Cybercrimes and Violations of Intellectual Property Law on Indigenous Papuans in Indonesia

Roberth Kurniawan Ruslak Hammar[1*], Henrikus Renjaan[2]
Lecture of Sekolah Tinggi Ilmu Hukum (STIH) Caritas Papua Manokwari, Indonesia

Abstract
The aim of the current study was to analyze the cybercrimes and violations of intellectual property law on the indigenous Papuans in Indonesia, particularly when technology and innovations are spreading fast in Papua. The study makes a thorough literature review in this regard in order to ensure a maximum outreach to information present on the factors and characteristics that enhance cybercrimes and that lead to violations of intellectual property laws. A qualitative non-empirical legal research approach was used in this study, according to which extraction of information and data was done from various legal documents, cases and laws from Papua, Indonesia. The current laws, regulations and policies protecting intellectual property laws against cybercrime were also analyzed, discussed and their shortcomings were presented and defined. A few recommendations were also provided for the betterment of the security of intellectual property laws against cybercrime in Papua, Indonesia. There is a requirement of novel comprehensive cybercrime law that significantly focuses on all different methods in which the intellectual property rights are now violated.

Keywords: Cybercrime violations, Intellectual Property Law, Indigenous Papuans Indonesia

Introduction
In recent times, the significant impact of computers and Internet is reflecting on the entire world in the form of both positive and negative outcomes. These outcomes have made the world think that putting in full confidence in technology and Internet is always not a wise choice, as far as the privacy and security is considered (Ajayi, 2016). Showing full confidence in modern technology of computing and Internet can be significantly dangerous as well with social, personal and economic consequences (Anderson et al., 2013). The modern computing technologies and the Internet represent the most revolutionary techniques and technological discoveries; however, every technology and revolutionary innovation has some kind of loopholes that resides negatively along with the positive aspects of any specific technology or innovation (Anderson et al., 2019).

[1] *Corresponding Author: Email: roberthstih43@gmail.com, Lecture of Sekolah Tinggi Ilmu Hukum (STIH) Caritas Papua Manokwari, Indonesia (Roberth Kurniawan Ruslak Hammar)
[2] Lecture of Sekolah Tinggi Ilmu Hukum (STIH) Caritas Papua Manokwari, Indonesia, henrikusrenjaan@gmail.com

Apart from all of the benefits and advantages that modern computing technologies and Internet have brought, they have significantly become tools of abuse for corporations, individuals and even the government of any country (Aransiola & Asindemade, 2011; Azad et al., 2017). As a result of being used as tools for abuse, illegal actions by organizations and groups and socially dangerous and unlawful activities have been reported on almost daily basis (Bernat & Godlove, 2012). There is a significant boom that has been caused due to cybercrimes spreading in households and offices through Internet. This has resulted in the creation of a significant base of users resulting in the potential victims of various crimes being conducted in the form of cybercrimes (Baeewe, 2021).

The cybercrime is referred to as a type of criminal activity or conduct, as a result of which an individual uses broadcasting technologies, computers, and various information technology based systems for the manifestation of various technical offences, where computer networks are utilized as the purpose or means of the enforcement of such offence (Adam M. Bossler, 2020). Significant level of technology can significantly be abused in different ways, and these crimes can result in various conventional types of crimes, involving tax evasion crime, the crime of fraud and the obtaining of data in various ways utilized and applied in illegal ways for illegal tasks (Adam M Bossler & Holt, 2012). These kinds of criminals and offenders significantly orient the action of robberies, where similarly, the object of usage involves modern technological systems and machines.

Papua is the eastern most province present in Indonesia and it encompasses the western half of the several islands and New Guinea as well (Brenner, 2012). The area involves biological and cultural diversity, where mountains and rainforests are inhabited by indigenous Melanesian tribes. It includes diverse wildlife as well. The capital town is Jayapura with a total population of around 3.379 million as recorded in the year 2019 (Fahlevi et al., 2019). The telecom sector is now significantly growing in Papua, having significant connectivity and quick setting and spreading of networks. The computer network is now reaching to the remotest parts of the province, helping people link various devices by a diverse range of customers and organizations (Fahlevi et al., 2019). This cellular coverage with the significant growing of the Internet is also raising various concerns and questions regarding the dangers that are conceived as a result of these technological innovations and developments, and also regarding how to deal with these innovations (Broadhurst & Chang, 2013).

