Jurnal Dinamika Global Vol. 8 No. 2, Desember 2023
P-ISSN 2548-9216 | E-ISSN 2684-9399

EUROPEAN UNION CYBER SECURITY IN DEALING WITH THE THREAT OF AI-CYBERCRIMES: LESSONS FOR INDONESIA

Mutia Hariati Hussin[1], Raninta Salwa Prilia Ginano[2]
[12]Department of International Relations, Faculty of Social and Political Sciences, Universitas Muhammadiyah Yogyakarta
[1]mutiahussin.suryo@umy.ac.id

Abstract

This paper discusses the evolution of Artificial Intelligence technology-related crimes, responses and mitigation initiatives taken by the European Union. This study aims to provide information about the early development of AI to how it is used as tool for cybercrime called deepfake. To collect data for this study, the qualitative research methodology will be used to gain information from a range of sources, such as pertinent books, news articles, and journals. The authors found that Artificial Intelligent, or AI, has become important part of daily lives. While it has provided benefits, it also created new problem such as artificial child pornography and porn being exploited for various reasons. This becomes a significant international risk to cybersecurity. The sensitivity and intricacy of this topic call for coordinated efforts from many different parties. In response to this problem, the European Union has formed their own solutions that Indonesia could learn from.

Keywords: cyber security, cybercrime, artificial intelligence, mitigation, European Union

INTRODUCTION

Marvin Minsky, an American cognitive and computer scientist specializing in AI or Artificial Intelligence defines AI as *"The science of making machines do things that would require intelligence done by men."* (Bolter, 1984). In short, AI is a new technology that is capable of mimicking the cognitive function of the human mind (Xie, Hwang, & Wong, 2021). The birth history of AI began in the mid-20th century when scientists and mathematicians such as Alan Turing began to think of possible computers that could mimic human thinking. In 1950, Alan Turing published an important article on "Computing Machines and Intelligence", describing how to build intelligent machines and test their intelligence. The experiment considered a measure to identify artificial system intelligence. An artificial system can be said to be intelligent when humans interact with humans and machines that cannot distinguish the two.

In 1956, John McCarthy and Marvin Minsky introduced the term "artificial intelligence" and defined computer programming as "human intelligence simulation." This meeting marked the start of the AI Spring funded by the Rockefeller Foundation which reunited the pioneers of AI (Haenlein & Kaplan, 2019). In the 1960s, computers began to be used in image processing. This was the beginning of the development of photo-computing technology. Although the computer's ability to recognize and process images was still limited, technological development was accelerating. The most significant development in photo-computing technology came with the advent of deep learning, which enabled the creation of deep and complex imitation neural networks. This technology allows computers to learn automatically from data, including images and videos.

Deep learning opens the door to deepfake development. Deepfake is the use of deep learning techniques to create highly convincing multimedia content, often disguised as public or individual figures (Hanif & Dave, 2022). This deepfake technology enables the creation of fake videos with very real sounds and faces, even when the original never happened. Deepfake originally appeared as a hobby or technical experiment. Over time, however, this trend developed into a serious worldwide problem. Anxiety grows along with deepfake's ability to spread false information, defame reputation, and be used in fraud (Becker & Laycock, 2023).

The problems caused by deepfakes have also spread in Europe. Some of the problems are: 1) the spread of false information. Deepfake can be used to create fake videos or audio that look very authentic. This creates a major risk in the dissemination of false information, which can affect public opinion and political decisions. 2) the security threat. Deepfake has the potential to be used in criminal fraud. Fraud involving deepfakes may include forgery of a person's face or voice for financial fraud purposes. 3) the political interest. Deepfake is also a concern in the political context. Creating fake videos of political figures or state leaders can create chaos and instability. Finally, 4) in terms of privacy and human rights, deepfake can involve invasion of privacy, such as creating fake intimate videos of individuals. This involves serious human rights issues.

Therefore, based on the above exposure this article will explain how AI development especially in deepfake system advancements can pose a threat to today's cyber systems. This article will take a case study that took place in Europe on European responses to trends in deepfake use. Thus, it is hoped that through this article, we can take lessons from Europe's handling of deepfake development, which can finally be used as a reference by cyber security in Indonesia. Indonesia can learn lessons from Europe's response. The Indonesian government can develop similar regulations to control the use of deepfake. Education and public awareness of deepfake threats are also essential. Regional and international cooperation can help Indonesia face cybersecurity challenges more effectively. In the increasingly complex digital age, efforts to protect communities and institutions from deepfake threats are becoming essential. With appropriate measures, Indonesia can face these challenges and ensure better cybersecurity in the future. Henceforth this article addresses the following inquiry of how can Indonesia learn from the European Union cyber security measures in fighting digital age, AI-cybercrime.

