and especially European countries. In addition, the resolution was also challenged by many civil society and human rights groups (Page, 2022). However, this did not make Russia unyielding, thus making it still insist on submitting its draft convention to the UN General Assembly.

In its draft, Russia outlines several procedures for cooperation between countries in extraditing hackers and providing legal assistance in criminal cases, including detecting crimes, arrests, seizures, and asset recovery. The draft is contained in a document called the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (TASS, 2021).

Article 32 of the Budapest Convention states that parties that have adopted the convention may receive and access publicly available information data, regardless of geographical differences (Convention on Cybercrime: Article 32, 2001). So, in addition to its national interests, the article became the basis for Russia to reject the Budapest Convention because, according to him indirectly, the convention would endanger state sovereignty because cybercrime not only attacks one aspect but can paralyze a country and interfere with the principle of sovereignty of a state.

Meanwhile, Russia has also long owned and regulated the law on the issue of cybercrime through Article 28 of the Criminal Code of the Russian Federation and Law of the Russian Federation of 27.07.2006 Number 149-FL "On Information, Information Technologies, and Protection of Information". The existence of these two pieces of legislation, especially in Article 28 of the Criminal Code of the Russian Federation, makes it unnecessary for Russia to

adopt the Budapest Convention (Wirasisya & Warsito, 2021, pp. 99–100). In other words, Russia has no interest in adopting the convention.

2. India

Between 2007 and 2008, India and the Council of Europe cooperated on reforms to the Indian Information Technology Act, which broadly aligned with the Budapest Convention. Meanwhile, the number of memberships in the Budapest Convention is about two times higher. India is the third country in the world affected by WannaCry ransomware because it was hit by more than 40 thousand computers. Even if viewed to date, India continues to experience an increase of more than 7 million crimes that require electronic evidence (Parashar, 2019, p. 131). Despite this being a matter of its territorial jurisdiction, India is still not a signatory to and has not ratified the Budapest Convention. India did not give a clear reason, but there were some who concluded that there were actually concerns voiced by various stakeholders.

First, India did not participate in the negotiations and draft the Budapest Convention, so it was not allowed to sign it. In fact, the parties to the convention agree and prefer that India contribute to and participate in the negotiations of the convention. The Budapest Convention is also a consideration for India; it has just ratified two other agreements with the Council of Europe that it did not negotiate on tax issues, the Organization for Economic Cooperation and Development (OECD), and the Convention on the Transfer of Sentenced Persons. Another consideration is that of the national interest on which accession to the treaty is based, which should also apply in the case of the Budapest Convention on the basis of similar national interests.

Secondly, Article 32b of the Budapest Convention has made it possible for cross-border access to data, which would infringe on national sovereignty. The Committee on Cybercrime Convention has further confirmed the limited scope of Article 32b. This has led some in the Indian government to criticize that Section 32b is too limited and should require additional options (Seger, 2016). Third, feel held hostage by diplomatic and foreign policy considerations and a lack of attention to actual criminal justice cooperation on cybercrime and electronic evidence.

Fourth, there are doubts about India's priority guarantees on terrorism issues and its national regulatory assistance related to cyber terrorism (Kovacs, 2016). Fifth, India already has its own regulations related to cybercrime through the Information Technology Act 2000 (IT Act 2000) and the Information Technology Amendment Act 2008 (IT Act 2008), which are particularly considered a good development in protecting cyber infrastructure in India (Hanna, 2022). The legislation was made in cooperation with the Council of Europe, which is broadly not much different from the Budapest Convention, so there is no urgency for India to join the Budapest Convention. In other words, India no longer has an interest in adopting the convention.

Thus, it's has become a challenge for the parties to the Budapest Convention. In fact, they have offered many advantages, ranging from offering a legal basis to a practical framework for security and judicial cooperation on cybercrime, as well as other electronic evidence so that these frameworks can be reviewed more effectively. Moreover, as the convention evolves, India can also contribute to shaping future solutions if it becomes a party and becomes a priority country in capacity building related to cybercrime. This is keeping in mind Prime Minister Narendra Modi's vision of a digital India, and considering the surge in cybercrime, it would be beneficial for India to join the agreement. (Seger, 2016).

