

Current Challenges in Need of More Stringent Sanctions to Combat Increasing High-tech Crimes in a Developing Country in the Age of Fourth Industrialization

Hoang Qui Do ^a, Tuan Van Vu ^a, Tuan Anh Le ^b

^a Hanoi Law University, Hanoi, Vietnam

^b Graduate Academy of Social Sciences, Hanoi, Vietnam

 Corresponding email: tuanvv@hlu.edu.vn

Abstract

High-tech crime, commonly called cybercrime, is considered a potential threat to individuals, businesses, and governments all over the world. Currently, the fourth industrialization substantially impacts human development, but it also poses many high-tech crimes, which requires a more stringent policy to combat these crimes. This report synthesizes the latest findings on the trends, impacts, and responses to high-tech crimes. The study used the secondary sources of the qualitative method based on the recent approach model of Long-Sutehall et al. (2010), researching, reviewing, generating and synchronizing the common legal frameworks of the legal normative documents, such as Vietnam Criminal Code No. 100/2015/QH13, Law on Cyber Security No. 24/2018/QH14, Budapest Convention (ETS No. 185) and its Protocols, and other legal documentary

references. At present, high-tech crime is regarded as a challenge and a new product of human evolution with profoundly negative impacts on each individual, legal entity, country or even the entire community. International cooperation in combating crimes has now shown effectiveness, as there is a lack of a unique legal framework to address this issue. Currently, there has yet to be a unique, effective international law regulating high-tech crimes; consequently, the legal ground, content and modes of international cooperation in combatting this kind of crime exhibit some differences and deliberately require the commitment and goodwill of the subjects on a global scale.

KEYWORDS *Stringent Sanctions, High-Tech Crimes, International Law, Practical Issues*

Introduction

High-tech crimes pose a significant and evolving threat to our digital society¹. The professionalization of cybercrime, the involvement of nation-states, and the exploitation of new technologies are trends that require vigilant attention. The economic and societal impacts are substantial, affecting individuals, businesses, and critical sectors like healthcare. A coordinated response involving law enforcement, legal frameworks, prevention strategies, and public education is crucial to mitigate the risks and protect against the ever-changing landscape of cybercrime. Schwab² introduces the phrase "*Fourth Industrial Revolution*", commonly called Industry 4.0, to a broader audience in an article by Foreign Affairs, indicating a significant change in how technology is integrated into various aspects of socio-economy. Soon after the introduction of Schwab's term, the terminology was named for the 2016 theme of the World Economic Forum Annual Meeting. This concept encompasses a number of technologies that blur the boundaries between the physical, digital and biological realms. Industry 4.0 flares the significant characteristics of the convergence of novel technology domains, including nanotechnology,

¹ Jim AM Schiks, Steve GA van de Weijer, and E. Rutger Leukfeldt. "High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals." *Computers in Human Behavior* 126 (2022): 106985. <https://doi.org/10.1016/j.chb.2021.106985>

² Schwab, K. (2017). *The Fourth Industrial Revolution*. Crown Publishing Group, New York.

biotechnology, new materials, and advanced digital production technologies. In other words, Industry 4.0 heralds a series of social, political, cultural, and economic upheavals that will unfold over the 21st century. It will be primarily influenced by the convergent revolution of digital, biological, and physical innovations, quickly changing how humans create, exchange, and maximize their values. Although scientific and technological developments have brought many advantages to international exchange and cooperation, they have also created conditions for various types of crimes to arise. The rapid, global spread of cybercrime imprints its severe damages, and criminal acts become more sophisticated, owing to the fact that criminals exploit advanced technologies in their methods of execution, which has a considerable impact and causes concern for not only one country but the entire international community. In addition to its tightly organized legislative bodies regulating the feasibilities of criminal actions, with the current rapid development of techno-sciences, the methods and tricks of high-tech crimes are becoming increasingly diverse, sophisticated, secretive, and unique, which constantly changes to avoid detection by authorities. High-tech crimes continue taking place in almost all areas of cooperation between subjects, causing enormous damage and seriously affecting each country's security and collective security. Recently, the term high-tech crimes might be referred to as cybersecurity, which entails “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets³”.

In recent studies⁴ the impacts of cybersecurity have been greatly discussed to point out the influences on many societies. Typically, McGuire and

³ International Telecommunication Union (ITU). *Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity*. <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Committed%20to%20connecting%20the%20world&text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets>.

⁴ Kranenbarg, Marleen, Weulen, Stijn Ruiter, Jean-Louis van Gelder, and Wim Bernasco. “Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison.” *Journal of Developmental and Life-Course Criminology* 4, no. 1, (2018): 343-364. <https://doi.org/10.1007/s40865-018-0087-8>; Rajasekharaiah, K. M., Chhaya, S. Dule, and Sudarshan, E. “Cyber Security Challenges and its Emerging Trends on Latest Technologies.” *IOP Conference Series: Materials Science and Engineering* 981, (2020): 022062. <http://dx.doi.org/10.1088/1757-899X/981/2/022062>; Matthew N. O. Sadiku, Omobayode I. Fagbohungebe, and Sarhan M. Musa. “Artificial Intelligence in Cybersecurity.” *International Journal of Engineering Research and Advanced Technology* 6, no. 5, (2020): 1-7. <https://doi.org/10.31695/IJERAT.2020.3612>; Wang, XiaoLing.