Theoretical Frameworks

Cybersecurity and Cybercrime

Cybersecurity is a concept that includes the domain of “cyber” and “security”. “Cyber” refers to cyberspace which consists of electronic communication networks and virtual reality. Cyberspace is commonly known to be designed as an environment that consists of information. Cyberspace is by nature dynamic, evolving, and multilevel. The implementation of cyberspace can be found in physical infrastructure, software, regulations, ideas, innovations, and interaction that is influenced by the expanding population of contributors which represent ranges of human intentions (Craigen, Diakun-Thibault, & Purse, 2014). On the other hand, “Security” refers to a discourse that necessarily includes an actor who securitizes threats tailored to the referent object under a certain condition or structure. Security’s meaning varies based on one’s perspective and value. Therefore, the security definition is a contested term, however, it always revolves around being free from danger or threat (Craigen, Diakun-Thibault, & Purse, 2014).

Meanwhile, Cybercrime, similar to cyber security can also be applied in a wide variety of scenarios and is prone to confusion to be distinguished from other forms of cyberthreats such as cyber warfare or cyberterrorism. In broad, cybercrime encompasses a wide number of acts, crimes, or illicit conduct perpetrated by individuals or groups against computer-related devices or information technology networks, and also traditional crimes that are done by the usage of the internet or information technology (Phillips, et al., 2022). Operationally, Sarah Gordon and Richard Ford suggest that cybercrime should be subdivided into two distinct types which are Type I and Type II Cybercrime. Type I Cybercrime refers to:

1. It is generally a singular, or discrete, event from the perspective of the victim
2. It often is facilitated by the introduction of crimeware programs such as keystroke loggers, viruses, rootkits, or trojan horses into the user's computer system
3. The introduction can be, but not necessarily, facilitated by vulnerabilities (Gordon & Ford, 2006).

However, putting aside the cybercrime's definition complexity, the term cybercrime is viewed differently on an organizational level. For example, The European Commission describes cybercrimes into three categories:

1. Offences unique to computers and information systems
2. Traditional offences
3. Content-related offences (Phillips, et al., 2022).

As AI grows and become common on cyberspace, Sarre, Lau and Chang extend the two-spectrum approach made by Gordon and Ford and presents the three-factor spectrum which adds Type III Cybercrimes that refers to cybercrimes perpetuated by AI, bots, or self-learning technology (Phillips, et al., 2022).

The AI technological growth has then transformed and used commonly for Type III cybercrimes, such as deepfakes in voices, image, videos and even pornography deepfake. The motives vary from fun use even to violence and monetization. AI crime has become advance that it is challenging to track down and tackle the problem. Both Europe Union and Indonesia are challenged in handling AI-related crime. While both countries have their own set of tools and legislation, the gap between them are too wide. With the advancement of European Union cybersecurity capability, Indonesia could learn many things from European Union.

Literature Review

Artificial intelligence (AI) is not new in International Relations but not yet popular. Undoubtedly, one of the most important and rapidly expanding areas of research in international relations is cyber security. Polls and the media's reaction to the topic imply that cyber dangers are one of the most critical issues on the world agenda. Still, scholars have needed help to take this framework's implications and prospective theoretical perspectives that could serve as a guide for research seriously. This part of article concentrates on what we already know about cyber security and crucial theoretical issues. Undoubtedly, cyber security is a crucial component of international relations, but does this sector develop original concepts or does it simply copy those of other security domains? Nowhere is this more evident than in Kello's article, which argues that present IR theories cannot meaningfully contribute to the study of cyber conflict and that the cyber danger continues to be unprecedented since it will widen the scope of harm in international interactions (Kello, 2013).

A study conducted by Bianca Britton, a reporter for BBC News, entitled ”They appeared in deep fake porn videos without their consent. Few laws protect them”, explained that the increasing prevalence of artificial intelligence-generated pornography, particularly deepfake videos, that feature faces of nonconsenting individuals, including popular influencers and streamers. It highlights a case involving the Twitch streamer "Sweet Anita," who discovered deepfake videos featuring her face edited onto explicit content online. The article also mentions how the number of deepfake pornographic videos has grown significantly over the years, with a focus on targeting individuals with smaller online footprints.

The ethical and legal challenges surrounding nonconsensual AI-generated pornography are explored, with some states in the United States having laws addressing deepfake media, and the United Kingdom planning to criminalize explicit nonconsensual deepfake content. Many victims of deepfakes feel helpless, as legal recourse is often limited. The article calls for holding platforms accountable for hosting such content and emphasizes the need for consequences for those involved in creating and distributing deepfakes.

A previous study conducted by Adriansyah Anugrah about the Indonesian law on the sexual violence crime (UU TPKS) explained that the passing of the TPKS Law provides an understanding of human rights, especially for women who are victims of sexual violence. The TPKS Law is the basis for law enforcement in Indonesia in enforcing and defining sexual violence. However, the presence of the TPKS Law in the judicial realm in Indonesia does not necessarily provide a positive breakthrough in handling sexual violence cases in Indonesia. The still high number of sexual violence occurring in 2020, ranging from rape, marital rape, and incest to cyber sexual violence, gives a clear picture that the passing of the TPKS Law is not enough moreover when the crime is done virtually in the cyber realm. The presence of the TPKS Law does not necessarily open the mental ability of victims to have the courage to speak out and even report the actions that occurred. Researchers believe that differences in law enforcement's knowledge in handling sexual violence cases are one of the factors driving the number of sexual violence to continue to increase.

