Bestuur
E-ISSN 2722-4708 | P-ISSN 2302-3783
Vol. 10, No. 2, December 2022, pp. 105-122

The Legal Policy of Criminal Justice Bureaucracy Cybercrime

Agus Raharjo[a,1,*], Rahadi Wasi Bintoro[a,2] Nurani Ajeng Tri Utami[a,3]

[a] Faculty of Law, Universitas Jenderal Soediran, Purwokerto, Indonesia.
[1] agus.raharjo007@gmail.com *, [2] rahadiwasibintoro@gmail.com [3] nurani.utami@unsoed.ac.id

* corresponding author

ARTICLE INFO

Article history
Received: March 25, 2022
Revised: November 30, 2022
Accepted: November 30, 2022

Keywords
Bureaucracy;
Criminal Justice;
Cybercrime;

ABSTRACT

Cybercrime has resulted in astronomical losses for the business community. However, the reactive policy model must be more effective at preventing cybercrime, and the due process model is also inappropriate for combating cybercrime with a high level of speed and mobility. This study is normative legal research employing a conceptual strategy and case studies. The results indicate that the reactive model must be improved in order to prevent cybercrime. The model of due process is not appropriate for deterring cybercrime with a high degree of speed and mobility. The preventative law enforcement strategy is effective, but it requires a high level of law enforcement capability to detect and disable cybercrime, which is something that few Indonesian law enforcement officials possess. Prevention based on the user, which places responsibility on internet users, is fine for individuals but not for businesses. Based on collaboration between corporations, universities, civic society, and non-governmental groups, the collaborative model synthesizes the aforementioned paradigms. Because they are based on plans or roadmaps created by internet stakeholders, regulations, technical aspects, and law enforcement may be effectively implemented and developed.

1. Introduction

The adoption of modern law by Indonesia has resulted in a number of complications. Modern law, which promotes greater certainty, order, and order in the practice or operation of law in society, is considered to be contradictory or to foster the opposite environment.[1] Such a legislation, according to Rahardjo, is not only biological but also criminally generative. Even the Criminal Justice System (CJS), which is expected to be a system of law enforcement and justice, has a criminal element.[2] Several factors contribute to the criminogenic factor in criminal justice: first, the legal factor that serves as the foundation for the operation of criminal justice; second, the factor of law enforcement behavior and

[1]Awaludin Marwan and Fiammetta Bonfigli, 'Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia', *Bestuur*, 10.1 (2022), 22–32 https://doi.org/https://doi.org/10.20961/bestuur.v10i1.59143
[2]Agus Raharjo, 'Law as Artificial Intelligence Products', *Advances in Social Science, Education and Humanities Research, Volume 358 3rd International Conference on Globalization of Law and Local Wisdom (ICGLOW 2019) Law*, 358.Icglow (2019), 389–93 https://doi.org/10.2991/icglow-19.2019.93

third, the judicial bureaucracy that allows law enforcers to "play" their roles and responsibilities for personal, group, and group interests. Each of the three cannot be separated from the others.[3]

The criminogenic aspect of the criminal justice system can be identified from the commencement of a case to its conclusion in a correctional facility, culminating in the court trial. In this process, actors (humans/law enforcement) and bureaucracy/procedures are heavily involved. A police officer is an example of the frontline of law enforcement. Professionalism is needed of police officers in their work. If they are unprofessional, they can become justice parasites who form a vicious cycle or judicial mafia in criminal justice. Numerous incidents demonstrate this, and as a result, people are unwilling to contact police or police institutions, which have become "horror machines." This is a strong illustration of the Criminal Justice System's (CJS) criminalizing nature.[4]

The workings of such criminal justice can be seen in handling cybercrime cases that are relatively more minor than conventional crimes. The number of cybercrime reporting is relatively minor, except for cases classified as cybercrime in a broader sense when referring to its categorization in the Vienna Convention. Many victims – primarily business entities – do not report to the police for various reasons, especially related to computer system attacks. In the business world, attacks on their computer systems mean threatening and even stopping the marketing of products that rely on the internet.[5]

Law enforcers must realize that technology continues to grow by presenting new challenges. The convergence of telecommunications and computing has turned mobile phones into mini-network computers, with the potential for criminality that accompanies them. It was predicted in 1981 by Stephens that the crime would cause a total loss of trillions of rupiah; committed by the main criminals who emerged in the 21st century – cybercriminals. This is a fairly accurate evaluation of the evolution of cybercrime.[6]

Still, with his prediction in 1995, Stephens is pessimistic about the capacity of the police in dealing with emerging cybercrime, so the prospect of limiting cybercrime with technology or conventional law enforcement methods looks bleak. Cybercrime cannot be controlled by conventional methods, technology stands for cyber criminals who have high motivation and commit crimes because it is fun, exciting, and profitable [7]. A similar statement was expressed by Brenner who said that the current crime management model is not effective in dealing with or fighting cybercrimes. Cybercrime is cross-border, carried out far beyond the scale that allows for the commission of a crime. These factors create

[3]Agus Raharjo, 'Prevention of Cybercrime through the Development of Criminal Responsibility Principles for Internet Users', *Jurnal Dinamika Hukum*, 21.3 (2015), 499–511 https://doi.org/10.20884/1.jdh.2021.21.3.3256.This

[4]Karl Kim, 'Dispatches from the Field: The 2022 United Nations Global Platform for Disaster Risk Reduction in Bali, Indonesia', *Transportation Research Interdisciplinary Perspectives*, 15.June (2022), 100644 https://doi.org/10.1016/j.trip.2022.100644

[5]Hany F. Atlam and others, 'Internet of Things Forensics: A Review', *Internet of Things (Netherlands)*, 11 (2020), 100220 https://doi.org/10.1016/j.iot.2020.100220

[6]Hani Y. Ayyoub and others, 'Awareness of Electronic Crimes Related to E-Learning among Students at the University of Jordan', *Heliyon*, 8.10 (2022), e10897 https://doi.org/10.1016/j.heliyon.2022.e10897

[7]Wibowo Heru Prasetiyo and others, 'Survey Data of Internet Skills, Internet Attitudes, Computer Self-Efficacy, and Digital Citizenship among Students in Indonesia', *Data in Brief*, 39 (2021) https://doi.org/10.1016/j.dib.2021.107569

challenges for bureaucracy and law enforcement procedures, as well as challenges for law enforcement investigative resources.[8]

This article will highlight the bureaucracy of law enforcement against cybercrime in Indonesia, especially by highlighting the weaknesses of existing and integrated crime prevention models in the criminal justice system. As an initial illustration, the researcher will illustrate the criminal statistics of cybercrime and end with an alternative solution that is expected to provide material for law enforcement and business entities to prevent cybercrime.

2. Research Method

The method used in this research is normative legal research with a conceptual approach and case studies. The conceptual approach is carried out to understand the concepts related to the bureaucracy and the criminal justice system, cybercrime, prevention, and overcoming of cybercrime.[9] The case approach is carried out to examine cases that occur and solve problems in these cases. The research specification is descriptive. The main data source is secondary data generated from the literature study. The obtained data is analyzed using qualitative descriptive analysis.[10]

3. Results and Discussion

3.1. *Defining and Statistic of Cybercrime*

There are various terms for describing cybercrime. First description from its terms including 'computer crime', 'computer-related crime' or 'crime by computer'. As digital technology became more pervasive, terms such as 'high-technology' or 'information' crime were added to the lexicon. The advent of the Internet brought us 'cybercrime' and 'Internet' or 'net' crime.[11] Other variants include 'digital', 'electronic', 'virtual', 'IT', 'high-tech', and 'technology-enabled' crime.[12] There is, at present, a wide range of adjectives used to describe computer crime – virtual, online, cyber-, digital, high-tech, computer-related, Internet-related, telecommunications-related, computer-assisted, electronic, and 'e-' (as in 'e-crime'). In the same way that the term 'white collar crime' sparked fifty years of discussion and controversy, these terms coined to delimit the scope of computer-related misconduct are likely to be similarly problematic.[13] Each of these terms has a different focus of study, but the general term to describe this form of crime on the Internet is cybercrime. As stated by Clough for several reasons, namely: first, it is commonly used in the literature; secondly, it has found its way into common usage; thirdly, it emphasizes the importance