Dowling⁵, and Harbinson and Selzer⁶ classify cybercrimes into two types, namely cyber-dependent crimes and cyber-enabled crimes. In particular, cyber-enabled crime refers to traditional criminal activities utilized or strengthened by the exploitation of computers, computer networks, or other means of information communications technology (ICT). These crimes might be committed without the help of technology but are significantly enhanced in scale or reach due to the cyber element. Examples of cyber-enabled crime include economic-related cybercrime, intellectual property crime, online marketplaces for unlawful goods, malicious and offensive communications, and offences that purposefully create harmful impacts on individuals, such as cyber-enabled violence against women and girls. On the contrary, cyber-dependent crime is a category of criminal offences executed by means of using of computers, computer networks, or other forms of ICT. These crimes are unique to the digital environment and would not exist without the internet or similar technology. These include activities such as creating and spreading malware, hacking to steal sensitive data, and denial of service attacks that cause financial and/or reputational harm. The Government's National Cyber Security Strategy⁷ identifies different types of criminal activities because cyber-dependent crimes can only be committed through the manipulation of ICT devices which are used as either the means of committing the crime or the aim of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). In contrast, cyber-enabled crime refers to traditional crimes which can be spread quickly by exploiting computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

There have been ongoing incidents relating to cybercriminals using the feasibilities of ICT in the age of highly digitalized societies to commit criminal

“Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime.” *Journal of Physics: Conference Series* 1533, (2020): 032014. <http://dx.doi.org/10.1088/1742-6596/1533/3/032014>

⁵ McGuire, Mike, and Samantha Dowling. *Cyber crime: A review of the evidence*. (October, 2013) <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9>

⁶ Harbinson, Erin, and Nicole Selzer. “The risk and needs of cyber-dependent offenders sentenced in the United States.” *Journal of Crime and Justice* 42, no. 5 (2019): 582-598. <https://doi.org/10.1080/0735648X.2019.1692422>

⁷ The Government's National Cyber Security Strategy. <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>

offences.⁸ Cybercriminals are defined as individuals or groups that engage in criminal activities by targeting or using computers, computer networks, or other networked devices. These illegal activities are carried out with various motivations, often involving the abuse of technology to commit or facilitate traditional crimes.⁹ Recently, cyber-crimes mostly refer to the criminal liability of artificial intelligence systems. The phrase “artificial intelligence (AI)” was coined in the 1950s¹⁰. Now, AI crimes refer to offences related to artificial intelligence technology carried out by unknown criminals through AI systems and robots. Currently, there is no specific legal category for AI criminal crimes; thus, AI criminal crimes are not currently defined as a separate category in criminal law. The regulation and prosecution of crimes related to AI technology may fall under existing categories, such as financial or statutory crimes. The development of AI technology and its potential impact on criminal activities shall require ongoing attention and legal adjustments in the coming time, as this type of crime is a new criminal phenomenon.¹¹

Based on the current situation and the consequences that high-tech crimes have caused, in reality, they have several specific features, creating differences between other types of crimes. Other international crimes are related to using electronic devices connected to the network, mainly utilizing computers or

⁸ Smith, Chris, Brian McGuire, Ting Huang, and Gary Yang. *The History of Artificial Intelligence*. University of Washington: Washington, DC, USA. (2006).

⁹ Schiks, et al. "High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals."; Kshetri, Nir. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly* 31, no. 7, (2010): 1057-1079. <http://www.jstor.org/stable/27896600>; Verma, Shivangi, and Neetu Gupta. "Application of Artificial Intelligence in Cybersecurity". In H. S. Saini, R. Sayal, R. Buyya, & G. Aliseri (Eds.), *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE* (pp. 65-72). Springer Singapore, 2020. https://doi.org/10.1007/978-981-15-2043-3_9

¹⁰ John, McCarthy. "From here to human-level AI." *Artificial Intelligence* 171, no. 18, (2007): 1174-1182. <https://doi.org/10.1016/j.artint.2007.10.009>

¹¹ Abbott, Ryan, and Alex F. Sarch. "Punishing artificial intelligence legal fiction or science fiction." *University of California, Davis* 53, no. 1 (2019): 323-384. <http://dx.doi.org/10.2139/ssrn.3327485>; Aldoseri, Abdulaziz, Khalifa N. Al-Khalifa, and Abdel Magid Hamouda. "Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges." *Applied Sciences* 13, no. 12 (2023): 7082. <https://doi.org/10.3390/app13127082>; Gunawan, Widjaja, Sridevi J, S. Rama Sree, A. Jasmine, and Melanie Lourens. "Implementing AI Techniques for Combating Cybercrimes in Political Science and Management." *European Chemical Bulletin* 12, no. 8, (2023): 8807-8819. <https://www.eurchembull.com/uploads/paper/54d70fb93b54381ecaaab4fdb4976600.pdf>; Sadiku, et al. "Artificial Intelligence in Cybersecurity."

digital devices¹². For these high-tech crimes, subjects committing crimes are those who have knowledge, the ability to update, quick access, and proficient skills in ICT. In particular, high-tech crimes often cause severe consequences for socio-economies and difficulty calculating specific damages later, which leads to the demand of the cooperation process in the security system carrying out at a high level. Additionally, requirements for connecting information and sharing information to identify criminals have also been raised. Punishing possible crimes shall be impossible in case of lacking a comprehensive cooperation level among countries.¹³ Most national security data breach services are typically performed by people who have held positions in government bodies, for example, the Edward Snowden case or the Wikileaks case. For the cooperation mechanism, the information technology (IT) expertise of the team preventing this type of crime shall be trained and retrained regularly to assure the ability to prevent and combat cybercrimes in the future.¹⁴

In current practice, international law needs a legal basis that is comprehensive enough and uniformly regulates activities of fighting and preventing cybercrimes. Accordingly, the international community soon realizes the necessity for a global legal document to create a common and practical framework for cooperation in fighting and preventing this type of crime. The Palermo Convention on Cybercrime, also so-called the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty to address Internet and computing crimes by harmonizing national laws, improving investigative techniques, and promoting transnational cooperation. It was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on November 8th 2001, and became effective in September 2003. This is the first international convention at the global multilateral level on combating transnational organized crime to address cybercrime by harmonizing national laws, improving investigative techniques, and developing cooperation among nations. Similarly, high-tech crime in

¹² Gunawan, et al. "Implementing AI Techniques for Combating Cybercrimes in Political Science and Management."