Methodology

This research uses a descriptive qualitative methodology. The data collection would be from the secondary sources, such as journals, books, reports, official website, and news reports. The literature review is from previous research that correlates and have discussed the topic. After gathering the data, this research employs a descriptive approach and connect it to the theoretical framework to address the research question.

DISCUSSION

Deepfakes: Status quo

The term *deepfakes* in pornography came into public in 2017 when a Redditor created a subreddit titled Deepfakes and shared face-swapped videos of celebrities into pornographic videos (Payne, 2023). While Reddit, Github, and fake porn websites played major roles in the birth of deep fake porn, Twitter became the platform that held the most story and became the platform where deep fake grew rapidly. The victims of deepfake porn shared similar circumstances. For example, deepfake porn could be found majorly targeting women and following patterns of cyberspace-gendered abuse (Maddocks, 2020). Deepfake which is used to sexualize women is generally found on popular streaming websites such as Twitch and involves popular streamers such as Maya Higa and Pokimane. The videos that were being shared on Twitch were then massively distributed on popular platforms like Reddit, Facebook, TikTok, and Twitter (Britton, 2023).

According to Genevieve Oh, a livestreaming Analyst, 1,897 videos had been uploaded to a popular streaming site and this number has been increased to 13,000 videos in 2022 with over 16 million monthly views. The deepfake pornographic case later continued in early 2023 when a popular Twitch streamer namely "Atrioc" is found uploading an apology video where he admits subscribing and paying for deepfake pornographic content featuring a popular Twitch live streamer as the porn actress. This video was receiving millions of views with more than 300,000 followers (Britton, 2023). Deepfake issues are not limited to the United States but are also a problem in Europe where a series of pornographic contents involving the usage of deepfake is also been an issue since 2017, when a popular actress Gal Gadot appeared in a pornographic movie which was made by superimposing Gadot's face onto an adult movie star's body. This matter is getting worse in 2020 in Europe where 1000 deepfake videos are being uploaded to porn sites every month (Sorban, 2023).

Another popular case of deepfakes included the most-followed women in TikTok: Bella Poarch, Charlie D'Amelio, and Addison Rae Easterling. The three women's explicit content that were made by AI became the trending searches on Twitter on June 12, 2023. For example, an explicit video of a woman on a bed was plastered by Addison Rae's face generated by AI and earned more than 21 million views. Meanwhile, Bella Poarch had a similar situation as Addison Rae while Charlie D'Amelio and her family became the target of AI deepfake porn. While Twitter is said to have two regulations against AI deep fake porn such as non-consensual nudity and synthetic and manipulated media policy, Twitter has been criticized for its lack of taking action against the emergence of deep fake porn (Tenbarge, 2023).

Motives of deep fakes

The motives of deepfakes porn varied. The most common motive for deepfake is to fulfill sexual pleasure by bypassing consent. The logic here is that by using AI, the pornographic content can technically be deemed "fake" and therefore there would be no need to seek the consent of the victim. Bullying and blackmailing done by the abuser to coerce their victims is the second common motive. Abusers seek to use the deepfake porn to control and silence them to obtain what they desire. This motive would usually correlate with sextortion. Sextortion is an act of forcing someone to perform or provide explicit pornographic content of themselves to the perpetrator without their consent. Sextortion is achievable by using threats from AI-generated pornographic content until the target complies. Another common motive in deepfake porn is revenge porn. Revenge porn is the act of sharing explicit pictures to counteract the victim to inflict harm to the victim, be it socially or psychologically. Cases of revenge porn are often found between ex-lovers (Okolie, 2023).

Aside from personal motives, Deepfake pornography is also monetized. For example, the case of an AI-powered bot that can produce photo-realistic women's nudes. The AI access is free and accessible due to its user-friendly nature. User can simply upload pictures of their target and let the AI generate the pornographic pictures. Sensity, an AI-powered identity verification website found around 104,852 women's nude images were shared with the public and 70% of the targeted victims were only private individuals. With the high user traffic, the AI and channels affiliated with it had more than 100,000 worldwide members and 70% of them were Russians and former Soviet Union countries. The developer was able to monetize the AI and earned money from substantial advertising revenues through VK and Russian social media with underage girls making up the majority of the victims (Nir, 2023).

Children and minors were also targeted by sex predators. For example, in Spain, police detained a computer programmer who used AI to create child pornography images in early 2023. The police also found a huge pile of abhorrent images stashed at his home in Valladolid. The criminal created the AI command by downloading and inputting real images of young girls and babies being sexually harassed and putting them in the AI generator to produce indecent images of children. The images are found to be spread around across popular social media platforms such as Instagram, Facebook, and Twitter. Instagram stories are also used by predators to advertise online image catalogs of child sex abuse that need payment to be accessed. Messaging apps such as Telegram and WhatsApp are used to trade such pictures discreetly (Cotteril, 2023).