[8]Mihail Antonescu and Ramona Birău, 'Financial and Non-Financial Implications of Cybercrimes in Emerging Countries', *Procedia Economics and Finance*, 32.15 (2015), 618–21 https://doi.org/10.1016/s2212-5671(15)01440-9

[9]Rian Saputra, M Zaid, and Silaas Oghenemaro, 'The Court Online Content Moderation : A Constitutional Framework', *Journal of Human Rights, Culture and Legal System*, 2.3 (2022), 139–48 https://doi.org/https://doi.org/10.53955/jhcls.v2i3.54

[10]Abdul Kadir Jaelani and Resti Dian Luthviati, 'The Crime Of Damage After the Constitutional Court ' s Decision Number 76 / PUU-XV / 2017', *Journal of Human Rights, Culture and Legal System*, 1.1 (2021), 31–41 https://doi.org/https://doi.org/10.53955/jhcls.v1i1.5

[11]Paul Atagamen, Oluwaseye Oluwayomi, and Alade Adeniyi, 'Legality of EndSARS Protest : A Quest for Democracy in Nigeria', *Journal of Human Rights, Culture and Legal System*, 2.3 (2022), 209–24 https://doi.org/https://doi.org/10.53955/jhcls.v2i3.40

[12]Jessica L. Kamerer and Donna McDermott, 'Cybersecurity: Nurses on the Front Line of Prevention and Education', *Journal of Nursing Regulation*, 10.4 (2020), 48–53 https://doi.org/10.1016/S2155-8256(20)30014-4

[13]Agnieszka Ubowska and Tomasz Królikowski, 'Building a Cybersecurity Culture of Public Administration System in Poland', *Procedia Computer Science*, 207 (2022), 1242–50 https://doi.org/10.1016/j.procs.2022.09.180

of networked computers; and fourthly, and most importantly, it is the term adopted in the Council of Europe Convention on Cybercrime.[14]

Another thing that can be used as a reason for using the word 'cybercrime' is that this crime occurs in the cyber world or cyberspace, not in real space. The perpetrator of this cybercrime can be in real space, but with the sophistication of the machine, the perpetrator does not need to do anything after acting and everything is solved by the machine.[15] It is because of this "machine assistance" that cybercrime is different from ordinary crimes, as stated by Brenner that criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. Cyberspace becomes the tool criminals use to commit old crimes in new ways. Another difference between cybercrime and ordinary crime is the mechanism used to victimize people.[16]

Cybercrime has been widely accepted as an act that is prohibited by regulations and/or law, which involves the use of digital technology in the commission of a crime, is directed at the computing and communication technology itself; or is related to the commission of another crime. Cybercrime also includes how computers and other types of portable electronic devices can be connected to the internet, used to violate the law, and cause harm. One of the keywords to identify whether it is cybercrime or not is connectivity.[17] Cybercrime occurs when a person – through his computer – connects to the Internet and carries out activities mediated by the connected computer. Connectedness is only one of the means that causes someone to commit cybercrime, but behind all of that, of course, other reasons motivate people to commit crimes. Clough wrote, that there are three factors necessary for the commissions of crime: a supply of motivated offenders, the availability of suitable opportunities, and the absence of capable guardians. On all three counts, the digital environment provides fertile ground for offending.[18]

Cybercrime is not just a matter of electronic engineering. Along with the utilization for economic activities as described in the introduction section above, cybercrime also threatens the business world writes that as the twenty-first century's first decade ended, cybercrime was becoming big business on a global scale. Experts estimated cybercriminals raked in more than $100 billion a year. And the influence of the Willie Sutton effect was not limited to hacking and malware.[19] Computer technology was being used to commit traditional crimes—fraud, theft, extortion, and copyright violations—in new ways that were at once more profitable and less likely to lead to the perpetrator being apprehended. Other cybercriminals exploited the technology for different purposes. They used computers to inflict nonfinancial ''harms''—some old, some new — in new ways. The twenty-first century saw a dramatic rise in online stalking, harassment, defamation, and invasion of privacy.[20]

---

[14] Manmeet Mahinderjit Singh and Anizah Abu Bakar, 'A Systemic Cybercrime Stakeholders Architectural Model', *Procedia Computer Science*, 161 (2019), 1147–55 https://doi.org/10.1016/j.procs.2019.11.227

[15] Henry Chong, 'SeCBD: The Application Idea from Study Evaluation of Ransomware Attack Method in Big Data Architecture', *Procedia Computer Science*, 116 (2017), 358–64 https://doi.org/10.1016/j.procs.2017.10.065

[16] Sylwia Ćmiel, 'Cyberbullying Legislation in Poland and Selected EU Countries', *Procedia - Social and Behavioral Sciences*, 109 (2014), 29–34 https://doi.org/10.1016/j.sbspro.2013.12.416

[17] Mark Button and Jack Whittaker, 'Exploring the Voluntary Response to Cyber-Fraud: From Vigilantism to Responsibilisation', *International Journal of Law, Crime and Justice*, 66.January (2021), 100482 https://doi.org/10.1016/j.ijlcj.2021.100482

[18] Fan Yang and Jiao Feng, 'Rules of Electronic Data in Criminal Cases in China', *International Journal of Law, Crime and Justice*, 64.December 2020 (2021), 100453 https://doi.org/10.1016/j.ijlcj.2020.100453

[19] Hwian Christianto, 'Measuring Cyber Pornography Based on Indonesian Living Law: A Study of Current Law Finding Method', *International Journal of Law, Crime and Justice*, 60.November 2019 (2020), 100348 https://doi.org/10.1016/j.ijlcj.2019.100348

[20] Victoria Wang, Harrison Nnaji, and Jeyong Jung, 'Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability', *International Journal of Law, Crime and Justice*, 62.May (2020), 100415 https://doi.org/10.1016/j.ijlcj.2020.100415

Collecting accurate and reliable statistics on cybercrime (both on the number of cases or incidents as well as the magnitude of the losses) is difficult, as is the actual number of victims. Two main sources are commonly used to see these statistics which are unreliable and biased, namely: reports from government institutions, which are often not representative samples; and reports from cyber security companies that only provide information about people or companies that already have cyber hygiene to buy computer security products.[21]

There is no consensus on how to define and measure cybercrime or its impact. Losses can mean material losses, or other dimensions of importance such as integrity, reputation, and functional (operational) privacy. While most of the affected businesses did not report their costs or losses, even though they considered the losses to internal operations to be serious, cyber extortion was considered the most dangerous.[22] In 2017, cybercrime losses reported to Internet Crime Complaint Center (IC3) reached US$1.4 billion. The value of these losses will continue to increase to reach US$6.9 billion in 2021 so the average increase in the value of losses due to cybercrime is recorded at 51.7% per year. IC3 has received an average of 552,000 complaints per year in the last five years, and phishing is the most common type of cybercrime with a total of 323,972 complaints in 2021.[23]

Based on research by security firm McAfee with Central for Strategic and International Strategic (CSIS), the annual loss from cybercrime globally reaches US$600 billion or equivalent to Rp. 8,160 trillion (assuming US$1 = Rp. 13,600) in 2017. The high value of the loss was driven by increased expertise in hackers and the increasing number of crimes in online shops and cryptocurrencies. This report comes after the White House released a report showing cyberattacks had resulted in US$57 billion – US$109 billion in losses in 2016. The study also shows Russia being the leader of cybercrimes reflecting the expertise of the hacker community, followed by North Korea accused of theft. cryptocurrency to fund his regime.[24]