There are various concerns that are linked with the technology innovations: defamation, cyberbullying, breaching of personal security, privacy and the leakage of important information that are coming along these innovations and technological advancements in Papua. Other concerns observed in different areas of Papua include sending off the indecent materials, spreading of significantly false information, hacking of systems and information and sedition (Cordova et al., 2018). However, above all of these concerns and factors, cyber-crime violations cover a very vast horizon and involve various other kinds of violations out of which, a very significant and adverse one is the violation of the intellectual property law (Broadhurst & Chang, 2013; Cordova et al., 2018). The intellectual property laws involve all the laws and regulations that are applied and regulated for the purpose of enforcing and protecting the rights of the owners and creators of writings, inventions, designs, music and all other works that fulfill the characteristics of being intellectual property of a specific individual or organization (Brenner, 2012; Broadhurst & Chang, 2013).

There are various areas of the intellectual property that are covered involving trademarks, copyright, trade secrets and patents. The spread of information technology all over Papua

and enhanced networked systems throughout the region have resulted in various social, economic and cultural positive impacts (Dashora, 2011; Davis, 2012). However, it is unfortunate that the criminal minded people and the individuals which focus on cyber-crime exploit the new technology and innovations in various ways which is draining the wealth and also undermining the rule of law in Indonesia (Fahlevi et al., 2019; Finklea & Theohary, 2015). The intellectual property right theft in the form of theft of writings, inventions and designs can be observed in Indonesia openly however, it can be increasingly now observed in the province Papua as well. In Papua, according to various reports, cyber-crimes and intellectual property thefts are being observed in the form of theft of designs, theft of music, theft or pharmaceutical formulas and machine tools (Gercke, 2016).

Cyber-crimes have significantly increased in the form of information technology enabled crimes all across the spectrum of the province. This includes virus attacks, hacking, identity theft, cyber smuggling and increasingly prevailing intellectual property theft as well (Gillespie, 2015). Due to the borderless nature of cyber-crimes, there is a need for effective law enforcement by the government and respond to the ever enhancing cyber-crimes against intellectual property laws. The government must emphasize on the capacity building within the legal system and of the law enforcement partners as well (T. Holt & Bossler, 2015). There is also a dire need to study and analyze the extent of cyber-crime violations of intellectual property law on the indigenous Papuans in Indonesia (T. J. Holt, 2018).

The current study aimed to make threefold contribution: first, this study is directly targeting the cyber-crime violations of intellectual property law in the context of indigenous Papuans in Indonesia, since it has been observed that previous studies have not considered the indigenous Papuans while analyzing the impact of the enhancing cyber-crime violations of intellectual property law (T. J. Holt & Bossler, 2014; T. J. Holt et al., 2015). Secondly, as far as the information technology and innovation in technology are concerned, previous studies have ignored Papua, Indonesia. This study aimed to highlight that technological innovations, advancements and the relevant concerns are very much increasing every passing day (Hooper et al., 2013). Thirdly, this study analyzed the current status of cyber-crime violations of intellectual property law on the indigenous Papuans in Indonesia since there is no significant focus on either the cyber-crime violations of intellectual property or the indigenous Papuans in Indonesia in this specific context (Hooper et al., 2013). This study will be theoretically and practically contributing towards the enhancement of the importance and incidence of the events of cyber-crime violations of the intellectual property laws in Papua, Indonesia (Hunton, 2011).

There are five sections of this study: the first section dealt with the introduction and background of this study, the problem statement, the justifications and rationale, the objectives, and the significance of the current research. The second section presents the literature review, which covers different facets and characteristics of cyber-crime, and the intellectual property law in detail along with a review and analysis of both these factors. This section also provides a relationship between cyber-crimes and intellectual property laws, in order to present with the impact of cyber-crimes on intellectual property laws. The third section of the study presents the research methodology adopted for this research; the fourth section contains discussion and analysis of the impacts of cyber-crimes on intellectual property law, in the context of the laws and regulations applied in Indonesia. The last section involves conclusion and recommendations showing how to minimize cybercrimes against intellectual property laws in Papua.

Literature review

Cybercrime violations

There are various IPR related acts such as Trademarks Act 1978, Patents and Industrial Designs Act 2000 and the Copyright and Neighboring Rights Act 2000, which focus on the protection of intellectual property rights in Papua. These acts can also be presented against cybercrimes and offences being conducted by various individuals (Martin & Rice, 2011). The intellectual property does not only involve copyrights, but it also involves and covers patents, trademarks, trade secrets and various other kinds of properties that fulfill all the characteristics of the intellectual property. The computer related offences and acts are now causing personal harm as they involve the usage of computer systems to harass, stock, threaten and bully the host by hackers and intimidators, (Martin & Rice, 2011; McDougal, 2015; Tomteberget & Larsson, 2020).