In Almendralejo, a town in Spain, another case of AI child porn was founded. The victims ranged from age 11 to 17 and there were around 28 girls who were the victims. Unlike the previously discussed case, the perpetrators were identified to be at least 11 local boys aged between 12 and 14 involved in creating to distributing the images via messaging apps such as WhatsApp and Telegram (Hedgecoe, 2023).

European Union: Action taken

Amidst the rise of AI Pornography cases around Europe, the European Union has passed a series of resolutions from 2017 to 2023 amidst cases of AI Pornography through the Digital Service Act. In 2017 a resolution was directed from the European Parliament concerning online intermediaries which includes cases of online sexual abuse. The concern was then passed to the European Union Commission to offer further guidance to online platforms in regards to their duty. The legislation was implemented by the parliament regarding online sexual abuse, hate speech and violence, and copyright infringements (Lomba & Evas, 2020).

The matter continues in the span from 2018-2020 which revised the Digital Service Act considering the increasing cases and concerns. In 2018 the parliament took a stance by passing a 2018 resolution on distributed ledger technologies and blockchains: building trust with disintegration. In 2019 the commission under von der Leyen proposed a new digital services act which was then processed in the fourth quarter of 2020 under two communications; "Shaping Europe's Digital Future" and "A European Strategy for Data" (Lomba & Evas, 2020). The series of resolutions was still heavily concerned with the operations of online commercials and single-market and is hardly about the resolution of online pornography. This partially fragmented response made the Digital Service Act (DSA) go through more revisions as non-consensual pornography, which commonly refers to image-based sexual abuse that is freely available and distributed on pornography websites. The emerging usage of deep fakes also plays a key factor in shaping the resolution of 2023 where the deep fake was misused to manipulate digital media into generating highly realistic videos of a certain person saying and acting that they never said or done, including the misuse of deep fake to generate pornography featuring popular public figures.

The concern was published by the European Parliamentary Research Service (EPRS) under the title "Tackling deepfakes in European policy" in 2021. The publication viewed the deep fake problem as "malicious, deceitful, and even destructive". The deep fake threats and risks can be differentiated into three categories of harm; psychological, financial, and societal. The sexual abuse threat is also mentioned within the categories which is a Psychological Harm of "(S)extortion". This harm becomes hardly distinguished as the deep fakes can generate an AI-based manipulation that can alter voices, facial features, and other authentic indicators (European Parliamentary Research Service, 2021).

The DSA was then again revised and passed to take effect on August 25, 2023. This digital legislation puts forward new rules that affect tech giants such as Facebook, Google, and other platforms such as Meta, X, Instagram, and TikTok, forcing them to initiate measures to ban and prevent illegal content such as hate speech (Shankar, 2023). The resolution is also hardly concerned with the mis usage of AI by adding feature changes on certain social media upon logging in to their accounts. The changes are heavily directed toward, AI, fake videos, and children's safety: turning off AI-recommended videos, ability to flag harmful content, transparency behind user's taken-down posts, ability to report fake products, and the crackdown on digital ads aimed at children (Associated Press, 2023). The DSA rules also come with statements that affect platforms that refuse to comply with the rules. According to the EU Commission, the Digital Service Coordinator and the Commission will have the power to take immediate actions necessary to address very serious harm. This sanction can affect badly to the platforms which can result in a temporary suspension in the EU (Roth & Castro, 2023).

Aside from tightening the existing regulations, the European Union created The European Union Agency for Cybersecurity, commonly known as ENISA (European Union Agency for Network and Information Security), was established in 2004 to promote a high and consistent level of network and information security across the EU member states. ENISA plays a vital role in eradicating the deep fake practice in the EU; to eliminate deep fake cases, ENISA has a role in providing guidance, support, and expertise in cybersecurity. An article published on January 20, 2022, on the ENISA website, titled *"Beware of Digital ID attacks: your face can be spoofed!"* mentions that the practice of deep fake can go anywhere, including making an Identity Card, Passport or official document that requires face record. Furthermore, if this kind of digital activity is not protected, cyber-attacks will be very easy; in the case of deep fake attacks, photos stolen will use leveraging software capable of creating a synthetic video or image realistically representing someone else. Attackers are suspected of accessing a broad dataset containing pictures or a video of their targets (ENISA, 2022).

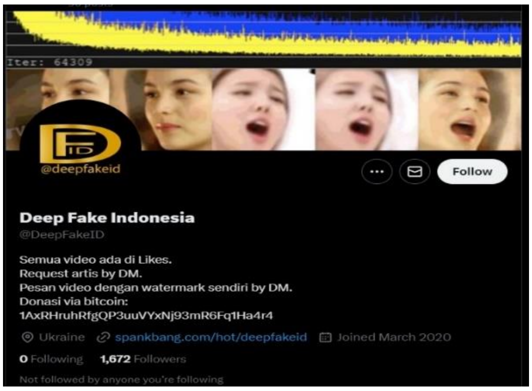
According to ENISA research, deep fake has a high probability of being misused in the upcoming election, talking imperatively from deep fake cases within Poland's and Slovakia's election campaigns and within the EU, the Netherlands is a country that will potentially have an election within 16 months. ENISA also reported that Deep Fake has been targeting two major sectors per 2022/2023 which are Public Administration and Targeted individuals. ENISA has recorded more than 2500 cyber incidents from July 2022 to June 2023 and targeted individuals seized the top 2nd spot with 11% of the cases which depicts the malicious risk of deepfake being used on a person (Roussi, 2023).