Cybercrime statistical data for Indonesia, shown by the National Cyber and Crypto Agency (BSSN) which recorded cyber-attacks in 2020 reached 495.3 million, an increase of 41% from 2019 which was 290,3 million. The Criminal Investigation Agency (Bareskrim) of the Indonesian National Police also noted that there was an increase in reports of cyber-crimes from 4,360 in 2018 to 4,586 in 2019. Based on the report, 2,549 cases of phishing emails were detected, 79,439 accounts experienced data breaches, and 9,749 websites experienced defacement with the academic sector being the most victims in 2020. According to McQuade III, phishing is a type of social engineering that cybercriminals use when attempting to deceive the potential victim into revealing private information about themselves or their computer accounts, such as usernames, passwords, and financial or bank account numbers. Information acquired through phishing is commonly used to carry out various cybercrimes.[25]

In January – July 2021, traffic anomalies/cyber-attacks reached 741.4 million, with the most categories being malware, denial of service attacks, and trojan activity. The trend of cyber-attacks is dominated by ransomware attacks (malware that demands a ransom) and index data leaks (data

[21]Sitara Karim and others, 'The Dark Side of Bitcoin: Do Emerging Asian Islamic Markets Help Subdue the Ethical Risk?', *Emerging Markets Review*, January, 2022, 100921 https://doi.org/10.1016/j.ememar.2022.100921

[22]Miriam F. Weismann, 'Regulating Unlawful Behavior in the Global Business Environment: The Functional Integration of Sovereignty and Multilateralism', *Journal of World Business*, 45.3 (2010), 312–21 https://doi.org/10.1016/j.jwb.2009.12.002

[23]Milla Sepliana Setyowati and others, 'Strategic Factors in Implementing Blockchain Technology in Indonesia's Value-Added Tax System', *Technology in Society*, 72.November 2022 (2022), 102169 https://doi.org/10.1016/j.techsoc.2022.102169

[24]Hai Tao and others, 'Economic Perspective Analysis of Protecting Big Data Security and Privacy', *Future Generation Computer Systems*, 98 (2019), 660–71 https://doi.org/10.1016/j.future.2019.03.042

[25]Marleen Weulen and others, 'Computers in Human Behavior Is There a Cybercriminal Personality ? Comparing Cyber Offenders and Offline Offenders on HEXACO Personality Domains and Their Underlying Facets', *Computers in Human Behavior*, 140.November 2022 (2023), 107576 https://doi.org/10.1016/j.chb.2022.107576

leaks). The government sector is the highest sector experiencing data leakage due to information stealing malware with a percentage of 45.5%, the financial sector (21.8%), telecommunications (10.4%), law enforcement (10.1%), transportation (10, 1%), and other SOEs (2.1%). There were 25,759 public complaints through the patrol portal in the last 6 years with a total loss of Rp. 5.05 trillion. Online fraud is the most common type of crime with a total of 8,541 cases reported. The losses suffered by corporations due to cyber-attacks averaged US$18.7 million based on a Frost & Sullivan study conducted by Microsoft (2018), while medium-sized companies suffered losses of US$47,000 per company. Cybersecurity incidents in Indonesia in 2017 caused economic losses of US$34.2 billion or IDR 478.8 trillion (equivalent to 3.7% of Indonesia's total GDP of US4932 billion.[26]

The cyber security sector in Indonesia is still very lacking and not even present based on data from A.T. Kearney, while in terms of national strategy, awareness raising, capacity building, and new legislation or regulations are starting to take shape. Data from the National Cyber Security Index (2021) places Indonesia in 5th place out of 10 ASEAN countries with an index score of 38.96 and ranks 77th out of 160 countries included in the 2020 NCSI analysis. The report also states that regulations in Indonesia (Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions) are still weak in addition to the protection of services that are essential in cyber security.[27]

Based on these statistical data, it can be seen that the number of losses suffered by businesses is very large. However, the reason that the image of the business or product produced by a company, the incidents, and losses caused by cybercrime is not disclosed to the public. Especially with the government's involvement in efforts to spy on the business world as reported by Mandiant, a cyber security company based in Virginia, the United States in 2013. Cybercrime against business is not only a war between business people, companies versus companies, but also between countries and the world. business or company.[28]

Mandiant's 60-page report is quite a shocker. The report, which is the result of a three-year investigation, exposed the cyber-espionage practices of Unit 61398, which is directly under China's People's Liberation Command (PLA). The report states that hacking and espionage practices have been going on for at least the last seven years. Recorded 141 companies from all over the world, 115 of them from the United States have become victims. The longest hacking and espionage practice lasted 4 years and 10 months, with the largest amount of data hacked being 6.5 terabytes experienced by one company over 10 months. Of course, the Chinese government denied any involvement in hacking and espionage, but Kevin Mandia – the founder of Mandiant – managed to trace the involvement of the Chinese government through its armed forces.[29]

3.2. The Existing Bureaucratic Criminal Prevention Model in the Criminal Justice System

Law enforcement is carried out through the criminal justice bureaucracy which must be taken through several stages. Bureaucracy in a more limited sense is the same as government organizations, and state administration (public administration). This limited understanding is in line with the term government bureaucracy as used by Almond and Powell, namely: government bureaucracy is a set of positions and tasks that are formally organized and related to complex levels that are subject to formal role makers.[30] Bureaucracy is a very powerful institution because bureaucracy is a neutral rational administrative means on a large scale. Bureaucracy is also an effective tool to help powerful groups dominate other groups. Another concept that I want to put

[26]In Lee, 'Cybersecurity: Risk Management Framework and Investment Cost Analysis', *Business Horizons*, 64.5 (2021), 659–71 https://doi.org/10.1016/j.bushor.2021.02.022
[27] Jaelani and Luthviati.
[28] Raharjo, 'Law as Artificial Intelligence Products'.
[29] Khairul Akram Zainol Ariffin and Faris Hanif Ahmad, 'Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0', *Computers and Security*, 105 (2021), 102237 https://doi.org/10.1016/j.cose.2021.102237
[30] U.W. Prakasa, Satria, 'Reduce Corruption in Public Procurement: The Effort Towards Good Governance', *Bestuur*, 10.1 (2022), 33–42 https://doi.org/https://doi.org/10.20961/bestuur.v10i1.51339

forward is the concept of bureaucratic law. This concept was put forward by Roberto Mangabeira Unger which he called regulatory law. This Regulatory Law consists of explicit provisions that are carried out by a certain government.[31]

Bureaucratic law is a law that is consciously made by the government rather than a law that appears immediately from society. Bureaucratic law marks the presence of the state to actively determine power relations between groups in the form of centralized power and its special staff. The presence of the ruler or the state with its power in the judiciary makes the bureaucracy a tool of rulers. Bureaucracy in law enforcement is needed because achieving justice in society requires management carried out by institutions to realize these goals.[32]

Bureaucracy is an ideal type of relational governance in a rational organization to deal with the tendency of human nature to organize. Weber once introduced the ideal type of bureaucracy, but bureaucracy is often connoted negatively, meaning administrative inefficiency, as depicted in the United States and France. Bureaucracy is described as an organization that cannot correct its behavior by learning from mistakes, the government becomes the master and not the public servant so people are afraid to take initiatives, pile up report files, waste time and drain government funds. The criminal justice bureaucracy is often violated by law enforcement to gain advantages in resolving a case, such as investigative procedures that ignore the suspect's right to legal assistance, use of violence, to restrictions on freedom. to choose a lawyer. Likewise, the performance of advocates who refuse to provide legal aid for the poor and the complicated bureaucracy to obtain it adds to the long list of justice gains in Indonesia.[33]

Bureaucracy in criminal law enforcement in Indonesia is carried out through a system called the CJS. Through this system, law enforcement is carried out in stages, starting from the police, prosecutors, and courts and ending with law enforcement in correctional institutions. Understanding the system in the CJS can be seen from a normative, management, and social point of view. For this article, we will describe the notion from the normative side which views law enforcement officials as implementing institutions for the applicable laws and regulations, so that the four apparatuses are an inseparable part of the law enforcement system. Packer distinguishes the normative approach into two models, namely the crime control model and the due process model. The crime control model is an affirmative type, while the due process model is negative. The definition of the affirmative model always emphasizes the existence and use of formal power in every corner of the criminal justice process, and this model of legislative power is very dominant. The negative definition of the model always emphasizes the limitations on formal power and the modification of the use of that power. The dominant power in this model is the judicial power and always refers to the constitution.[34]