Most multilateral and regional cybersecurity organizations and treaties like the Arab Convention on Combating Information Technology Offences, the Cybercrime Convention, the Cyber Security and Personal Data protection and African Union Convention significantly focus on the minimization of computer related offences such as cybercrimes, cyber bullying, cyber stalking and cyber harassment (Moore, 2014). Along with these cybercrimes, the infringement of the intellectual property laws is something that needs further focus and research before the implementation of any other laws and regulations that regulate the cybercrime violations against intellectual property laws (Nzeakor et al., 2020; Odumesi, 2014; Olayemi, 2014; Shah et al., 2020). First of all, a gap has been identified in previous studies that which suggest that not much attention has bene paid on technological innovations in Papua, Indonesia. Moreover, these studies have also not focused on the technological and science-based innovations that are have brought up several concerns and questions in Papua. As a result of which, it is difficult to make thorough decision making nor laws can be generated and applied in the region (Mazur & Kuć, 2020; Papathanasiou et al., 2013; Rajan et al., 2017; Rashkovski et al., 2016).

Intellectual property rights and laws

Intellectual property rights (IPR) provide creators or inventors legal rights and protection against their original work, appearance of products, inventions, scientific developments or artistic works (Reyes et al., 2011). The intellectual property law significantly focuses on and deals with all regulations and laws to enforce and protect rights of the owners and creators of writings, inventions, designs, music and all other work that fulfills the characteristics of intellectual property and can be called as intellectual property of a specific individual, corporation or body (Sabillon et al., 2016).

The IPR laws are of different types, namely copyright laws, trademark laws, patent laws, and trade secrets. The copyright laws are protected in the umbrella of the intellectual property law, and are concerned with the rights of the work related with entertainment, arts, publishing and development of computer software. These laws protect the work of the owner or the creator, against use or exploitation by any individual under any circumstances without the permission of the creator or the producer (Setiawan et al., 2018). The trademark laws also come under the umbrella of the intellectual property laws, and these are the laws for the protection of words, symbols, phrases and designs, used by individuals, or the entities for the identification of specific services or products. The trademark owners can significantly prevent any other individual from utilizing these marks under the trademark laws (Setiawan et al., 2018).

The Patent laws also come under the umbrella of the intellectual property laws, and these protect inventions of new designs, processes, products or mechanisms. The patent law promotes sharing of the new developments with the world but not on the same pattern, only on the option of fostering further innovation (Somer, 2019; Spulbar & Birau, 2020). The patent owner has every right to protect the innovation or invention from the others that might be using, producing, importing or distributing similar item based on the similar idea and invention point of view. The laws related with the protection of trade secrets also come under the intellectual property laws, but the trade secrets involve business formulas, processes, practices and designs that are the major assets of a business or are the major component of the design of a business that provide businesses with competitive advantages. These trade secrets must not be known by outsiders otherwise the business might lose its competitive advantage. In order to protect these trade secrets, trade secret laws are regulated and applied (Somer, 2019; Spulbar & Birau, 2020).

Cybercrime Violations of Intellectual Property Law

In accordance with the intellectual property laws, the trademarks act 1978 protects the products and services from violations of the intellectual property laws through cybercrimes or any other crimes that can be committed by criminals in order to exploit the intellectual property in any way possible (Lusthaus, 2013; Lusthaus & Varese, 2021). In accordance with the law, "assignment" represents the assignment by the act associated with the concerned parties, and the "date of commencement" represents the date following which the operations of the intellectual property laws are applicable (Kolouch, 2016; Kumar, 2016). The non-use of the trademarks in accordance with the trademarks act 1978, focuses on the nonuse of the trademarks related with the product services, under any circumstances, involving under the circumstances of the commitment of cybercrime as well (Kolouch, 2016; Kumar, 2016). However, there are some exceptions as well, involving any instance in which the trademark is not registered with the intention in good faith from the side of the applicant at the time of the registration, clearly explaining that it should be utilized only in relationship to the goods by the applicant or anyone referred to by the applicant, according to the section 35(1) (Liu, 2018).

However, as a result of commitment of a crime, up to one month of the application, the product is strictly protected under the intellectual property laws, and there can be no use of the product or property by anyone, under good faith or otherwise as well (Ledingham & Mills, 2015). The law defines the such crime against the intellectual property as distribution, access, user offering of the intellectual property without and beyond any kind of initial authorization and the violation of the intellectual property laws associated with the protection of that intellectual property (Loader & Thomas, 2013). Furthermore, the law states that intellectual property laws violation as a crime committed against the owner of the property and the property itself as well, however, the law states that in the case of this crime and the theft of intellectual property, even if the property is utilized and offered by the criminal online, the owner is not denied of the rights to the property, and actions are taken against the criminal (Liu, 2018).