ENISA combat the deep fake threats by making a verification system which put emphasis on facial recognition system which has been exploited by deep fake attacks. This system focusses on the presentation attacks that aim to fool the facial recognition. The system is called Remote Identity Proofing, which method is to gather proofs to prove whether the identity of the applicant is genuine or an attacker (European Union Agency for Cybersecurity, 2021).

Indonesia: Deepfake status quo

So, what is happening in Indonesia? Indonesia is also struggling with deepfake porn threats. Similar to the universally known threat, cyber threat in Indonesia is also increasing throughout the year as long as the computer is connected to internet access. The cyber threat increased significantly during the coronavirus pandemic and is even more concerning since AI cyber-attack was put on the equation. Several AI-generated pornographies have been produced by using Indonesian renowned public figures and have been distributed throughout the Internet.

Image 1. Example of X (formerly Twitter) deep fake porn account



Deep Fake Indonesia
@DeepFakeID

Semua video ada di Likes.
Request artis by DM.
Pesan video dengan watermark sendiri by DM.
Donasi via bitcoin:
1AxRHruhRfgQP3uuVYxNj93mR6Fq1Ha4r4

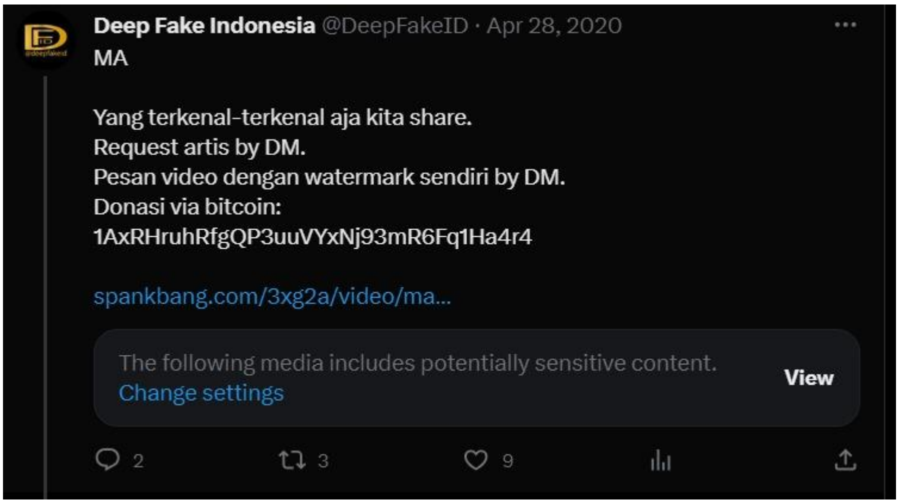
Ukraine spankbang.com/hot/deepfakeid Joined March 2020

0 Following 1,672 Followers

Not followed by anyone you're following

Source: X

Image 2. Post on the transaction and request any person



Deep Fake Indonesia @DeepFakeID · Apr 28, 2020
MA

Yang terkenal-terkenal aja kita share.
Request artis by DM.
Pesan video dengan watermark sendiri by DM.
Donasi via bitcoin:
1AxRHruhRfgQP3uuVYxNj93mR6Fq1Ha4r4

spankbang.com/3xg2a/video/ma...

The following media includes potentially sensitive content.
Change settings

Source: X

The above images are the examples of deepfake porn communication in Indonesia. While it is quite challenging to find accounts that sell deepfake porn in Indonesia due to its discreet nature, it is not impossible to find one. The previous images showed an Indonesian X account selling deepfake porn yet set their location in Ukraine. The account also only receive transaction via bitcoin, which is one of the existing cryptocurrencies to conceal their identities. Buyers can also request the celebrities that they wish to be made deepfake of with a "watermark."

Cases of deep fake pornography in Indonesia have been a wide concern since 2020 with a viral post of deep fake pornography reanimating Syahrini, a local renowned actress. The suspect was seized on May 28, 2020 (Firmansyah, 2020). According to the report, the suspect motive was jealousy of Syahrini. A similar case was also reported in January 2022, this time it featured Nagita Slavina. The video was 61 seconds long and was distributed throughout the internet. Nagita Slavina admitted that she never recorded her private activity and the statement was backed by her husband, Raffi Ahmad. Police reports explained that the video was artificially made (Kamaliah, 2022).

Indonesia is still making progress in tackling deep fake pornography. For Indonesia, a deep fake technology that generates pornography is a new case that can be challenging. The hindrances that Indonesia faces in tackling deep fake pornography can be seen from three factors: the Law Factor, the Technology Factor, and the Law Enforcer Factor (Utawi & Ruhaeni, 2023). There is no specific law that regulates the production and distribution of AI-generated deep fake pornography. In remedy of that matter, Indonesia has some regulation that rules out pornography and electronic transactions (ITE) that could be used against the suspect. However, the law that varies in solving the matter makes it vague on which law that generates deep fake pornography should be put in (Utawi & Ruhaeni, 2023).