Samuel Walker said that the models developed by Packer are classic distinctions in the criminal justice system, and the distinction between the two models is the result of conflicts between conservative and liberal thinking or between punishment and rehabilitation. The perception of the supporters of the crime control model and the due process model of the criminal justice process is that the process is nothing but decision-making [35]. The crime control model is decision-making that prioritizes excessive leniency, while the due process model is decision-making that prioritizes accuracy and equality. The debate between proponents of these two models revolves around the issue of how to control decision-making to achieve the desired goals. Both models focus on

[31] Zainal Arifin Mochtar and Kardiansyah Afkar, 'President's Power, Transition, and Good Governance', *Bestuur*, 10.1 (2022), 68–83 https://doi.org/https://dx.doi.org/10.20961/bestuur.v10i1.59098
[32] Alok Mishra and others, 'Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations', *Computers and Security*, 120 (2022) https://doi.org/10.1016/j.cose.2022.102820
[33] Alena Yuryna Connolly and Hervé Borrion, 'Reducing Ransomware Crime: Analysis of Victims' Payment Decisions', *Computers and Security*, 119 (2022), 102760 https://doi.org/10.1016/j.cose.2022.102760
[34] Oluwafemi Olukoya, 'Assessing Frameworks for Eliciting Privacy & Security Requirements from Laws and Regulations', *Computers and Security*, 117 (2022), 102697 https://doi.org/10.1016/j.cose.2022.102697
[35] Weulen and others.

decision-making by the police; and questions relating to control over the authority of police officers.[36]

Muladi pointed out the weaknesses of these models and that they are not suitable if applied in Indonesia. According to Muladi, the crime control model is not suitable because this model views repressive actions as the most important in carrying out the criminal justice process, while the due process model is not entirely beneficial because it has anti-authoritarian values. The third model is the inadequate family model because it is too offender oriented.[37] After all, there are still victims (victims) who also need serious attention. According to Muladi, a suitable model for the Indonesian criminal justice system is one that refers to the *daad-dader strafrecht* which he calls the balance of interest model. This model is a realistic model that pays attention to various interests that must be protected by criminal law, namely the interests of the state, the public interest, the interests of individuals, the interests of the perpetrators of crimes, and the interests of victims of crime.[38]

KUHAP adheres to the due process of law (fair legal process) which has a broader meaning than just the formal application of laws or regulations. According to, an understanding of a fair legal process should also contain an inner attitude of respect for the rights of citizens, even though they are the perpetrators of a crime. The system regulated in the Criminal Code can be divided into three stages, namely: pre-adjudication, adjudication, and post-adjudication.[39] The adjudication stage is the dominant stage, this is based on the Criminal Procedure Code which states that both acquittal and guilty verdicts, must be based on facts and circumstances as well as evidence obtained from examination in court. According to him, an CJS that sincerely wants to protect the rights of a citizen who is a defendant will most clearly be revealed in the adjudication stage. It is only at the stage in the trial court that the defendant and his defense can stand upright as parties who are actually at the same level as the public prosecutor.[40]

Mardjono's opinion was opposed by Atmasasmita. Atmasasmita does not deny that the adjudication stage is important in CJS, but it is not the dominant stage. According to him, from the point of view of criminology and victimology, the process of stigmatization has been going on ever since the pre-trial stage, namely at the stage of arrest and detention. At the adjudication stage, there is a process of structural stigmatization and victimization, even though this process has been running since the investigation stage.[41]

Based on the description above, it can be seen that each model has significant weaknesses in the process of preventing and overcoming crime. The crime control model or reactive model as it is known in criminal justice and carried out by the police is not effective enough to prevent cybercrime.[42] Reactive strategies for cybercrime cannot be implemented properly because once the crime is committed, the perpetrator can easily remove the trail. After all, this crime takes place in an electronic environment, so physical evidence is easily lost from memory, or evidence can be easily destroyed. The police may be able to determine the location where the perpetrator accessed the internet after tracing the activity through log files, but when examined, the perpetrator may have

[36]Edward J. Malecki, 'Real People, Virtual Places, and the Spaces in Between', *Socio-Economic Planning Sciences*, 58 (2017), 3–12 https://doi.org/10.1016/j.seps.2016.10.008
[37]Lee.
[38]Richard Apau and Felix N. Koranteng, 'An Overview of the Digital Forensic Investigation Infrastructure of Ghana', *Forensic Science International: Synergy*, 2 (2020), 299–309 https://doi.org/10.1016/j.fsisyn.2020.10.002
[39]Shaun S. Wang, 'Integrated Framework for Information Security Investment and Cyber Insurance', *Pacific Basin Finance Journal*, 57.July (2019), 101173 https://doi.org/10.1016/j.pacfin.2019.101173
[40] Tao and others.
[41] Setyowati and others.
[42] Setyowati and others.

left or even used anonymity where which is possible in cyberspace. In other words, the use of formal activities (affirmative model) is not suitable for dealing with cybercrime.[43]

The structure and process of the criminal justice system find it difficult to overcome cybercrime which has its characteristics, the police have traditionally operated within local boundaries that focus on crimes that occur around their territory.[44] The global nature of the internet is a deterritorialized phenomenon, which brings together perpetrators, victims, and targets that allow physical existence in different times and places. The current law enforcement model will never be enough to protect cyberspace, not be effective enough in controlling cybercrime.[45]

Likewise, with the due process model, it is not suitable to solve cybercrime completely. The typology of the due process model with the negative model always emphasizes restrictions on formal power and modification of the use of that power, where the dominant power in this model is judicial and always refers to the constitution. In Indonesian criminal justice, judicial power rests with the courts and is said to be the last wall of justice, even though cybercrime cannot be quickly prevented through a complicated court process. This model is suitable for legal certainty but is not suitable for preventing crime, especially the types of crimes that have a high level of speed and mobility such as cybercrime.[46]

In addition to the difficulties caused by the incompatibility of the cybercrime prevention and control model in the criminal justice system, other problems arise along with the distinctive characteristics of cybercrime that are not the same as traditional crimes, both in terms of actions, means, and ways to overcome them. Yar argues that the resources and expertise of law enforcement are also a problem. Cybercrime investigations require specialized technical knowledge and skills and these capabilities only a few police officers have the competence to do. Moreover, many police officers do not view cybercrime as a normal parameter of their responsibilities, thereby undermining efforts to put such policing on a systematic footing.[47]

The traditional reactive model is ineffective because cybercrime is difficult to understand. Offenders are difficult to understand because there is no necessary connection between the site being the target of the crime and him either before or after. They are also difficult to understand because they can hide behind the anonymity of identity and leave no physical evidence. “Crimes” are difficult to understand because they do not fall within any identifiable offense and/or pattern of offenders and because they can be committed on such a scale that law enforcement officials cannot react to all of them.[48]

The difficulties in law enforcement against cybercrime are increasing along with the various problems caused by the lack of a legislative framework to deal with this crime effectively. The reactions of various countries (such as Russia; United Arab Emirates; Austria, Georgia cybercrime

---

[43]Moh Iqra, Syabani Korompot, and Al-fatih David, ‘The Principle of Equality Before the Law in Indonesian Corruption Case : Is It Relevant ?’, *Journal of Human Rights, Culture and Legal System*, 1.3 (2021), 135–46. https://doi.org/10.53955/jhcls.v1i3.13

[44]Bambang Ali Kusuma, ‘Establishment of Indonesian Maritime Power: Regulation of Transnational Organized Crime on Illegal, Unreported, and Unregulated (IIU) Fishing’, *International Journal of Criminal Justice Sciences*, 16.2 (2021), 251–66 https://doi.org/10.1016/j.avb.2012.10.005