The intellectual property theft is elaborated as the theft of the material or the product that is copyrighted, or is protected by the intellectual property laws. These can involve the theft of the trademarks, the theft of the trade secrets or the general violations of the invention of an individual that has been protected under the intellectual property law (Tsakalidis & Vergidis, 2017). Copyrights provide with legal right to the publishers, authors, composers

or the inventors, involving any individual who creates an original work and has the will to protect the original work exclusively from performance, printing, distribution or publishing in the public (Tyendezwa, 2012). The theft of the intellectual property laws are becoming more and more dominant and prevailing nowadays, like the theft of the trade secrets which means the theft of methods, plans, technologies, ideas and the sensitive information involving all types of data that are exclusively the original property of any specific corporation, industry, individual or body (Urbas, 2012; Vukelić & Škaron, 2013).

These secrets are owned by the individuals or the corporations exclusively and provide them with the competitive advantage. Any violation of thee secrets may result in the damage to the competitive advantage, to the image and also to the economic base of an individual, corporation or anybody (Urbas, 2012; Vukelić & Škaron, 2013). The two major kinds of cybercrime violations of the intellectual property law that have been observed in the last decade involved the cybercrimes attacking the trade secrets and the cybercrimes attacking the copyrighted material as well. Piracy is the term that is most of the time utilized for describing the theft of intellectual property, which significantly and directly violates the intellectual property law in any country (Wall & Yar, 2013). This does not only cause economic damages to the owner but also results in mental and social problems for that specific individual or owner of the intellectual property (Wall & Yar, 2013).

Specifically in the 21st century music software and trade secrets piracy has enhanced significantly, and the piracy is being done through the Internet utilizing the most developed and innovative technological mechanisms and devices (Yar & Steinmetz, 2019). There is no doubt in the fact that anything that can be directly converted into zero and one can be transmitted smartly from one computer to another computer, and there is also no reduction in any kind of quality of that content up to the second, third and the fourth generations of the copies (Zagaris & Boyle, 2020). The pirated digital copies of the work being stolen is then transmitted on the Internet is called as the warez and the warez groups are also known to be responsible for illegally distributing and copying millions of dollars against the copyrighted materials (Ajayi, 2016).

Methodology

A qualitative and non-empirical legal research design was adopted in this study as it involved qualitative extraction of data and information from the text of various documents. This is related to a specific law, the text of court documents and the extraction of text from various legal scriptures and data banks that were then analyzed, organized and interpreted in order to address a specific problem of research (Bernat & Godlove, 2012). The objectives of this research involved analyzing the cybercrime violations of intellectual property law on indigenous Papuans in Indonesia. This specific objective was undertaken in this study because previous studies have not significantly focused on the technological innovation and advancements that are happening in Papua. No research in the past has focused on the enhancing concerns of cybercrime violations related to intellectual property law in Papua, Indonesia (Broadhurst & Chang, 2013; Cordova et al., 2018).

Furthermore, this topic was chosen in order to significantly analyze the current status of intellectual property laws being applied in Papua, Indonesia and find out ways how to tackle with cybercrime violations and what recommendations can be provided for the betterment of these laws and the legal framework against cybercrime violations. This research study is based on non-empirical and qualitative data collected from the Papuans, Indonesia in the form of text related to the intellectual property law (Fahlevi et al., 2019; Finklea &

Theohary, 2015). Furthermore, the sample of this research involved indigenous Papuans from Indonesia, selected through random sampling method. Different Indonesian legal sites and databases were searched in order to find out cases of cybercrime violations of intellectual property law, and these cases were analyzed in the light of intellectual property law applied in Papua, Indonesia (Gercke, 2016; Gillespie, 2015).

Discussion

This section involves the discussion of various acts and cases which calls for the betterment and updating of the already existing intellectual property law that is being applied and practiced in Papua, Indonesia. Significant cases were observed in this region regarding defamation, cyber bullying, theft of the intellectual property and receiving and sending of indecent material on a daily basis (Anderson et al., 2019). Ultimately, this issue has now become the problem of national security, as proposed by Jim Miringtoro, "We have to understand from a security point of view what is coming in and what is going out of the country". According to the authorities as well, the creation of the right and novel framework for the minimization of the cybercrime is a challenging task and this requires complex technologies and legislators to deal with the evolving range of crimes being committed with the help of the ever developing technology (Baeewe, 2021; Adam M. Bossler, 2020).

The Patents and Industrial Designs Act, 2000 is responsible for the provisions that protect different industrial property rights involving geographical indications, patents and industrial designs that are protected under the law. The act significantly focuses on all of the factors that can result in the violations of the intellectual property laws, and a significant portion of this act is dedicated to the cybercrime protection as well, against the intellectual property laws, however, analysis of these laws and areas is very important, in order to propose recommendations for the amendments (Liu, 2018; Lusthaus & Varese, 2021). The constitutional and compliance requirements involved the right to the freedom of expression, the right to the privacy of the intellectual property and the right to the freedom of the employment as well. The law represents various facets under which, the intellectual property laws must not be violated as a result of cybercrime, and it states that the exploitation of a patented invention as a result of cybercrime is prohibited under any circumstances following, when the matter of subject is protected by patent laws, the intellectual property cannot be utilized for using, making, offering or for hiring, moreover, these can also not be utilized for importing, selling or any other trade objectives (Cordova et al., 2018).