¹³ Abbott, and Sarch. "Punishing artificial intelligence legal fiction or science fiction."

¹⁴ Alexander, P. Sukhodolov, Artur, V. Bychkov, and Anna, M. Bychkova. "Criminal policy for crimes committed using artificial intelligence technologies: State, problems, prospects." *Journal of Siberian Federal University, Humanities & Social Sciences* 13, no. 1, (2020). <https://doi.org/10.17516/1997-1370-0542>; Sessa, Francesco, Massimiliano Esposito, Giuseppe Cocimano, Sara Sablone, Michele Ahmed Antonio Karaboue, Mario Chisari, Davide Giuseppe Albano, and Monica Salerno. "Artificial Intelligence and Forensic Genetics: Current Applications and Future Perspectives." *Applied Sciences* 14, no. 5, (2024): 2113. <https://doi.org/10.3390/app14052113>

Vietnam is a new type of crime that has emerged for the past few years, but it is increasing rapidly in quantity, has a dangerous nature, and has a level of damage in all essential areas of the country. In other words, Vietnam has been experiencing a rapid increase in high-tech crimes, reflecting the dark side of its digital growth. Cybercrime in Vietnam has grown in quantity and sophistication, posing significant challenges to law enforcement and the general public. While the country is taking steps by promulgating many legal sanctions to improve its cybersecurity infrastructure and legislation, the difficulties of tracing cybercriminals and raising public awareness remain. Collaboration with international organizations and the continual development of law enforcement capabilities are crucial in the fight against cybercrime in Vietnam. Stemming from the above reasons, further research and clarification of international law provisions concerning cybercrimes and cooperation to combat this type of crime are practically essential. Activities in combating cybercrime are regarded as very necessary, especially in the current context of Industry 4.0. Consequently, useful experience from valuable referential sources might be beneficial for developing countries like Vietnam in the effort to cooperate in fighting against cybercrime. The following questions are set out to highlight these above concerns: *first*, what is the present situation of the control of cybercrime, and *second*, comparing some international laws on the issue of preventing and fighting cybercrime, how does it affect developing countries like Vietnam?

The paper aims to clarify the theoretical and legal issues of cybercrime and the regulation of international law in cooperation to fight and prevent high-tech crimes. Concurrently, the study investigates Vietnamese regulations and implementational practices, predicts and proposes solutions to amend the law and maximize the effectiveness of law enforcement activities in Vietnam. It also analyzes and conducts research on theoretical issues about cybercrime, as well as the contents, principles, roles, and sources of international law to combat high-tech crimes. It examines the provisions of international law and its implementation influencing the fight and prevention of cybercrime in some countries. Accordingly, developing countries like Vietnam might take advantage of integrating references and experiences from developed countries to construct and amend their current regulations and practices of the law enforcement process in terms of cybercrime fighting and prevention. In addition, examining international legislative documents is resourceful for developing countries to legalize their legal sanctions in international cooperation in fighting and preventing high-tech crimes.

The qualitative study used secondary sources based on the approach model suggested by Long-Sutehall et al.¹⁵ It pivoted the analysis, synthesis, comparison, systematization, and generalization of the common legal frameworks of the legal normative documents, such as Vietnam Criminal Code No. 100/2015/QH13, Law on Cyber Security No. 24/2018/QH14, the Budapest Convention (ETS No. 185) and its Protocols, and other legal documentary references. Besides, the study was constructed via statistical data to address three main sources, particularly an overview of high-tech crimes and their classification, international law and cooperation, and legal practices of combating high-tech crimes in several countries and regions, especially in Vietnam.

Some reflections of international law in cooperation to combat high-tech crimes

Although Industrial 4.0 has been defined in recent decades, the technoscientific revolution has made many economic, scientific and social sectors dependent on its new technologies. Together with human evolution, the more widely inventions have emerged in social life, the more feasible it is to be exploited or targeted by some novel kinds of criminals¹⁶. As a result, a new form of high-tech crime has emerged in today's society, which is a new term for Vietnam and many countries worldwide. Hence, from the emergence of terminology to introducing concepts, characteristics, or the arrangement of socially dangerous acts, there are still many heterogeneous opinions about its definitions, scope, and limitations. Oxford online dictionary¹⁷ defines a high-tech crime as the use of information or communications technology, and it varies differently between investigative and prosecution agencies. It is also classified as computer intrusions (e.g., malicious hacking), unauthorized modification of data, including destruction of data, denial-of-service (DoS) attacks, and the creation and distribution of malicious software (e.g., viruses, worms, or trojans). Another typical definition from the Oxford Dictionary of

¹⁵ Long-Sutehall, Tracy, Magi Sque, and Julia Addington-Hall. "Secondary analysis of qualitative data: a valuable method for exploring sensitive issues with an elusive population?." *Journal of Research in Nursing* 16, no. 4, (2010): 335-344. <https://doi.org/10.1177/1744987110381553>

¹⁶ El-Din, Eman Ahmad Alaa. "Artificial Intelligence in Forensic Science: Invasion or Revolution?" *Egyptian Society of Clinical Toxicology Journal* 10, no. 2, (2022): 20-32. https://esc tj.journals.ekb.eg/article_272046.html

¹⁷ <https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095936331>

Law¹⁸ is that high-tech crime or cybercrime refers to a crime committed over the Internet. Currently, there are no specific laws regulating cybercrime; however, such cybercrimes might include hacking to commit further offences, unauthorized acts causing or creating a severe risk of damage, distributing or possessing (i.e., downloading) obscene images of children, defamation over the Internet, copyright infringement, and fraud.