[45]Frank Ferdik, George Frogge, and Mikaela Cooney, ‘Exploring Further Determinants of Citizen Satisfaction with the Police: The Role of Strain’, *Journal of Criminal Justice*, 81.May (2022), 101931 https://doi.org/10.1016/j.jcrimjus.2022.101931

[46]Sultan Altikriti, Joseph L. Nedelec, and J.C. Barnes, ‘The Influence of Individual Differences on the Formation of Perceptions of Risk, Social Cost, and Rewards of Crime: A Meta-Analysis’, *Journal of Criminal Justice*, 82.April (2022), 101962 https://doi.org/10.1016/j.jcrimjus.2022.101962

[47]Jihong Solomon Zhao and Yan Zhang, ‘Proactive Policing Embedded in Two Models: A Geospatial Analysis of Proactive Activities by Patrol Officers and COP Officers’, *Journal of Criminal Justice*, 82.May (2022), 101972 https://doi.org/10.1016/j.jcrimjus.2022.101972

[48]Alex Tepperman and Jay Rickabaugh, ‘Historical Criminology, a Moving Target: Understanding and Challenging Trends in British and American Periodization’, *Journal of Criminal Justice*, March, 2022, 101978 https://doi.org/10.1016/j.jcrimjus.2022.101978

by trying to adopt various strategies to maintain social order in cyberspace. Russia goes through the same phase as the rest of the world in responding to cybercrime by criminalizing, developing a regulatory system that is by the characteristics of cybercrime, and transforming law enforcement policies and international treaties ratified by Russia. Russian hackers are a major threat to Russia itself and the global threat in general.[49]

The legal measures that have been implemented in many countries lack the resources needed to enforce them. Developing countries – such as Indonesia – have their journey and digital design, but building cyber security based on public sector (government) responsibility is no longer valid. The cyber security ecosystem is not only built through cooperation between the government and the governments of other countries but needs to be carried out in synergy with business, academics, civil society, and non-governmental organizations. Building cybersecurity requires coordination and partnership because cybersecurity is a global issue as well as a prerequisite for economic success.[50]

However, efforts to align strategies in cybercrime prevention and countermeasures are not an easy task. It is very difficult to align the strategy between the government, academia, the business world, and military interests so that it affects the level of strategic and practical policy formulation. Cybercrime is often seen as a technical violation that requires a technical solution, but these crimes are committed by individuals or networks of people, which result in human victims, being detected and prosecuted by criminal justice personnel. Human decision-making, therefore, plays an important role in abuses, justice responses, and policymakers trying to legislate against these crimes.[51]

3.3. Prevention Based on User Model in Cybercrime

Based on the weaknesses that exist in the existing crime prevention model, new steps are needed, because preventing cybercrime is more than just a legal or technical issue, it is not just the job of the police but also the task of stakeholders who use the Internet for various purposes. The policeman is not the god of a savior who is in the place anytime, he is often left behind by the crime itself. In other words, the crime had outrun when the police arrived on the scene.[52]

The need for a new approach to cybercrime prevention is based on three premises. First, it is clear that the traditional law enforcement model – with its reactive approach and hierarchical, military-style organization – cannot deal with cybercrime effectively. The second premise comes from the proliferation of technology, especially information and communication technology with its various products which cover most of our daily life thus changing our environment. The proliferation of technological devices is connected in various ways and creates and maintains a global network that continues to operate smoothly. The third premise is that the proliferation of technology will affect organizational systems and human social activities which have been hierarchical with a top-down approach to structuring social relations and allocation of authority. This hierarchical organizational model evolved to deal with the organization of human activities in

[49]Lin Huff-Corzine and Kayla Toohy, 'The Life and Scholarship of Pauline Tarnowsky: Criminology's Mother', *Journal of Criminal Justice*, January, 2022, 101986 https://doi.org/10.1016/j.jcrimjus.2022.101986
[50]Eric J. Connolly, Joseph A. Schwartz, and Kristina Block, 'The Role of Poor Sleep on the Development of Self-Control and Antisocial Behavior from Adolescence to Adulthood', *Journal of Criminal Justice*, 82.September (2022), 101995 https://doi.org/10.1016/j.jcrimjus.2022.101995
[51]Michael J. Frith, Kate J. Bowers, and Shane D. Johnson, 'Household Occupancy and Burglary: A Case Study Using COVID-19 Restrictions', *Journal of Criminal Justice*, 82.April (2022), 101996 https://doi.org/10.1016/j.jcrimjus.2022.101996
[52]Lynne McCormack and Brendan Lowe, 'Making Meaning of Irreconcilable Destruction of Innocence: National Humanitarian Professionals Exposed to Cybercrime Child Sexual Exploitation in the Philippines', *Child Abuse and Neglect*, 131.September 2021 (2022), 105770 https://doi.org/10.1016/j.chiabu.2022.105770

the real world that are subject to the physical constraints of empirical reality and thus require the use of techniques.[53]

The internet places us not in a hierarchy as in an organization, it can be anywhere, which forms a new type of social organization, namely networks. If the hierarchy places a person in proportion to the social organization, so in connection smash the boundaries, tear down the hierarchy and dismantle the bureaucracy. Networks, unlike hierarchies, are lateral, fluid systems. Networks, unlike hierarchies, decentralize power and authority, thereby empowering individuals. Networks have the capacity to, and very likely will, usher in a new era of cooperation among peoples and social systems. Unfortunately, they can also be exploited for destructive purposes.[54]

Several alternative solutions can be given. First, adding police personnel to be able to react quickly to the occurrence of cybercrime. The assumption is that with the increase in personnel, the speed of handling cybercrime can increase. The problem for Indonesia is whether the state budget is sufficient to finance the addition of police personnel. This is a classic problem that always plagues the police when dealing with relatively new crimes. Second, is the establishment of cyber police or cybercop, which specifically handles cybercrime issues and can react quickly if an incident occurs. If the first is more about the quantity of police, then in the second it is more about the quality of personnel by increasing their capabilities and tools. In some cases, this has been followed up by the establishment of a special cybercrime unit, however, this cannot cover the entire police area in Indonesia, only urban areas have it. This cyber cop does not have to be human, but it can also be automatic policing in cyberspace. Several police agencies have turned to the use of special cybercrime police units. Cybercrime units have evolved and are on track to become a normative aspect of policing, this is a specialization strategy.[55]

Brenner stated that this would involve using automated agents to react to completed cybercrimes and to "patrol" public areas of cyberspace to prevent the commission of cybercrime. While automated cyber policing is certainly a logical alternative, its implementation is surrounded by technical and legal difficulties, thus making it an unrealistic option for the foreseeable future. The third alternative is to build civil defense technology, namely by allowing cybercrime victims to counterattack against their attackers. In other words, victims react when they are targeted by crime. This model is vulnerable to the so-called cyberwar, which can cause chaos in an endless war. This model has minimal intervention by law enforcement (police) so that the outcome of the war is only for those who know about it. However, this model is good for building self-defense and increasing awareness against various threats of cyber-attacks.[56]

This alternative prevention model is based on internet users themselves (prevention based on user). This means that the focus to prevent cybercrime is no longer on the government, police, or judiciary, but on internet users. In a narrow sense, internet users must be equipped with knowledge about good ways of using the internet (guidance principles using the internet) or understanding cyber ethics or netiquette. This step is referred to as prevention by defense by the user himself which tends to arise within him. In addition, users must also equip their internet infrastructure with a security system that should continue to be updated keeping in mind the speed of technological development. This model relies more on the user's sense of responsibility for himself and more broadly for the community to feel safe using the internet. This model places criminal law (and its

[53]Dr Chat Le Nguyen and Dr Wilfred Golman, 'Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: "Law on the Books" vs "Law in Action"', *Computer Law and Security Review*, 40.June 2020 (2021), 105521 https://doi.org/10.1016/j.clsr.2020.105521