The *Section 266* of the Act represents that some of the efforts are not at all controversial and straightforward as well. The Customs Department has already started working with the NICTA or National Information And Communications Technology Authority for the purpose of stopping the flow of any illegal information, communication and technology goods into or out of the country (Adam M. Bossler, 2020). However, the government is significantly and highly concerned regarding the use of communication devices and information technology as well for illegal processes such as the processes that involve stealing of very sensitive and important information, from the individuals, corporations or even from the government itself (Cordova et al., 2018). So cybercrimes must be dealt as a problem of national security, however, under the section 266 present in the NICTA Act, the abuse of the ICT services for the exploitation of intellectual property is properly now being considered as an offence (Fahlevi et al., 2019). In the recent years, as a result of this several cases have been brought to the court that are relevant to the section 266. These cases involved material theft, offensive language usage and harassment of people, however, the

problem was far too complicated and significantly serious, and was now being considered by officials that it cannot be resolved under the NICTA Act (T. J. Holt, 2018).

The market of Papua, Indonesia is significantly smaller in comparison with other markets all around the world however, there is a significant requirement of intellectual property laws and regulations for the people that can stop the violation of the intellectual property rights and cybercrimes (T. J. Holt, 2018). The intellectual property laws that are implemented in the Papua, Indonesia right now are more or less similar to the countries like New Zealand, where some of the legislations involving trademarks were directly adopted from Australia. However, it does not suggest that there is a significant difference in the market between Papua, Indonesia and Australia as well (Jain & Gupta, 2020; Khan et al., 2020).

The three major pieces of the legislations being followed for the intellectual property security in Papua, Indonesia includes the Trademarks Act 1978, the Patents and Industrial Designs Act 2000 and the Copyright and Neighboring Rights Act 2000. These acts prevent the stocking of the intellectual properties for the purpose of offering to someone, for selling it or for introducing any kinds of hurdles in the patent procedure (Loader & Thomas, 2013). The usage of a product that is protected under intellectual property law is prohibited for being offered for a sale as a result of cyber-crime. It is prohibited for importing or using as well, as a result of cybercrime. Other characteristics that are related to industrial designs and are protected by the intellectual property law, relate to three-dimensional forms, colors or materials from being utilized, offered for sale, imported or imitated (T. J. Holt, 2018). Moreover, under the international classification of the patents and industrial designs Act 2000, cybercrime is deemed to have been committed when it comes to selling and offering any kind of discovery, scientific theory or any kind of mathematical method online, offering any kind of protected scheme, method and formula of performing business activities is also prohibited under this act (T. J. Holt, 2018).

The intellectual property office of Papua is responsible for the registration and controlling of the patents, designs and the trademarks. However, currently all of the applications need to be filled at the intellectual property office of Papua present in the Port Moresby (Liu, 2018; Lusthaus & Varese, 2021). Yet, the intellectual property office of Papua is in the procedure of the establishment of electronic registry however, as soon as it is complete, the electronic registry will result in patent searching, electronic filing and trademark searching as well (Lusthaus & Varese, 2021). The intellectual property rights are being considered as the private rights and are also being enforced by the intellectual property owners against the individuals that can infringe those rights. The courts in Papua, Indonesia have the power to make various orders including provisional seizure orders, interim injunctions and awards of compensatory damages against the damages to the intellectual property of any individual, corporation or body present in Papua, Indonesia (Lusthaus & Varese, 2021; Spulbar & Birau, 2020).

According to the 2000 act, the intellectual property laws are strictly applicable to the inventions on which patent is applicable, in accordance with the section 13, section 14 and section 15. This prevents criminals to copy the invention, or perform commercial exploitation of the product or in which the criminals offer the product for import or selling purposes, online (Liu, 2018; Lusthaus & Varese, 2021). Furthermore, the new inventions are also protected under this act from any online intangible exploitation, oral disclosure online, usage or selling online. Under this law, the right to the intellectual property is strictly to the inventor, furthermore, in case there are two or more persons involved in an invention, the right to the intellectual property is held by both of these persons, however, in the case, where there are two people involved in the interdependent invention of a

product, the patent will belong to the person that files for the patent earliest, and that product will directly be protected against any kind of patent infringement, intellectual property stealing and cybercrimes as well (Liu, 2018; Lusthaus & Varese, 2021).