Justia¹⁹ defines computer crime, or “*cybercrime*,” as offences by using computing devices over ICT. Cybercrime activities involve high-tech forms of theft or fraud for the purpose of financial gain. Other types of crime involve copyright infringement, exchange of child pornography, and even espionage. Europol²⁰ states that hi-tech crimes are crimes committed using new electronic and digital technology such as the Internet or the help of computers. These crimes are also known as cybercrimes, computer crimes and technology crimes, depending on the area in which they are committed. Kim et al.,²¹ claim that IT crimes are any violation of criminal law that involves the use of knowledge about computer technology in the commission of a crime, investigation or trial. Currently, there is yet to be a unified concept of high-tech crime on an international scale due to inconsistent views on the complicated characteristics of high-tech crime. According to the inaugural meeting in Vienna of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders²², high-tech crimes have been divided into two types of crimes. Firstly, IT crimes, in a narrow sense, are defined as criminal acts of using computers and computer networks to violate the security of computer systems and data storage processes. According to this approach, this type of crime can be understood as a new type of crime directly related to computers and computer networks, affecting and causing damage to users. Secondly, cybercrimes are defined as crimes using computers or other methods related to computers and computer networks, including crimes such as illegally seizing and threatening or falsifying information using computer networks. In this sense, this type of crime has a broad boundary, including many kinds of

¹⁸ *Oxford dictionary of law*. Oxford University Press, 10th Edition, p. 719. <https://global.oup.com/academic/product/a-dictionary-of-law-9780192897497?cc=vn&lang=en&#>

¹⁹ <https://www.justia.com/criminal/offenses/other-crimes/cybercrimes/>

²⁰ *High-tech crime* <https://www.europol.europa.eu/crime-areas/cybercrime/high-tech-crime>

²¹ Kim, Chris, Barrie Newberger, and Brian Shack. “Computer Crimes.” *American Criminal Law Review* 49, no. 2, (2012): 443-488. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7>

²² United Nations (A/CONF.187/15). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. Vienna, 10-17 April 2000.

traditional criminal acts committed with the help of computer tools, such as fraud, phishing, evasion of telecommunication charges, and violation of data privacy. Although these perspectives are not well-defined and lack concrete legal binding, they cemented the first steps of the concept of cybercrime, which has been recognized by many countries. In essence, hyper-tech crimes are crimes related to computers and the information revolution. Thus, these crimes include new crimes formed in the environment of IT and traditional crimes committed with the help of new information technologies.²³ High-tech crime is committed by using computing knowledge, skills, tools, means, and IT achievements at a high level, illegally affecting digital information and electronic data stored, processed, and transmitted in computer systems and high-tech devices. It violates information security and order to severely endanger the rights and legitimate interests of individuals, organizations, countries, or even the entire international community.²⁴

Current globalization significantly affects high-tech crimes in both number and scale, so high-tech crimes also feature more sophisticated tricks. Unlike traditional crimes, high-tech crimes have characteristics that are much more different and complex than any other kind of crime, which mainly entails three factors determining their complexities. Specifically, *firstly*, high-tech crimes have the exact nature and characteristics of all other traditional crimes; that is, they encompass dangerous acts for society with similarities in the essential components of a crime. Nonetheless, the significant distinction between high-tech crimes and other conventional crimes is that ICT plays a decisive role and level in carrying out, concealing and causing unpredictable consequences for society of criminal acts in committing cybercrimes. In other words, high-tech crimes, computers, and IT technology are three essential and indispensable tools for cybercrime.²⁵ If considered from the perspective of the

²³ Galante, Nicola, Rosy Cotroneo, Domenico Furci, Giorgia Lodetti, and Michelangelo Bruno Casali. "Applications of artificial intelligence in forensic sciences: Current potential benefits, limitations and perspectives." *International journal of legal medicine* 137, no. 2, (2023): 445-458. <https://doi.org/10.1007/s00414-022-02928-5>; Kshetri, "Diffusion and Effects of Cyber-Crime in Developing Economies"; Raed, S. A. Faqir. "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview." *International Journal of Cyber Criminology* 17, no. 2, (2023): 77-94.

²⁴ Ellamey, Yasser, and Amr Elwakad. "The criminal responsibility of artificial intelligence systems: A prospective analytical study." *Corporate Law & Governance Review* 5, no. 1, (2023): 92-100. <https://doi.org/10.22495/clgrv5i1p8>

²⁵ Dongmei, Pang, and Nikolay V. Olkhovik. Criminal liability for actions of artificial intelligence: Approach of Russia and China. *Journal of Siberian Federal University, Humanities & Social Science* 15, no. 8, (2022): 116-122. <https://doi.org/10.17516/1997-1370-0542>; Esposito, Massimiliano, Francesco Sessa, Giuseppe Cocimano, Pietro

object and tools of crime, high-tech criminals first violate and affect the regular operation of computer systems, connection networks and related auxiliary devices. Infringement here is understood broadly, meaning damaging, appropriating, or falsifying information about servers, computer networks, other supplementary computing devices, and the information belonging to computer systems and networks. These objects are diverse, from single computers to computer network conversion devices to software programs and information in computer and network systems. Furthermore, computers and connected equipment are valuable assets, so they can become the subject of violating property rights such as theft or property destruction. Compared to conventional crimes, cybercrime is a relatively new type of crime that causes significant losses and is not inferior to traditional crimes.²⁶