[54]Dr Vasileios Karagiannopoulos and others, 'Cybercrime Awareness and Victimisation in Individuals over 60 Years: A Portsmouth Case Study', *Computer Law and Security Review*, 43 (2021), 105615 https://doi.org/10.1016/j.clsr.2021.105615

[55]Michael Palmieri, Neil Shortland, and Presley McGarry, 'Personality and Online Deviance: The Role of Reinforcement Sensitivity Theory in Cybercrime', *Computers in Human Behavior*, 120.October 2020 (2021), 106745 https://doi.org/10.1016/j.chb.2021.106745

[56]Palmieri, Shortland, and McGarry.

apparatus) in the right proportion, namely as the *ultimum remidium*, by prioritizing public participation (internet users) in crime prevention.[57]

Another model is the model introduced by Brenner, namely prevention law enforcement. This model gives the police or law enforcement officers the power to identify and incapacitate those who might commit crimes before they commit them. In other words, law enforcement has acted before the evidence is complete by intervening before the crime materializes. This allows law enforcement to intervene and incapacitate individuals based on predictions of their potential for crime. However, this model tends to rely on someone's indicators that appear on the surface, are too broad, and tend to ignore legal process guarantees. If this is implemented, it will be dangerous because law enforcers can be suspected of having abused power, and there will certainly be more law enforcement actions that will be pre-trial.[58]

Although the burden of crime prevention through the above model shifts to Internet users, this does not mean that the function of legislation and judiciary (criminal justice system) is not important. These functions are still important considering the speed of development of information technology, especially the Internet, which needs to be anticipated immediately through regulation in a law. McQuede III wrote that the Internet carries with it significant new risks of criminal victimization, and thus presents some pressing challenges for legislators and criminal justice agencies. However, attempts to police the Internet for crime control also raise serious dilemmas and dangers. Central here is the tension between surveillance and monitoring of online activities, on the one hand, and the need to protect users' privacy and confidentiality, on the other. Law enforcement agents need to be able to identify offenders and collect evidence of online crimes. Offenders, however, can exploit anonymity and disguise to hide themselves and their activities from praying eyes.[59]

Prevention based on the user model requires users (individuals or business entities) to always know, understand and update information technology developments, especially Internet security technology. However, given the limited knowledge of the user, some basic security systems should have been built up on the computer or laptop. In other words, this model also emphasizes the importance of computer producers (business entities) to be responsible in the form of participating in cybercrime prevention, but this is not hierarchical as in the organizations mentioned above. Users still have the authority in determining the security system used on their computers.[60]

Some of the prevention models above are based on territories with communities that exist in the real world. Of course, with such a background and rationale, prevention by relying on the police and victims cannot prevent cybercrime properly. Once again, cybercrime is different from the real world, because cybercrime is a fluid, lateral phenomenon; it is, in effect distributed "crime". Since cybercrime is a lateral, pervasive phenomenon, it demands a lateral, pervasive solution. This solution can incorporate a reactive element, a purely reactive approach will be inadequate. The solution, therefore, needs to be proactive; it must focus on preventing cybercrime, not merely reacting to it. The solution also needs to employ a collaborative approach, one that combines the efforts of civilians and law enforcement; this approach addresses the problem noted earlier namely that it is neither financially nor pragmatically possible to deploy enough law enforcement officers

[57]Jelle Brands and Janne Van Doorn, 'The Measurement, Intensity and Determinants of Fear of Cybercrime: A Systematic Review', *Computers in Human Behavior*, 127 (2022), 107082 https://doi.org/10.1016/j.chb.2021.107082
[58]Daniel Drewer and Vesela Miladinova, 'The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information under the Europol Regulation', *Computer Law and Security Review*, 33.3 (2017), 298–308 https://doi.org/10.1016/j.clsr.2017.03.006
[59]Benoit Dupont and Thomas J. Holt, 'Advancing Research on the Human Factor in Cybercrime', *Computers in Human Behavior*, 138.August 2022 (2022), 2022–24 https://doi.org/10.1016/j.chb.2022.107410
[60]Thomas J. Holt, 'Understanding the State of Criminological Scholarship on Cybercrimes', *Computers in Human Behavior*, 139.August 2022 (2023), 107493 https://doi.org/10.1016/j.chb.2022.107493

to maintain order in cyberspace. Therefore, the way to address cybercrime is to utilize the community policing model's concepts of a proactive, collaborative approach to "crime".[61]

This collaborative approach to preventing cybercrime needs to be developed with synergy between various parties (stakeholders) who use the internet for various purposes. Thus, information system security is no longer the responsibility of public institutions such as the police but is the responsibility of all parties. The collaborative approach is indeed quite promising, but the right design must be found so that all parties – especially business entities – want to share experiences and technology in building a national cyber security design. In other words, it is necessary to build a roadmap for the development of computer/internet network security, so that there is a direction and a goal to be achieved, namely the security and welfare of internet users.[62]

As the most basic anticipatory step, internet users need to have basic security in their computer systems. Basic security which is a prerequisite for system security and protection must be owned by every internet user, such as antivirus. They also use software and hardware firewalls that regulate communication between computers on the internet network and protect computers from intruders and block worms or hackers that attack the system. In addition to basic security and firewalls, to avoid cybercriminals exploiting system vulnerabilities, it is also necessary to use patches that protect software.[63] Other software that you need to have is antispyware and adware. Spyware attacks are designed to run silently, capturing information about the activities of people, institutions, or corporations. Antispyware and adware will help detect and remove this type of malware from the system and can speed up system operation and can protect internet users when visiting malicious websites. In addition to this basic security, there is much more software that can help protect computer devices and information systems, and more than that, user awareness and interacting and communicating behavior are other factors that are quite decisive.[64]

A collaborative approach that will later produce a design or roadmap for information system security and self-defense from users is also an anticipatory step from cyber-attacks. This can overcome the weaknesses of the cybercrime prevention and countermeasures model. However, it is also necessary to learn from the steps developed by other countries as material for thinking to develop and if appropriate, it can be practiced in Indonesia.[65] Russia is developing a center of incident response to detect, prevent and eliminate the effects of cyber-attacks, as well as working with insurance companies to provide cybercrime risk insurance and legal assistance. An insurance-based model – with subsidies – may be an elegant and new solution that offers assistance to transnational corporations or other aggrieved entities. Is there an insurance company in Indonesia that is willing to bear the risk of internet users being exposed to cyber-attacks? This needs an in-depth study, especially in terms of corporate finance and of course the nature of the internet there is no guarantee of security in it.[66]

4. Conclusion

The business world currently occupies the first and foremost position in the use of the Internet. Along with this, the business world is also the party that suffers the most due to cybercrime. Given the great potential, the prevention of cybercrime is something that must be done. Criminal law and

[61]Jan Gruber and others, 'Foundations of Cybercriminalistics: From General Process Models to Case-Specific Concretizations in Cybercrime Investigations', *Forensic Science International: Digital Investigation*, 43 (2022), 301438 https://doi.org/10.1016/j.fsidi.2022.301438

[62]Patrick Michaud, Eric Beauregard, and Jean Proulx, 'Criminal Nomadism: A Neglected Dimension of Spatial Mobility in Sex Offending', *Journal of Criminal Justice*, 81.May (2022), 101928 https://doi.org/10.1016/j.jcrimjus.2022.101928

[63] Shaen Corbet and Constantin Gurdgiev, 'What the Hack: Systematic Risk Contagion from Cyber Events', *International Review of Financial Analysis*, 65.January (2019), 101386 https://doi.org/10.1016/j.irfa.2019.101386

[64]Huff-Corzine and Toohy.

[65]Marwan and Bonfigli.