However, the major shortcoming and gap right here involves the lack of proper rules, laws and regulations that can control any factors that can result in the cybercrime violations of the intellectual property laws in Papua, Indonesia or any factors that can lead towards the violation of these laws. Furthermore, the Banks and Financial Institutions Act, 2000, Business Names Act, 1963, Central Banking Act, 2000, The Classification Of Publication Act 1989, Companies Act, 1997, Copyright And Neighboring Rights Act, 2000, Criminal Code Act, 1974, Customs Act, 1951, Evidence Act, 1975, Internal Security Act, 1993, National Broadcasting Corporation Act, 1973, National Intelligence Organization Act, 1984, National Information And Communications Technology Act, 2009, Patent And Industrial Designs Act, 2000, Protection Of Private Communication Act, 1973, Securities Act, 1997 And Trademarks Act, 1978, are some of the Acts and legislations that are applied in Papua against various aspects of IPR related crimes however, it has been observed that the niche for intellectual property laws protection is very limited in the case of cybercrime (Lusthaus & Varese, 2021; Spulbar & Birau, 2020). Analyzing most of the acts and legislation, the researcher has found out that the rules, regulations and laws cover various general aspects when it comes to cybercrime however, there is no significant focus on very specific aspects when it comes to the protection from cybercrime in Papua, Indonesia (Lusthaus & Varese, 2021; Spulbar & Birau, 2020). So, accumulatively, on the basis of the above analysis and discussion as well, it is proposed for the regulations and laws being applied and practiced in Papua, Indonesia, that there must be direct laws and regulations in support of the cyber security against the cybercrimes and violations of the intellectual property laws.

Conclusion and recommendations

Apart from all of the benefits and advantages that the modern computing technologies and Internet have brought, both of these can significantly become tool of abuse for corporations, individuals and even the government of any country. The cybercrime is referred to as a type of criminal activity or conduct, as a result of which an individual uses broadcasting technologies, computers, and various information technology-based systems for the manifestation of various technical offences, where the computer networks and computers are utilized as the purpose or means of the enforcement of such offence. It is unfortunate that the criminal minded people and the individuals focused on cybercrime are exploiting the new technology and innovations in various ways that are draining the wealth and are also undermining the rule of law in Papua, Indonesia.

This study focused on Cybercrime Violations of Intellectual Property Law on Indigenous Papuans Indonesia. The study provided with extensive and significant literature review which reviewed characteristics of the criminal offences related to cybercrime, the computer based criminal offences were discussed, intellectual property rights and laws were examined along with all the laws that come under the umbrella of these laws. Furthermore, the cybercrime violations and their impact on the intellectual property law were also discussed as well. The research methodology adopted for this study was qualitative non-empirical legal research design, which involves qualitative extraction of data and information from the text of various documents. This information was related to specific laws, texts of court documents and text from various legal scriptures and data banks. These documents were analyzed, organized and interpreted in order to address a specific problem of research. The

cybercrime has been mentioned along with intellectual property laws violations during in national ICT policy of 2008. However, in the case of Papua, it has not been seen and analyzed as a priority, in order to more directly and significantly address the problems related with the cybercrimes violating the intellectual property rights. The government needs to directly work on legislation and policies that focus on both current and potential offences.

It is suggested that as the first step all SIM cards must be registered so that crimes must not be committed. This will significantly decrease the level of these crimes being transnational. There is also a requirement of novel comprehensive cybercrime law that significantly focuses on all the different methods in which the intellectual property rights are now being violated with the help of cybercrime. Furthermore, the tracking mechanism needs to be more vigilant and first, if the criminals are to be caught, so, there should be significant focus on the tracking down of the individuals as well that are committing cybercrimes in Papua, Indonesia.

References

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems, 6*(1), 1-12. https://doi.org/10.5897/JIIS2015.0089

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., . . . Vasek, M. (2019). Measuring the changing cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security*. https://doi.org/10.17863/CAM.41598

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759-763. https://doi.org/10.1089/cyber.2010.0307

Azad, M. M., Mazid, K. N., & Sharmin, S. S. (2017). Cyber crime problem areas, legal areas and the cyber crime law. *International Journal of New Technology and Research, 3*(5), 1-6. https://www.neliti.com/publications/263300/cyber-crime-problem-areas-legal-areas-and-the-cyber-crime-law

Baeewe, S. S. (2021). Cybercrime under the New Iraqi Draft Cybercrime Law. *journal of the college of basic education*, 123-141. https://www.iasj.net/iasj/article/213239

Bernat, F. P., & Godlove, N. (2012). Understanding 21st century cybercrime for the 'common'victim: Frances P Bernat and Nicholas Godlove argue that it is time to extend the principle of universal jurisdiction to the typical types of cyber-offences. *Criminal Justice Matters, 89*(1), 4-5. https://doi.org/10.1080/09627251.2012.721962