Second, regarding the subject of crime, high-tech crimes are committed by subjects with updated knowledge and a deep understanding of computers. To commit a crime, offenders must have enough computer knowledge to commit the act and hide evidence. There are, however, cases where the subjects do not fully understand the regulations related to the operation, exploitation, and use of computer networks or electronic tools, which leads to unintentional damages.²⁷ Another remarkable issue is that the subjects of this criminal group are becoming increasingly "younger" in terms of hackers.²⁸ With the unpredicted developments of IT and new software programs, young people are now quick to take up new technologies. However, their impulsive personalities are likely to commit hyper-tech crimes due to their straightforward and

Zuccarello, Salvatore Roccuzzo, and Monica Salerno. "Advances in Technologies in Crime Scene Investigation." *Diagnostics* 13, no. 20, (2023): 3169. <https://doi.org/10.3390/diagnostics13203169>

²⁶ Dakalbab, Fatima, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas, and Qassim Nasir. "Artificial intelligence & crime prediction: A systematic literature review." *Social Sciences & Humanities Open* 6, no. 1, (2022): 100342. <https://doi.org/10.1016/j.ssaho.2022.100342>; Schiks, and Leukfeldt. "High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals"; Kranenbarg, et al, "Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison."

²⁷ Rajasekharaiah, et al, "Cyber Security Challenges and its Emerging Trends on Latest Technologies"; Verma, and Gupta. "Application of Artificial Intelligence in Cybersecurity"; Wexler, Chuck. "Crime Has Been Changing, and Police Agencies Need to Catch Up". In *The Changing Nature of Crime and Criminal Investigations* (pp. 4-8). Police Executive Research Forum, (2018). <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>

²⁸ Raed, "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview."

innocent motives and purposes, such as creating and spreading harmful information viruses just for fun, sabotaging or infiltrating computers to show off their abilities or satisfy their curiosity.²⁹ Thirdly, the nature of the crime and acts related to high-tech crimes are often very tricky and sophisticated. This feature is determined by many factors; for example, high-tech criminals either destroy the activities of objects in non-physical forms, such as computer programs or electronic data, or without destroying the computer and information networks or their components.³⁰ Consequently, this destruction does not leave traces of destruction in physical form. Besides, the speed at which criminal acts are committed is relatively fast, counting one million seconds using computers with super-fast processing speeds or USB drives containing super malware.³¹

Furthermore, criminals are not limited by time or space because they can commit crimes anytime, anywhere, even in a foreign country or a place very far from the scene. Therefore, investigating and collecting traces is extremely difficult in the fight to prevent and eliminate this type of crime, as the criminal can completely erase the traces of the crime with a pre-installed trace deletion program when the criminal orders are carried out. It can be opined that high-tech crime is the emerging "product" of the era that individuals, organizations, countries and the international community must accept in exchange for prosperity and development³². Most countries have been developing legal norms to prevent and punish this crime. Current criminal laws in developing countries like Vietnam have taken their first steps in criminalizing high-tech crimes. Even though the content is still relatively vague and needs to be specified and detailed for each specific act and adding new criminal acts, the initial

²⁹ Esposito, et al, "Advances in Technologies in Crime Scene Investigation."; Kharbanda, Varun, Seetharaman A, and Maddulety K. "Application of Artificial Intelligence in Cyber security." *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)* 15, no. 1, (2013): 1-13. <http://doi.org/10.4018/ijsppc.318676>; Rajasekharaiah, et al., "Cyber Security Challenges and its Emerging Trends on Latest Technologies."

³⁰ Čerka, Paulius, Jurgita Grigienė, and Gintarė Sirbikytė. "Is it possible to grant legal personality to artificial intelligence software systems?" *Computer Law & Security Review* 33, no. 5, (2017): 688-699. <https://doi.org/10.1016/j.clsr.2017.03.022>

³¹ Almailubi, Arwa Nassar. "Adaptation of Metadata as Supporting Evidence in Digital Criminal Investigation Processes: Proposed Model." *Arab Journal of Criminal Evidences and Forensic Sciences* 3, no. 2, (2021): 3060-3077. <https://doi.org/10.26735/FPFI3820>; Kim, et al., "Computer Crimes."; Rajasekharaiah, et al., "Cyber Security Challenges and its Emerging Trends on Latest Technologies."

³² Hall, W. Stuart, Amin Sakzad, and Kim-Kwang Raymond Choo. "Explainable artificial intelligence for digital forensics." *WIREs Forensic Science* 4, no. 2, (2021): 1-11. <http://dx.doi.org/10.1002/wfs2.1434>

approach and regulation shall also be a basis. A good foundation for the fight and cooperation to prevent and eliminate this new type of crime.³³

The objective of the United Nations Office on Drugs and Crime³⁴ clearly states that international cooperation in the fight against cybercrime is an activity of countries and other subjects of international law based on national laws, international treaties or international practices, and international principles. Other principles include coordinating and helping each other formulate a legal basis and implementing mutual legal assistance in criminal matters, extradition, reception, transfer of convicted persons and other cooperative activities to serve for the investigation, prosecution, trial, enforcement and reduction of cybercrime risks. International law in cooperation in fighting and preventing cybercrime includes a comprehensive set of principles and legal norms governing the relationship between international law subjects in conducting all necessary activities between the parties to prevent, punish, and reduce cybercrime risks from national to international scales.

The main concepts of international cooperation in terms of combating cybercrimes are clearly prescribed in the Budapest Convention.³⁵ *Firstly*, international law in cooperation in fighting and preventing high-tech crimes is considered a content formed and associated with techno-scientific developments. In reality, every legal system, whether international or national, is cautious about newly emerged issues, especially new areas with the early formation of international legal instruments regulating binding adjustment. Moreover, as a "product" of the times, high-tech crime is currently receiving the international community's attention in establishing comprehensive and substantive cooperation mechanisms.