[66]Ćmiel.

its law enforcers have limitations in law enforcement, as well as the existing models of cybercrime prevention which have shortcomings based on the rationale and performance of law enforcers who are the core of the model and the bureaucratic disease that undermines it. Therefore, a collaborative approach based on the collaboration of business, academics, civil society, and non-governmental organizations needs to be done, to create a design or roadmap for internet-based information system security. Law enforcement can also be carried out by the nature and character of cybercrime, with support from stakeholders and appropriate and adaptive regulations with developments in information technology.

References

Altikriti, Sultan, Joseph L. Nedelec, and J.C. Barnes, 'The Influence of Individual Differences on the Formation of Perceptions of Risk, Social Cost, and Rewards of Crime: A Meta-Analysis', *Journal of Criminal Justice*, 82.April (2022), 101962 https://doi.org/10.1016/j.jcrimjus.2022.101962

Antonescu, Mihail, and Ramona Birău, 'Financial and Non-Financial Implications of Cybercrimes in Emerging Countries', *Procedia Economics and Finance*, 32.15 (2015), 618–21 https://doi.org/10.1016/s2212-5671(15)01440-9

Apau, Richard, and Felix N. Koranteng, 'An Overview of the Digital Forensic Investigation Infrastructure of Ghana', *Forensic Science International: Synergy*, 2 (2020), 299–309 https://doi.org/10.1016/j.fsisyn.2020.10.002

Ariffin, Khairul Akram Zainol, and Faris Hanif Ahmad, 'Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0', *Computers and Security*, 105 (2021), 102237 https://doi.org/10.1016/j.cose.2021.102237

Atagamen, Paul, Oluwaseye Oluwayomi, and Alade Adeniyi, 'Legality of EndSARS Protest : A Quest for Democracy in Nigeria', *Journal of Human Rights, Culture and Legal System*, 2.3 (2022), 209–24 https://doi.org/https://doi.org/10.53955/jhcls.v2i3.40

Atlam, Hany F., Ezz El-Din Hemdan, Ahmed Alenezi, Madini O. Alassafi, and Gary B. Wills, 'Internet of Things Forensics: A Review', *Internet of Things (Netherlands)*, 11 (2020), 100220 https://doi.org/10.1016/j.iot.2020.100220

Ayyoub, Hani Y., Ahmad A. AlAhmad, Amani Al-Serhan, Mohammad F. Al-Abdallat, Esra'a Al-Muheisen, Hadeel Boshmaf, and others, 'Awareness of Electronic Crimes Related to E-Learning among Students at the University of Jordan', *Heliyon*, 8.10 (2022), e10897 https://doi.org/10.1016/j.heliyon.2022.e10897

Brands, Jelle, and Janne Van Doorn, 'The Measurement, Intensity and Determinants of Fear of Cybercrime: A Systematic Review', *Computers in Human Behavior*, 127 (2022), 107082 https://doi.org/10.1016/j.chb.2021.107082

Button, Mark, and Jack Whittaker, 'Exploring the Voluntary Response to Cyber-Fraud: From Vigilantism to Responsibilisation', *International Journal of Law, Crime and Justice*, 66.January (2021), 100482 https://doi.org/10.1016/j.ijlcj.2021.100482

Chong, Henry, 'SeCBD: The Application Idea from Study Evaluation of Ransomware Attack Method in Big Data Architecture', *Procedia Computer Science*, 116 (2017), 358–64 https://doi.org/10.1016/j.procs.2017.10.065

Christianto, Hwian, 'Measuring Cyber Pornography Based on Indonesian Living Law: A Study of Current Law Finding Method', *International Journal of Law, Crime and Justice*, 60.November 2019 (2020), 100348 https://doi.org/10.1016/j.ijlcj.2019.100348

Ćmiel, Sylwia, 'Cyberbullying Legislation in Poland and Selected EU Countries', *Procedia - Social and Behavioral Sciences*, 109 (2014), 29–34 https://doi.org/10.1016/j.sbspro.2013.12.416

Connolly, Eric J., Joseph A. Schwartz, and Kristina Block, 'The Role of Poor Sleep on the Development of Self-Control and Antisocial Behavior from Adolescence to Adulthood', *Journal of Criminal Justice*, 82.September (2022), 101995 https://doi.org/10.1016/j.jcrimjus.2022.101995

Corbet, Shaen, and Constantin Gurdgiev, 'What the Hack: Systematic Risk Contagion from Cyber Events', *International Review of Financial Analysis*, 65.January (2019), 101386 https://doi.org/10.1016/j.irfa.2019.101386

Drewer, Daniel, and Vesela Miladinova, 'The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information under the Europol Regulation', *Computer Law and Security Review*, 33.3 (2017), 298–308 https://doi.org/10.1016/j.clsr.2017.03.006

Dupont, Benoit, and Thomas J. Holt, 'Advancing Research on the Human Factor in Cybercrime', *Computers in Human Behavior*, 138.August 2022 (2022), 2022–24 https://doi.org/10.1016/j.chb.2022.107410

Ferdik, Frank, George Frogge, and Mikaela Cooney, 'Exploring Further Determinants of Citizen Satisfaction with the Police: The Role of Strain', *Journal of Criminal Justice*, 81.May (2022), 101931 https://doi.org/10.1016/j.jcrimjus.2022.101931

Frith, Michael J., Kate J. Bowers, and Shane D. Johnson, 'Household Occupancy and Burglary: A Case Study Using COVID-19 Restrictions', *Journal of Criminal Justice*, 82.April (2022), 101996 https://doi.org/10.1016/j.jcrimjus.2022.101996

Gruber, Jan, Lena L. Voigt, Zinaida Benenson, and Felix C. Freiling, 'Foundations of Cybercriminalistics: From General Process Models to Case-Specific Concretizations in Cybercrime Investigations', *Forensic Science International: Digital Investigation*, 43 (2022), 301438 https://doi.org/10.1016/j.fsidi.2022.301438

Holt, Thomas J., 'Understanding the State of Criminological Scholarship on Cybercrimes', *Computers in Human Behavior*, 139.August 2022 (2023), 107493 https://doi.org/10.1016/j.chb.2022.107493

Huff-Corzine, Lin, and Kayla Toohy, 'The Life and Scholarship of Pauline Tarnowsky: Criminology's Mother', *Journal of Criminal Justice*, January, 2022, 101986 https://doi.org/10.1016/j.jcrimjus.2022.101986

Iqra, Moh, Syabani Korompot, and Al-fatih David, 'The Principle of Equality Before the Law in Indonesian Corruption Case : Is It Relevant ?', *Journal of Human Rights, Culture and Legal System*, 1.3 (2021), 135–46 https://doi.org/10.53955/jhcls.v1i3.13

Jaelani, Abdul Kadir, and Resti Dian Luthviati, 'The Crime Of Damage After the Constitutional Court ' s Decision Number 76 / PUU-XV / 2017', *Journal of Human Rights, Culture and Legal System*, 1.1 (2021), 31–41

https://doi.org/https://doi.org/10.53955/jhcls.v1i1.5

Kamerer, Jessica L., and Donna McDermott, 'Cybersecurity: Nurses on the Front Line of Prevention and Education', *Journal of Nursing Regulation*, 10.4 (2020), 48–53 https://doi.org/10.1016/S2155-8256(20)30014-4

Karagiannopoulos, Dr Vasileios, Dr Annie Kirby, Shakiba Oftadeh-Moghadam, and Dr Lisa Sugiura, 'Cybercrime Awareness and Victimisation in Individuals over 60 Years: A Portsmouth Case Study', *Computer Law and Security Review*, 43 (2021), 105615 https://doi.org/10.1016/j.clsr.2021.105615

Karim, Sitara, Brian M. Lucey, Muhammad Abubakr Naeem, and Samuel A. Vigne, 'The Dark Side of Bitcoin: Do Emerging Asian Islamic Markets Help Subdue the Ethical Risk?', *Emerging Markets Review*, January, 2022, 100921 https://doi.org/10.1016/j.ememar.2022.100921