Technology of deep fake which involves AI to combine, alter, or layer pictures and video clips into a newly formed video makes it hard to distinguish whether the video is real or fake. This advanced technology hinders the body that investigated the matter from processing the problem, moreover, deep fake is sophisticated which makes tracking the suspect a challenge due to the usage of the newest technology (Utawi & Ruhaeni, 2023). The last factor that hinders Indonesia from tackling deep fake pornography is the Law Enforcer factor. Indonesian Law Enforcers were less responsive to finding the suspect or enforcing the law. This was due to the intricate problem that makes the law enforcers unable to directly track the individuals who are producing and distributing AI-generated deep fakes. In practice, the law enforcers should first coordinate with various parties that are experts on the matter, which makes the investigation slow (Utawi & Ruhaeni, 2023).

Opinions have emerged online regarding the hard path for Indonesia to "Cyber Sovereignty" amidst the large amount of personal data that are leaked to the internet according to the yearly report that was released by Badan Siber dan Sandi Negara (BSSN). This is also worsened by Indonesia's low cyber security, which is the third lowest among G-20 countries to protect personal data from the probability of unaccountable individuals generating deep fake pornography (Syauqillah, 2023).

In 2022, *Komisi Nasional Anti Kekerasan Terhadap Perempuan* in Indonesia pressured the Indonesian government to immediately pass the RUU TPKS, laws against sexual harassment physically, verbally, and in cyber (Dewi, 2022). It was then passed on 9th May 2022 (Andriansyah, 2023). Although UU TPKS does not specify deepfake pornography, it contains a law that forbids any sexual harassment in cyber form, which is one step forward for Indonesia in tackling this issue (Aeni, 2022).

Indonesia cybersecurity capability

Indonesia's cybersecurity capability faced numerous challenges that has yet to be tackled. According to the report released by Center for Digital Society titled *"Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities"*, The cybersecurity challenges in Indonesia can be divided into three different sections: regulation, technology, and human capita/resources. From the perspective of regulation, while Indonesia currently has UU ITE, Indonesia has no regulation that specifically regulates cybersecurity and cybercrime. The draft related to cybersecurity and cyber resilience in Indonesia (*Rancangan Undang-Undang Keamanan dan Ketahanan Siber*) was canceled by business entities. The draft was protested by business entities due to its burdening and heavy conditions. Therefore, Indonesia has no choice but to rely on umbrella laws related to technology such as *UU No. 19/2016 tentang Informasi dan Transaksi Elektronik, UU No. 36 Tahun 1999 tentang Telekomunikasi, dan Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2017.* In the technological aspect, Indonesia does not have any patented technological products yet as the majority of Indonesia technological products were imported. This became an obstacle for Indonesia in ensuring the safety of using technological products that were often used widely. In the perspective of Human capital, Indonesia lacks in not only cybersecurity skill-related knowledge, but also lack of awareness. For example, individuals would carelessly upload their personal data without regards to their personal safety for trends (Loviana, 2022).

According to Hasyim Gautama, the Deputy director of Indonesia's Ministry of Information and Communication Technologies, there are six problems that hindered the development of Indonesia's cybersecurity development: 1. Lack of understanding and awareness of cyber world and security as well as the need to limit the usage of services that uses international server; 2. The legality in handling cyberattacks; 3. Cyberattacks has quick and swift patterns that made it hard to be handled and traceable; 4. Due to the multilayers of complexity in cybercrime nature, it caused multiple institutions to overlap with each other in the responsibilities to handle the cybercrime cases; 5. The lack and low awareness of international attack against Indonesia that can potentially cripple vital infrastructures in this country; 6. Indonesia's lack of technological industry in producing and developing information technology-related hardware (Ardiyanti, 2014).

In the current present timeline, Indonesia has taken measures in protecting Indonesia's cyber realm and ensuring safe space in the Internet for Indonesian citizens. For example, Indonesia created *Badan Siber dan Sandi Negara (BSSN)* as a specific body in overseeing the cyber realm in Indonesia. Originally, BSSN only works in issues related to codes and cipher and was formerly *Lembaga Sandi Negara (Lemsaneg).* Acknowledging the various cyber threats faced by Indonesia, President Joko Widodo signed *Peraturan Presiden (Perpres) No. 28 Tahun 2018* that became the foundation of BSSN. Moreover, *Peraturan BSSN No. 6 Tahun 2021* regulates the structure and responsibilities of BSSN (Badan Siber dan Sandi Negara, n.d.). Ideally, BSSN is responsible in handling, tackling and preventing any future cyberattacks in Indonesia. However, cyberattacks in Indonesia increased rapidly. In the INTERPOL ASEAN cyberthreat assessment report 2021, Indonesia is reported to have more ransomware attacks amongst the Southeast Asian country. From 2.7 million ransomware attack detected in ASEAN region, 1.3 million were detected in Indonesia (INTERPOL, 2021). During the early 2022, Indonesia suffered over 11.8 million cyberattacks. BSSN also reported that there were over 1.6 billion of anomalies detected in traffic and 62% of it were related to malware, trojan and phishing activities and attempts (Chen, 2022).