3. Brazil

Brazil has declared itself sceptical of joining the Budapest Convention. Brazil considers that the convention is discriminatory. The parts of the drafting process has created the same concerns as India. However, for the accession application, the Council of Europe invited Brazil to agree to the convention in December 2019, which is aimed at making Brazil a priority country in the same capacity-building program as India. (Ebert & Groenendaal, 2020)

However, the Brazilian government insists it does not want to sign the Budapest Convention, so it is actively shaping domestic and international norms regarding cybercrime. At the domestic level, some of the cybercrime laws contained in the Budapest Convention conflict with laws on privacy and data protection. Ultimately, through President Rousseff, Brazil developed a cybercrime law that is stronger, more likely, compliant for governments and security forces to access data without a court order, but still in line with the preferences of law enforcement agencies.

In addition, Brazil is also making laws that modify the criminal code in general to define electronic crimes and categorize and determine penalties for various types of cybercrime that have not previously entered criminal law. However, both articles of the law make unauthorized access to computer devices a criminal offense (Yustani, 2028, p. 21). It can be said that Brazil has made regulations related to the issue of cybercrime in its own way. The regulation, called the National Cyber Security Strategy, came into effect in February 2020.

In its regulations, the National Cyber Security Strategy makes at least 10 strategic actions, including strengthening international cooperation, centralizing the national cyber security system, increasing protection for critical infrastructure, and strengthening cyber governance in both the public and private sectors (Stronell, 2020). At the national level, the National Cyber Security Strategy emphasizes building information channels related to cyber vulnerabilities, incidents, and risks. The various information is written in SK 10.046 of 2019, which defines governance for various data at a broader, limited, and specific level (Hurel, 2021, p. 22).

Meanwhile, at the international level, Brazil is more inclined toward cybercrime collaboration, international cooperation exercises related to cybersecurity, and foreign policy consolidation. It has been seen that Brazil refused to adopt the Budapest Convention because, in the drafting process, they did not include extensively developing countries such as Brazil and India (Kovacs, 2016).

Therefore, Brazil basically has the same position as India, which is not to oppose the Budapest Convention but to use it as a guideline to reform its national legislation, but also not to support it because there is no involvement of its country in the drafting process.

D. Conclusion

The Budapest Convention, as a treaty that focuses on cybercrime, is still having difficulty spreading its wings in the world, namely by adding countries to sign and ratify it. It's can be seen from the reluctance of Russia, India, and Brazil to join the convention based on reasons of sovereignty and national interests. All three countries considered that if they entered into the Budapest Convention, it would threaten their sovereignty and be solely incompatible with their national interests. The existence of national legislation on cybercrime in the three countries has been a challenge for the Budapest Convention because there is no urgency or interest for the three countries to adopt it.

It is undeniable that the Budapest Convention has become a 'benchmark' for countries in the world to model their national legislation on the convention, as India did. However, it also did not encourage universal adoption of the convention, as India did. Therefore, these challenges must be faced by the Council of Europe as the initiator of the convention, which

must create an agenda to realize the universal adoption of the Budapest Convention in order to take into account and overcome the challenges faced.

References

Bossler, Adam M & Tamar Berenblum. (2019). Introduction: New Direction in Cybercrime Research. Journal of Crime and Justice. Vol. 42. No. 5. 495-499. https://doi.org/10.1080/0735648x.2019.1692426.

Britanica. (2023). Cybercrime. https://www.britannica.com/topic/cybercrime.

Chadd, Katie. (2020). The History of Cybercrime and Cybersecurity 1940-2020. Cybercrime Magazine. https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/.

Council of Europe. (2001). Chart of Signatures and Ratifications of Treaty 185. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

Council of Europe. (2001). Convention on Cybercrime: Article 32. https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf.