Bossler, A. M. (2020). Cybercrime Legislation in the United States. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 257-280). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_3

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies and Management, 35*(1), 165-181. https://doi.org/10.1108/13639511211215504

Brenner, S. W. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Northeastern University Press. https://books.google.com.pk/books?id=HIip2uXE4gcC

Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: Trends and challenges. In *Handbook of Asian criminology* (pp. 49-63). Springer. https://doi.org/10.1007/978-1-4614-5218-8_4

Cordova, J. G. L., Álvarez, P. F. C., Ferrandiz, F. d. J. E., & Pérez-Bravo, J. C. (2018). Law versus cybercrime. *Global Jurist, 18*(1). https://doi.org/10.1515/gj-2017-0024

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences, 3*(1), 240-259. https://www.academia.edu/download/38110491/11._Dashora_1_.pdf

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies and Management, 35*(2), 272-284. https://doi.org/10.1108/13639511211230039

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. *E3S Web of Conferences. 125* (pp. 21001). EDP Sciences. https://doi.org/10.1051/e3sconf/201912521001

Finklea, K. M., & Theohary, C. A. (2015). *Cybercrime: conceptual issues for congress and US law enforcement*. Congressional Research Service, Library of Congress. https://www.ipmall.info/sites/default/files/hosted_resources/crs/R42547_120720.pdf

Gercke, M. (2016). *Understanding cybercrime: a guide for developing countries*. International Telecommunication Union. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf

Gillespie, A. A. (2015). *Cybercrime: Key issues and debates*. Routledge. https://doi.org/10.4324/9781315884202

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge. https://doi.org/10.4324/9781315775944

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140-157. https://doi.org/10.1177%2F0002716218783679

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40. https://doi.org/10.1080/01639625.2013.822209

Holt, T. J., Burruss, G., & Bossler, A. (2015). *Policing cybercrime and cyberterror*. Criminal Justice and Criminology Faculty Publications. https://digitalcommons.georgiasouthern.edu/crimjust-criminology-facpubs/70

Hooper, C., Martini, B., & Choo, K.-K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review, 29*(2), 152-163. https://doi.org/10.1016/j.clsr.2013.01.006

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review, 27*(1), 61-67. https://doi.org/10.1016/j.clsr.2010.11.001

Jain, A., & Gupta, N. (2020). Cyber crime. *National Journal of Cyber Security Law, 2*(2), 152-158. https://www.nci.tmu.ac.in/conference_proceeding/NCI26.pdf

Khan, S., Khan, N., & Tan, O. (2020). Efficiency of legal and regulatory framework in combating cybercrime in Malaysia. In *Understanding Digital Industry* (pp. 333-336). Routledge. https://doi.org/10.1201/9780367814557

Kolouch, J. (2016). *CyberCrime*. CZ. NIC, zspo. https://eknizky.sk/wp-content/uploads/2018/12/cybercrime.pdf

Kumar, P. V. (2016). Growing cyber crimes in India: A survey. *International Conference on Data Mining and Advanced Computing (SAPIENCE)* (pp. 246-251). IEEE. https://doi.org/10.1109/SAPIENCE.2016.7684146

Ledingham, R., & Mills, R. (2015). A preliminary study of autism and cybercrime in the context of international law enforcement. *Advances in Autism, 1*(1), 2-11. https://doi.org/10.1108/AIA-05-2015-0003

Liu, H. (2018). In the shadow of criminalisation: Intellectual property criminal law, enforcement institutions and practices in China and the United States. *Information & Communications Technology Law, 27*(2), 185-220. https://doi.org/10.1080/13600834.2018.1458451

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Security and Surveillance in the Information Age*. Taylor & Francis. https://books.google.com.pk/books?id=MtP1AhhZcfAC

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime, 14*(1), 52-60. https://doi.org/10.1080/17440572.2012.759508

Lusthaus, J., & Varese, F. (2021). Offline and local: The hidden face of cybercrime. *Policing: A Journal of Policy and Practice, 15*(1), 4–14. https://doi.org/10.1093/police/pax042

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security, 30*(8), 803-814. https://doi.org/10.1016/j.cose.2011.07.003

Mazur, J., & Kuć, M. (2020). Wspólnoty wirtualne między bezpieczeństwem a zagrożeniem i mitem a rzeczywistością. *socialspacejournal.eu, 19*(1), 165-183. http://socialspacejournal.eu/Social%20Space%20Journal%2012020(19).pdf#page=165