Lesson learned for Indonesia

There are several points that Indonesia can learn from the European Union in combating porn deepfake threats as well as analyzing Indonesia's weaknesses in cybersecurity. First, the collective awareness of the European Union citizen of the danger in deepfake and threats in cybersecurity contributed in the development of cybersecurity in Europe. Second, through the Digital Service Act, the European Union has slowly acknowledged the threat and harm of deepfake, addressing it in law explicitly and make the issue much more urgent. Third, the formation of ENISA by European Union and ENISA's attempt in combating deepfake by raising awareness and creating Remote Identity Proofing method to verify deepfake and real media and lastly, European Union effort in tackling deepfake crime has been based on cooperation amongst the member states. European Union acknowledged that since the cyber world is vast, collaboration between states and third parties are needed in tackling this issue in order not to let borders amongst nations to become obstacles. In the case of Indonesia, the measure in realigning the BSN (Badan Sandi Negara) becoming BSSN is seen as part of the process to equip the government with more adapt agency in fighting the cybercrime vast structure.

CONCLUSION

With the rapid development of technology and industry, states are expected to follow to not get left behind. In the development itself, new forms and types of crimes will rise inevitably. Artificial Intelligence is the epitome of technological development and has assisted human in many ways and various forms, especially with its ability to mimic human ability. However, the development of AI is followed also by AI-related crimes such as voice, image, even porn manipulation called deepfake. The development deepfake that started from sub reddit has changed from a form of entertainment, into harassment, violence, and monetization. Porn deepfake used pornography from different websites and combine them with pictures of unrelated person to create an artificial yet realistic porn. Women and children were the main target of porn deepfake.

To combat this issue, the European Union has revised the Digital Service Act law and formed a new body called ENISA specifically to tackle cybersecurity issues. Moreover, ENISA has acknowledged the harm and threat possessed by deepfake and created Remote Identity Proofing method in verifying and identifying deepfakes in various forms. Indonesia on the other hand, has yet to have law that can specifically regulate cybersecurity, let alone deepfake. While Indonesia has created BSSN in 2021 to tackle cybercrimes, Indonesia has suffered at least 11.8 million cyberattacks only in the early 2022 and are facing series of challenges in the development of cybersecurity. Thus, making Indonesia behind European Union.

Therefore, it is important for Indonesia to be able to learn from European Union and implement it in Indonesia's cybersecurity. From the regulations and laws, technological capability from hardware to human capital, and the cooperation amongst internal and external parties in state and international level in ensuring that cybercrimes can be stopped and prevented in the future.

REFERENCES

Aeni, S. N. (2022, April 14). *10 Poin UU TPKS yang Penting untuk Diketahui.* Retrieved from Katadata.co.id: https://katadata.co.id/agung/berita/6257c2bb3c3bd/10-poin-uu-tpks-yang-penting-untuk-diketahui

Andriansyah, A. (2023, May 12). *Setahun Disahkan UU TPKS: Beri Pemajuan HAM dan Pengetahuan Publik Soal Kekerasan Seksual.* Retrieved from VOA Indonesia: https://www.voaindonesia.com/a/setahun-disahkan-uu-tpks-beri-pemajuan-ham-dan-pengetahuan-publik-soal-kekerasan-seksual/7089202.html

Ardiyanti, H. (2014, June). Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Politica, 5*(1).

Associated Press. (2023, 08 25). *EU Digital Services Act: 5 things that will change when you sign into your social media accounts*. Retrieved from euronews.com: https://www.euronews.com/next/2023/08/25/eu-digital-services-act-5-things-that-will-change-when-you-sign-into-your-social-media-acc

Badan Siber dan Sandi Negara. (n.d.). *Tentang BSSN*. Retrieved from Badan Siber dan Sandi Negara: https://www.bssn.go.id/tentang-bssn/

Becker, C., & Laycock, R. (2023). Embracing deepfakes and AI-generated images in neuroscience research. *European journal of neuroscience, 58*(3), 2657-2661.

Bolter, J. D. (1984). Artificial Intelligence. *Daedalus, 113*(3).

Britton, B. (2023, February 15). *They appeared in deepfake porn videos without their consent. Few laws protect them.* . Retrieved from nbcnews: https://www.nbcnews.com/tech/internet/deepfake-twitch-porn-atrioc-qtcinderella-maya-higa-pokimane-rcna69372

Chen, E. (2022, June 30). *As Cyber Threats Grow, Indonesia's Data Protection Efforts Are Falling Short: Bureaucratic rivalry and overlapping mandates have prevented the country from pushing ahead with a planned data protection bill.* Retrieved from The Diplomat: https://thediplomat.com/2022/06/as-cyber-threats-grow-indonesias-data-protection-efforts-are-falling-short/

Cotteril, T. (2023, February 19). *Paedophiles are using AI to create child abuse images: National Crime Agency warns artificial intelligence is being harnessed to make pictures and 'deep fake' videos of real-life victims.* Retrieved from Mail Online: https://www.dailymail.co.uk/news/crime/article-11665797/Paedophiles-using-AI-art-generators-create-child-porn.html

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13-17.