Kim, Karl, 'Dispatches from the Field: The 2022 United Nations Global Platform for Disaster Risk Reduction in Bali, Indonesia', *Transportation Research Interdisciplinary Perspectives*, 15.June (2022), 100644 https://doi.org/10.1016/j.trip.2022.100644

Kusuma, Bambang Ali, 'Establishment of Indonesian Maritime Power: Regulation of Transnational Organized Crime on Illegal, Unreported, and Unregulated (IIU) Fishing', *International Journal of Criminal Justice Sciences*, 16.2 (2021), 251–66 https://doi.org/10.1016/j.avb.2012.10.005

Lee, In, 'Cybersecurity: Risk Management Framework and Investment Cost Analysis', *Business Horizons*, 64.5 (2021), 659–71 https://doi.org/10.1016/j.bushor.2021.02.022

Malecki, Edward J., 'Real People, Virtual Places, and the Spaces in Between', *Socio-Economic Planning Sciences*, 58 (2017), 3–12 https://doi.org/10.1016/j.seps.2016.10.008

Marwan, Awaludin, and Fiammetta Bonfigli, 'Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia', *Bestuur*, 10.1 (2022), 22–32 https://doi.org/https://doi.org/10.20961/bestuur.v10i1.59143

McCormack, Lynne, and Brendan Lowe, 'Making Meaning of Irreconcilable Destruction of Innocence: National Humanitarian Professionals Exposed to Cybercrime Child Sexual Exploitation in the Philippines', *Child Abuse and Neglect*, 131.September 2021 (2022), 105770 https://doi.org/10.1016/j.chiabu.2022.105770

Michaud, Patrick, Eric Beauregard, and Jean Proulx, 'Criminal Nomadism: A Neglected Dimension of Spatial Mobility in Sex Offending', *Journal of Criminal Justice*, 81.May (2022), 101928 https://doi.org/10.1016/j.jcrimjus.2022.101928

Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, and Asif Qumer Gill, 'Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations', *Computers and Security*, 120 (2022) https://doi.org/10.1016/j.cose.2022.102820

Mochtar, Zainal Arifin, and Kardiansyah Afkar, 'President's Power, Transition, and Good Governance', *Bestuur*, 10.1 (2022), 68–83 https://doi.org/https://dx.doi.org/10.20961/bestuur.v10i1.59098

Nguyen, Dr Chat Le, and Dr Wilfred Golman, 'Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: "Law on the Books" vs "Law in Action"', *Computer Law and Security Review*, 40.June 2020 (2021), 105521 https://doi.org/10.1016/j.clsr.2020.105521

Olukoya, Oluwafemi, 'Assessing Frameworks for Eliciting Privacy & Security Requirements from Laws and Regulations', *Computers and Security*, 117 (2022), 102697 https://doi.org/10.1016/j.cose.2022.102697

Palmieri, Michael, Neil Shortland, and Presley McGarry, 'Personality and Online Deviance: The Role of Reinforcement Sensitivity Theory in Cybercrime', *Computers in Human Behavior*, 120.October 2020 (2021), 106745 https://doi.org/10.1016/j.chb.2021.106745

Prakasa, Satria, U.W., 'Reduce Corruption in Public Procurement: The Effort Towards Good Governance', *Bestuur*, 10.1 (2022), 33–42 https://doi.org/https://doi.org/10.20961/bestuur.v10i1.51339

Prasetiyo, Wibowo Heru, Noor Banu Mahadir Naidu, Beti Indah Sari, Rochman Hadi Mustofa, Naillysa Rahmawati, Gilang Pambudi Adi Wijaya, and others, 'Survey Data of Internet Skills, Internet Attitudes, Computer Self-Efficacy, and Digital Citizenship among Students in Indonesia', *Data in Brief*, 39 (2021) https://doi.org/10.1016/j.dib.2021.107569

Raharjo, Agus, 'Law as Artificial Intelligence Products', *Advances in Social Science, Education and Humanities Research, Volume 358 3rd International Conference on Globalization of Law and Local Wisdom (ICGLOW 2019) Law*, 358.Icglow (2019), 389–93 https://doi.org/10.2991/icglow-19.2019.93

———, 'Prevention of Cybercrime through the Development of Criminal Responsibility Principles for Internet Users', *Jurnal Dinamika Hukum*, 21.3 (2015), 499–511 https://doi.org/10.20884/1.jdh.2021.21.3.3256.This

Saputra, Rian, M Zaid, and Silaas Oghenemaro, 'The Court Online Content Moderation : A Constitutional Framework', *Journal of Human Rights, Culture and Legal System*, 2.3 (2022), 139–48 https://doi.org/https://doi.org/10.53955/jhcls.v2i3.54

Setyowati, Milla Sepliana, Niken Desila Utami, Arfah Habib Saragih, and Adang Hendrawan, 'Strategic Factors in Implementing Blockchain Technology in Indonesia's Value-Added Tax System', *Technology in Society*, 72.November 2022 (2022), 102169 https://doi.org/10.1016/j.techsoc.2022.102169

Singh, Manmeet Mahinderjit, and Anizah Abu Bakar, 'A Systemic Cybercrime Stakeholders Architectural Model', *Procedia Computer Science*, 161 (2019), 1147–55 https://doi.org/10.1016/j.procs.2019.11.227

Tao, Hai, Md Zakirul Alam Bhuiyan, Md Arafatur Rahman, Guojun Wang, Tian Wang, Md Manjur Ahmed, and others, 'Economic Perspective Analysis of Protecting Big Data Security and Privacy', *Future Generation Computer Systems*, 98 (2019), 660–71 https://doi.org/10.1016/j.future.2019.03.042

Tepperman, Alex, and Jay Rickabaugh, 'Historical Criminology, a Moving Target: Understanding and Challenging Trends in British and American Periodization', *Journal of Criminal Justice*, March, 2022, 101978

https://doi.org/10.1016/j.jcrimjus.2022.101978

Ubowska, Agnieszka, and Tomasz Królikowski, 'Building a Cybersecurity Culture of Public Administration System in Poland', *Procedia Computer Science*, 207 (2022), 1242–50 https://doi.org/10.1016/j.procs.2022.09.180

Wang, Shaun S., 'Integrated Framework for Information Security Investment and Cyber Insurance', *Pacific Basin Finance Journal*, 57.July (2019), 101173 https://doi.org/10.1016/j.pacfin.2019.101173

Wang, Victoria, Harrison Nnaji, and Jeyong Jung, 'Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability', *International Journal of Law, Crime and Justice*, 62.May (2020), 100415 https://doi.org/10.1016/j.ijlcj.2020.100415

Weismann, Miriam F., 'Regulating Unlawful Behavior in the Global Business Environment: The Functional Integration of Sovereignty and Multilateralism', *Journal of World Business*, 45.3 (2010), 312–21 https://doi.org/10.1016/j.jwb.2009.12.002

Weulen, Marleen, Jean-louis Van Gelder, Ard J Barends, and Reinout E De Vries, 'Computers in Human Behavior Is There a Cybercriminal Personality ? Comparing Cyber Offenders and Offline Offenders on HEXACO Personality Domains and Their Underlying Facets', *Computers in Human Behavior*, 140.November 2022 (2023), 107576 https://doi.org/10.1016/j.chb.2022.107576

Yang, Fan, and Jiao Feng, 'Rules of Electronic Data in Criminal Cases in China', *International Journal of Law, Crime and Justice*, 64.December 2020 (2021), 100453 https://doi.org/10.1016/j.ijlcj.2020.100453

Yuryna Connolly, Alena, and Hervé Borrion, 'Reducing Ransomware Crime: Analysis of Victims' Payment Decisions', *Computers and Security*, 119 (2022), 102760 https://doi.org/10.1016/j.cose.2022.102760

Zhao, Jihong Solomon, and Yan Zhang, 'Proactive Policing Embedded in Two Models: A Geospatial Analysis of Proactive Activities by Patrol Officers and COP Officers', *Journal of Criminal Justice*, 82.May (2022), 101972 https://doi.org/10.1016/j.jcrimjus.2022.101972