McDougal, T. (2015). Establishing Russia's Responsibility for Cyber-Crime Based on Its Hacker Culture. *Int'l L. & Mgmt. Rev., 11*(2), 55-80. https://digitalcommons.law.byu.edu/ilmr/vol11/iss2/4/

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge. https://doi.org/10.4324/9781315721767

Nzeakor, O. F., Nwokeoma, B. N., & Ezeh, P.-J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology, 14*(1), 283-299. http://dx.doi.org/10.5281/zenodo.3708924

Odumesi, J. O. (2014). Combating the Menace of Cyber crime. *International Journal of Computer Science and Mobile Computing, 3*(6), 980-991. https://www.academia.edu/download/34139516/V3I6201499a72.pdf

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116-125. https://doi.org/10.5897/IJSA2013.0510

Papathanasiou, A., Papanikolaou, A., Vlachos, V., Chaikalis, K., Dimou, M., Karadimou, M., & Katsoula, V. (2013). Legal and social aspects of cyber crime in Greece. *International Conference on e-Democracy* (pp. 153-164). Springer. https://doi.org/10.1007/978-3-319-11710-2_14

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017). UAE cybercrime law and cybercrimes—An analysis. *International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)* (pp. 1-6). IEEE. https://doi.org/10.1109/CyberSecPODS.2017.8074858

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime tendencies and legislation in the Republic of Macedonia. *European journal on Criminal policy and research, 22*(1), 127-151. https://doi.org/10.1007/s10610-015-9277-7

Reyes, A., Brittson, R., O'Shea, K., & Steele, J. (2011). *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*. Elsevier. https://www.sciencedirect.com/book/9781597491334/cyber-crime-investigations

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security, 4*(6), 165-176. http://hdl.handle.net/10609/78507

Setiawan, N., Tarigan, V. C. E., Sari, P. B., Rossanty, Y., Nasution, M., & Siregar, I. (2018). Impact Of Cybercrime In E-Business And Trust. *International Journal of Civil Engineering and Technology (IJCIET)*, *9*(7), 652-656. https://www.researchgate.net/publication/327335383

Shah, S. A., Balasingam, U., Salman, N. W., Dhanapal, S., & Ansari, K. M. (2020). Restorative Juvenile Justice System in Pakistan: An Overview. *International Journal of Criminal Justice Sciences, 15*(2), 266-282. http://dx.doi.org/10.5281/zenodo.3890056%20

Somer, T. (2019). Taxonomies of cybercrime: An overview and proposal to be used in mapping cyber criminal journeys. *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (pp. 475-482). Academic Conferences and publishing limited. http://toc.proceedings.com/49816webtoc.pdf

Spulbar, C., & Birau, R. (2020). The Effects of Cybercrime on the Banking Sector in ASEAN. In *Financial Technology and Disruptive Innovation in ASEAN* (pp. 130-148). IGI Global. https://doi.org/10.4018/978-1-5225-9183-2.ch007

Tomteberget, D. T., & Larsson, G. (2020). Interrelationship of daily uplifts, daily hassles, coping strategies and stress reactions over time among Norwegian military veterans. *Res Militaris, 10*(2), 1-21. https://resmilitaris.net/index.php/2020/06/01/id1032021/

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(4), 710-729. https://doi.org/10.1109/TSMC.2017.2700495

Tyendezwa, T. G.-M. (2012). Legislation on cybercrime in Nigeria: Imperatives and challenges. *Conference on Regulatory Imperatives for Cybercrimes and Cyber Security in Nigeria, organized by Nigerian Communications Commission, held at International Conference Centre, Abuja, and March 5, 2012.* (pp. 1-17). Federal Ministry of Justice. http://computelsys.com/Downloads/trs-cybersecurity-conference-george-tyendezwa-legislation-on-cybercrime-in-nigeria.pdf.pdf

Urbas, G. (2012). Copyright, crime and computers: new legislative frameworks for intellectual property rights enforcement. *J. Int'l Com. L. & Tech., 7*, 11. https://www.neliti.com/publications/28694/copyright-crime-and-computers-new-legislative-frameworks-for-intellectual-proper

Vukelić, B., & Škaron, K. (2013). Cyber crime and violation of copyright. *36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1127-1130). IEEE. https://ieeexplore.ieee.org/abstract/document/6596426

Wall, D. S., & Yar, M. (2013). Intellectual property crime and the Internet: cyber-piracy and 'stealing'informational intangibles. In *Handbook of internet crime* (pp. 273-290). Willan. https://doi.org/10.4324/9781843929338

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and Society*. SAGE Publications. https://books.google.com.pk/books?id=gpuHDwAAQBAJ

Zagaris, B., & Boyle, D. (2020). Intellectual Property, Cybercrime, Espionage. *IELR, 36*(10), 403. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ielr36&section=131