Dewi, A. P. (2022, November 24). *Komnas Perempuan Dorong perumusan aturan turunan UU TPKS*. Retrieved from Antara News.com: https://www.antaranews.com/berita/3265581/komnas-perempuan-dorong-perumusan-aturan-turunan-uu-tpks

ENISA. (2022, January 20). *Beware of Digital ID attacks: your face can be spoofed!* Retrieved from ENISA: https://www.enisa.europa.eu/news/enisa-news/beware-of-digital-id-attacks-your-face-can-be-spoofed

European Parliamentary Research Service. (2021, July). Tackling deepfakes in European policy. *European Parliamentary Research Service,* 4-5. Retrieved from European Parliamentary Research Service.

European Union Agency for Cybersecurity. (2021). *Remote ID Proofing Analysis of Methods to Carry Out Identity Proofing Remotely.* ENISA.

Firmansyah, T. (2020, May 28). *Penyebar Video Porno Mirip Syahrini Seorang Ibu Rumah Tangga.* Retrieved from Republika:

https://news.republika.co.id/berita/qb1a1w377/penyebar-video-porno-mirip-syahrini-seorang-ibu-rumah-tangga

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. doi:10.1007/s11416-006-0015-z

Haenlein, M., & Kaplan, A. (2019). On the past, present, and future of artificial intelligence. *California Management Review*, 5-14.

Hanif, S. M., & Dave, V. (2022). Deepfakes Technology Using AI. *International Journal of Scientific research in Acience, Engineering and Technology*, 152-159.

Hedgecoe, G. (2023, September 24). *AI-generated naked child images shock Spanish town of Almendralejo.* Retrieved from BBC: https://www.bbc.com/news/world-europe-66877718

INTERPOL. (2021). *ASEAN CYBERTHREAT ASSESSMENT 2021: Key cyberthreat trends outlook from the ASEAN cybercrime operations desk.* INTERPOL.

Kamaliah, A. (2022, January 17). *Video 61 Detik Mirip Nagita Slavina, Awas Deepfake Ancaman Nyata.* Retrieved from detikInet: https://inet.detik.com/cyberlife/d-5901376/video-61-detik-mirip-nagita-slavina-awas-deepfake-ancaman-nyata

Lomba, N., & Evas, T. (2020). Digital Services Act. *European Parliamentary Research Service*, 4-5.

Loviana, K. (2022). *Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities.* Center for Digital Society.

Maddocks, S. (2020). 'A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and. *Porn Studies*, 1-9.

Nir, K. (2023). *Computing: The Economics of Deepfakes.* IEEE.

Okolie, C. (2023, March). Artificial Intelligence-Altered Videos (Deepfakes), Image-Based sexual abuse, and Data privacy concerns. *Journal of International Women's StudiesJournal of International Women's Studies, 25*(2).

Payne, L. (2023, September 27). *deepfakes*. Retrieved from Britannica: https://www.britannica.com/technology/deepfake

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies, and Taxonomies. *Forensic Sciences*, 382-383.

Roth, E., & Castro, A. (2023, August 25). *The EU's Digital Services Act goes into effect today: here's what that means*. Retrieved from The Verge:

https://www.theverge.com/23845672/eu-digital-services-act-explained

Roussi, A. (2023, October 19). *European election at risk from AI, says EU's cyber agency*. Retrieved from politico.eu: https://www.politicio.eu/article/european-union-election-risk-artificial-intelligence-interference-cybersecurity-agency-enisa/

Shankar, P. (2023, August 25). *What impact will the EU's Digital Services Act have? – DW – 08/25/2023*. Retrieved from DW: https://www.dw.com/en/what-impact-will-the-eus-digital-services-act-have/a-66631337

Sorban, K. (2023). An elephant in the room—EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms. *International Journal of Law and Information Technology*.

Syauqillah, M. (2023, September 21). *Jalan Terjal Menuju Kedaulatan Siber*. Retrieved from mediaindonesia: https://mediaindonesia.com/opini/615393/jalan-terjal-menuju-kedaulatan-siber

Tenbarge, K. (2023, June 12). *Deepfake porn of TikTok stars thrives on Twitter even though it breaks the platform's rules*. Retrieved from NBC News: https://www-nbcnews-com.translate.goog/tech/internet/deepfakes-twitter-tiktok-stars-rcna87295?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc&_x_tr_hist=true

Utawi, E. I., & Ruhaeni, N. (2023). Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial. *Bandung Conference Series: Law Studies*, 368-369.

Xie, H., Hwang, G.-J., & Wong, T.-L. (2021). Editorial Note: From Conventional AI to Modern AI in Education: Re-examining AI and Analytic Techniques for Teaching and Learning. *Educational Technology & Society, 24*(3).