Secondly, the subjects of international law in cooperation to fight and prevent high-tech crimes involve subjects of international law. In particular, countries and international intergovernmental organizations operating in the sector of international criminality play crucial roles in building the legal framework and legally enforcing all contents. International cooperation to prevent and eliminate high-tech crimes. Subjects of international law in cooperation to fight and prevent high-tech crimes have participated in the process of building principles and regulations and are also the subjects affecting and enforcing these principles and norms. Stemming from the nature of the

³³ Kshetri, "Diffusion and Effects of Cyber-Crime in Developing Economies."

³⁴ *United Nations Office on Drugs and Crime*.
<https://www.unodc.org/unodc/en/cybercrime/home.html>

³⁵ Council of Europe. *The Budapest Convention (ETS No. 185) and its Protocols*.
<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

power of each subject of international law, each subject shall have different levels and scopes of participation in cooperation in each specific case.

Thirdly, the subject of regulation of international law in cooperation in fighting and preventing high-tech crimes is the relationship between countries and subjects of international law in conducting all necessary activities between the parties to prevent, punish, and eliminate high-tech crimes from each country to a global scale. The principal contents of cooperative activities include stipulating obligations for countries to harmonize laws and building and perfecting the national legal basis for combat and prevention activities, namely high-tech crime, criminal justice assistance, extradite criminals, transfer of convicted persons, and delimitation of criminal jurisdiction.

Fourthly, in terms of construction and enforcement mechanisms, the principles and norms of international law in cooperation in fighting and preventing high-tech crimes are within the general construction and enforcement mechanism of international law; that is, the self-negotiation or self-enforcement mechanism. The subjects of international law shall be the subjects of the agreement to develop and enforce principles and norms. The unique feature in the formation and application of principles and norms of international law in cooperation in fighting and preventing high-tech crimes lies in the fact that these principles and norms are greatly influenced by the "wave" of development of science and technology.

Therefore, its regulations could be more challenging in achieving long-term stability. Creating a comprehensive mechanism for practical implementation still faces many difficulties when the level of scientific and technical development of different countries is partially the same. Therefore, monitoring and understanding the development trends of science and technology shall have a significant impact on the mechanism for building and implementing the principles and norms of international law in cooperation in fighting and preventing high-tech crime. Finally, international law in cooperation in fighting and preventing high-tech crimes is closely related to other contents of international criminal law, such as extradition issues and jurisdiction, or especially international cooperation matters to fight against international crimes. In reality, some contents of international criminal law in determining jurisdiction or issues extradition and the fulfilment of membership obligations are fully applicable to high-tech crimes, which is extremely necessary when there is a specific correlation between different types of crimes. Besides, this supplement also contributes to reducing "gaps" in the provisions of international law regarding high-tech crimes - a kind of crime that is born and associated with the stages of techno-scientific development of ICT.

Content and its practical implementation of international law in cooperation to combat high-tech crime

The content of international cooperation in fighting and preventing high-tech crimes shall be examined in five aspects, particularly, international law determining the work of harmonizing laws in the process of formulation and application of mechanisms for different countries in terms of strengthening national legal activities to combat and reduce high-tech crime risks; mutual criminal justice assistance; extradition; international transfer of sentenced persons; and determination of judicial jurisdiction.

Firstly, when considering international law relating to harmonizing laws and improving the national legal basis for activities to fight and prevent high-tech crimes, legal harmonization is recognized as one of the fundamental contents to create similarities between the legal systems of the countries involved. A harmonized legal system reduces barriers to implementing specific cooperation activities in investigating and adjudicating criminals or avoiding creating loopholes for criminals to escape punishment by one law. The level of harmonization depends on many factors, such as the level of cooperation between country members, the degree of difference between countries in policies and their "*openness*" in adopting changes to the national legal system when implementing harmonization commitments. For example, in accordance with the provisions of the African Union Convention on Cyber Security and Personal Data Protection, Member States shall ensure that legal and/or regulatory measures are adopted to combat crime. The network shall enhance regional harmonization of these measures and respect the principle of dual identification (as prescribed thereof in Art. 28).³⁶

This comes from the fact that the same act is considered a crime in some countries but not in other countries, or both are identified as crimes but the minimum penalties in different countries might not be similar. Such a difference shall either create a loophole for criminals to avoid extradition under the "*double identification*" principle when fleeing to a country that has yet to define this act as a crime or fail to implement appropriate punishments in case those countries apply much lighter punishments than other countries. Therefore, legal harmonization can prevent criminals from making use of diversification in legal regulations between countries to avoid legal punishment,

³⁶ *African Union Convention on Cyber Security and Personal Data Protection*. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

and simultaneously, it shall also promote international cooperation in preventing and punishing high-tech crimes, especially related to requests for extradition and criminal justice assistance.

Currently, legal documents of international criminal law often stipulate the issue of legal harmonization at a standard level, criminalizing certain acts to create a legal basis for criminalization punishment by law, as well as conducting extradition activities and criminal justice assistance when necessary. In addition, if there is a high level of cooperation between country members, the level of harmonization includes harmonization of penalties, that is, stipulating the minimum penalty level for each act committing certain crimes to create a standard threshold in criminal handling of criminal acts in all members, a typical example at this level is the European Union.³⁷

Secondly, the principle of mutual legal assistance recognized in the Budapest Convention³⁸ denotes that member states must ensure the broadest possible provision of mutual legal assistance to serve investigations or proceedings related to computer crimes, privacy data crimes or collecting evidence in electronic forms about crimes. Similar to other types of crimes, the content of criminal justice assistance for high-tech crimes also includes activities to support the prosecution agencies of countries during the investigation process and prosecutions. Accordingly, common criminal justice assistance activities include (i) exchanging of information such as information related to criminal acts that are in the process of being prepared or having been committed, related natural persons and legal entities, methods and means of committing crimes, and ways to prevent, detect and investigate criminal acts; (ii) planning and carrying out coordinated activities to prevent, detect and investigate criminal acts; (iii) supporting for expert training; (iv) setting up an information system to support activities to prevent and investigate criminal acts; (v) exchanging of legal regulations and documents related to high-tech crimes; (vi) conducting investigation and litigation requests and other specific contents as agreed by the parties.