Council of Europe. (2001). Cybercrime Legislation. Domestic Equivalent to the Provisions of the Budapest Convention. https://rm.coe.int/octocom-legal-profile-kosovo/16809e5451.

Council of Europe. (2001). The Budapest Convention on Cybercrime (ETS No. 185) and its Protocols. Explanatory Report to the Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

Creswell, John W. (2012). Qualitative Inquiry & Research Design (Edisi Ke-3). USA: Sage Publication.

Ebert, Hannes & Laura Groenendaal. (2020). Brazil's Cyber Resilence and Diplomacy: The Place for Europe. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2IbYw_1n/brazil_digital-dialogue_eucd_he.pdf.

Federal Bureau of Investigation (FBI). (2019). The Melissa Virus. https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519.

Hanna, Katie Terrell. (2022). Information Technology Amendment Act 2008 (IT Act 2008). https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008.

Hurel, Louise Marie. (2021). Cybersecurity In Brazil: an Analysis of the National Strategy. Igarape Institute: Strategic Paper 54. https://igarape.org.br/wp-content/uploads/2021/04/SP-54 Cybersecurity-in-Brazil.pdf .

Jemadu, Aleksius. (2008). Politik Global dalam Teori dan Praktik. Yogyakarta: Graha Ilmu.

Kovacs, Anja. (2016). India and The Budapest Convention: To Sign or Not? Considerations for Indian Stakeholders. Report: Internet Democracy Project. https://cdn.internetdemocracy.in/idp/assets/downloads/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/Dr.-Anja-Kovacs-Inda-and-the-Budapest-Convention.pdf

Legal Information Institute. Sovereignty. https://www.law.cornell.edu/wex/sovereignty#:~:text=Sovereignty%20is%20a%20political%20concept,%22sovereign%22%2C%20or%20king.

MacMillan Dictionary. Cybercrime. https://macmillaneducation.secure. force.com/help/.

Page, Mercedes. (2022). The Hypocrisy of Russia's Push for a new Global Cybercrime Treaty. Lowy Institute. https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

Parashar, Deepak. (2019). Budapest Convention on Cybercrime: Assessment of India's Concert. ILI Law Review. Vol. 2. Winter Issue. 126-143. https://www.ili.ac.in/pdf/dpa.pdf.

Renard, Thomas. (2018). EU Cyber Partnership: Assessing the EU Strategic Partnership with Third Countries in the Cyber Domain. European Politics and Society. Vol. 19. No. 3. 321-337. https://doi.org/10/1080/23745118.2018.1430720.

Riyanto, Sigit. (2017). The Emergence of Universalism and The Decline of Supranationalism. Mimbar Hukum. Vol. 29. No. 2. 308-320. http://dx.doi.org/10.22146/jmh.23873.

Seger, Alexander. (2016). India and The Budapest Convention: Why Not?. Observer Research Foundation (ORF). https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

Stronell, Alexander. (2020). Brazil's Cyber Security Strategy Leaves Much to be Desired. International Institute for Strategic Studies (IISS). https://www.iiss.org/online-analysis/online-analysis//2020/09/csfc-brazils-cyber-security-strategy.

TASS. (2021). Press Review: Russia Unveils Bid to Fight Cybercrime and Samsung Pay Faces Patent Issue. https://tass.com/pressreview/1320973.

Wirasisya, Muhammad Granit Ady & Tulus Warsito. (2021). Penolakan European Convention on Cybercrime oleh Rusia dalam Mempertahankan Kepentingan Nasional. Vol. 12. No. 1. http://openjournal.unpam.ac.id/index.php/ sks/article/view/10210.

Wolf, Arctic. (2022). A Brief History of Cybercrime. https://arcticwolf.com/ resources/blog/decade-of-cybercrime/

Yustani, W., dkk. (2018). Keamanan Sistem Informasi. Sidoarjo: Zifatama Publishing.