Thirdly, regarding the principles of extradition, it is subject to a national right and belongs to national sovereignty. On the legal ground of supreme power within its territory, a country has the right to decide whether or not to transfer individuals present in its territory to the requesting country for criminal prosecution.³⁹ Criminal extradition as a binding international legal obligation

³⁷ *Explanatory Report to the Convention on Cybercrime*. <https://rm.coe.int/16800cce5b>

³⁸ The Government's National Cyber Security Strategy. <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>

³⁹ Dongmei, Pang, and Nikolay V. Olkhovik. Criminal liability for actions of artificial intelligence: Approach of Russia and China. *Journal of Siberian Federal University*,

only occurs when a corresponding international treaty between the countries involved stipulates specific conditions allowing extradition. However, this obligation is not absolute because extradition, even in cases where there is a treaty, can only be carried out in accordance with the formalities and conditions consistent with the provisions regulated in that international treaty.⁴⁰ Specifically, to be considered a transnational crime, high-tech crime must involve at least two countries, it must be in accordance with and manifested in one of the aspects specified in the United Nations Convention on Prevention and Control against transnational organized crime stipulates that (i) organized criminal group (Art. 2(a, c)),⁴¹ (ii) transnational offence (Art. 3(2)), and (iii) treaties on high-tech crimes with provisions on extradition (Art. 24(3)).⁴²

Fourthly, the commonly international legal basis for transferring convicted persons is the distinctive regulatory treaties on the transfer of convicted persons, including bilateral and multilateral treaties, of which the most common are bilateral agreements.^{43,44} Common conditions for the transfer of convicted persons stipulated in treaties are prescribed as follows:

- a) The sentenced person is a citizen of the country executing the sentence;
- b) The announced sentence is final, and there are no pending procedures related to the convicted person;
- c) There is the consent of the convicted person;
- d) At the time of receipt of the request for transfer, the remaining time to serve the sentence according to the imposed sentence must be not less than the time prescribed in international treaties or national laws;

Humanities & Social Science 15, no. 8, (2022): 116-122. <https://doi.org/10.17516/1997-1370-0542>; Esposito, et al., "Advances in Technologies in Crime Scene Investigation"; Raed, "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview."

⁴⁰ Čerka, Paulius, Jurgita Grigienė, and Gintarė Sirbikytė. "Is it possible to grant legal personality to artificial intelligence software systems?" *Computer Law & Security Review* 33, no. 5, (2017): 688-699. <https://doi.org/10.1016/j.clsr.2017.03.022>; Kranenbarg, et al., "Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison"; Senthil, C. Selvi, Ramesh N. Sripada, Gunawan Widjaja, Radha, T, and Auadhathi Datta. "Impact and limitations of artificial intelligence in cyber security awareness." *European Chemical Bulletin* 12, no. 8, (2023): 8820-8829.

⁴¹ *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*. <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html>

⁴² The Government's National Cyber Security Strategy. <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>

⁴³ Aldoseri, et.al, "Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges."

⁴⁴ El-Din, "Artificial Intelligence in Forensic Science: Invasion or Revolution?"

- e) Meet the "*dual identification*" conditions according to the criminal laws of the sentencing and execution countries;
- f) The sentencing country and the executing country agree to transfer.

Regarding the conditions of consent of the convicted person and dual identification, there are specific exceptions to these two conditions set out in European Union instruments. Specifically, the regulations are regulated in Article 4 of the Council's Framework Decision 2008/909/JHA⁴⁵ dated November 27, 2008, on the application of the principle of mutual recognition in criminal matters for prison sentences or deprivation penalties, freedom with an aim to enforcement in the European Union. Similarly, the "*dual identification*" condition as prescribed in Article 5 thereof does not apply in the case of a person convicted of cybercrime or child pornography if that person is sentenced to imprisonment or deprivation of liberty measures for a period of at least three years.

In addition to the standard conditions above, some countries now also consider conditions related to human rights to decide whether to transfer convicted persons. The European Court of Human Rights⁴⁶ has applied the same rules for the extradition and deportation of foreigners as for transferring sentenced persons. Accordingly, in some instances, a foreigner cannot be deported if deportation causes a loss of compatibility between the individual's rights and his family or private life (Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms⁴⁷). In some cases, this content may be specifically recognized in bilateral treaties. After receiving the prisoner, the executing country must ensure that the execution of the sentence continues in accordance with its law and simultaneously based on the judgment of the court of the sentencing country. The issue of termination of sentence execution will be implemented when the sentencing country sends a decision confirming that the sentence no longer has to be executed to the executing country.⁴⁸

Finally, regarding a jurisprudential perspective, international law determines the jurisdiction of a country in two senses. On the one hand, the

⁴⁵ Council Framework Decision 2008/909/JHA. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0909&from=EN>

⁴⁶ European Court of Human Rights. <https://www.echr.coe.int>

⁴⁷ European Convention for the Protection of Human Rights and Fundamental Freedoms. https://training.itsilo.org/actrav_cdrom1/english/global/law/coeprot.htm

⁴⁸ Mijwil, Maad, Mohammad Aljanabi, and ChatGPT. "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime." *Iraqi Journal for Computer Science and Mathematics* 4, no. 1, (2023): 65-70. <https://doi.org/10.52866/ijcsm.2023.01.01.0019>

jurisdiction of a particular country is understood—in a broad sense—as the separate rights of each country in the fields of national activity, specifically in the legislative, executive and judicial branches. Thus, national jurisdiction is comprised of the nation's legislative, executive and judicial powers, and this is the ultimate power of a State within its territory—an important factor of national sovereignty. On the other hand, in the narrow sense of this term (national jurisdiction), international law defines national jurisdiction as simply the authority to adjudicate and resolve cases within the scope of one national law. Hence, it can be concluded that some principles of International Criminal Law in determining jurisdiction apply to cybercrime. For example, territorial principles include the location where the act was committed, the place where a computer station was located, and the place where the impact of the offence occurred. After considering the territorial principle, it is necessary to take the principle of the offender's nationality (active nationality) into consideration, and this is the second most popular principle to determine a country's jurisdiction over high-tech crimes. According to the provisions of the Budapest Convention, a State has jurisdiction over an offender of its nationality if one act is punishable under the criminal law of the State in which the act is violated or its committed act is carried out outside the territory of any country (Art. 22(1)(d)).

Practical issues of Vietnam laws concerning international cooperation in struggling high-tech crime

Currently, Vietnam has formulated fairly thorough legal grounds in international cooperation to combat cybercrimes, including regulations issued by Vietnam and international treaties that Vietnam has officially signed or entered into an agreement. Regulations issued by Vietnam in international cooperation in the fight against cybercrimes have been enacted promptly to legalize and supplement deficiencies in legal normative documents related to cybercrimes. In Vietnam, high-tech crimes are classified as ICT-related crimes from Article 285 to Article 294 of the 2015 Criminal Code (amended and supplemented in 2017).

The 2015 Criminal Code establishes a comprehensive framework for addressing high-tech crimes, defining them not as isolated offenses but as a series of illegal activities that exploit advanced technology to undermine social relationships protected by law. Articles 285 to 294 specify various offenses, such as the manufacturing and distribution of tools and software for illicit purposes

(Article 285) and the spreading of harmful software that disrupts computer networks (Article 286). Other articles address illegal access to information, unauthorized infiltration of networks, and the appropriation of property through digital means, as well as the illegal collection and trade of sensitive bank information. This structured approach reflects a commitment to safeguarding both individual rights and societal integrity in an increasingly digital world.

In addition to its legal framework, Vietnam actively pursues a policy of multilateralism and international cooperation. By September 2017, the country had joined 22 international treaties focused on mutual legal assistance in criminal matters, including extradition and the transfer of sentenced individuals. To effectively combat cybercrime, specialized agencies like the Cyber Security and Crime Prevention Department within the People's Police, along with the Vietnam People's Army, have been tasked with direct action and guidance against cyber threats.⁴⁹ These efforts are complemented by collaboration with various organizations and individuals, reinforcing Vietnam's commitment to maintaining cybersecurity and participating as a responsible member of the international community.

From the experiences of developed countries around the world in fighting and preventing high-tech crimes, some valuable solutions can be applied to improve the effectiveness of fighting high-tech crimes for developing countries, typically in Vietnam today, as follows:

First, it is necessary to promote international cooperation to prevent high-tech crimes by strengthening negotiations and signing and joining international treaties on crime prevention and control, particularly high-tech crimes. It shall focus on strategic partner countries and global partners, countries with traditional relations, neighbouring countries, countries with a large population of Vietnamese people, and countries with economic and investment cooperation and development with Vietnam. Cooperation in this way is set as a channel for sharing information, experience, and mutual support in crime prevention and training and developing cyber security solutions. In addition, Vietnam has to establish a legal mechanism for coordination between forces specialized in preventing and combating cybercrimes between Vietnam and other countries. Along with that, it is essential to build a coordination agency responsible for linking forces specialized in preventing and combating crimes using high technology between countries so that they can regularly and quickly create close connections with each other in fighting and preventing high-tech

⁴⁹ *People's Police - Department of Cyber Security and Crime Prevention*. <https://en.cand.com.vn/public-security-forces/Department-of-Cyber-Security-and-Hi-tech-Crime-Prevention-requested-to-effectively-prevent-cyber-crimes-i549548/>

crimes. It is crucial to continue to effectively carry out the plans to implement the conventions and agreements on cooperation to combat crimes between the Government and the Ministry of Public Security of Vietnam and respective bodies of other countries with a large number of criminals committing crimes using high technology in Vietnamese territory. Simultaneously, it is necessary to strengthen diplomacy to reach an agreement to have signatories and agreements on cooperation in the fight against crimes, especially high-tech crimes, with other countries where Vietnam has not signed agreements on mutual legal assistance in criminal matters, extradition agreements, and agreements on cooperation in crime prevention and control.

Second, law enforcement agencies in charge of preventing high-tech crime need to utilize human resources and learn from other countries' experiences in combatting cybercrimes in terms of their management and operation network. In addition, conducting research and exploiting sponsored projects on equipment and facilities is required. Similarly, international training courses, conferences, and seminars on preventing and combating crimes using high technology to share information and coordinate to prevent crimes using high technology effectively shall be implemented thoughtfully. In particular, it is vital to participate proactively and actively in bilateral and multilateral cooperation frameworks, international law enforcement organizations, and associations such as INTERPOL⁵⁰, ASEANAPOL⁵¹, and the United Nations Office on Drugs and Crime (UNODC).⁵²

Third, one of the core issues to enhance the role and ensure effective crime fighting and prevention activities using high-tech instruments is to strengthen the capacity of specialized agencies. To improve the capacity to prevent, investigate and discover high-tech crimes, the Government shall have projects for training, retraining and coaching both domestically and internationally on international law, professional techniques, and languages to meet changes in criminal methods and tactics using high technology. It is necessary to concentrate better on promoting the role and strengthening the activities of the specialized force in preventing high-tech crimes, namely the INTERPOL Vietnam Office⁵³ and the cyber security and crime prevention force using high technology. The Government needs to orient a strategy to set up and develop a team of specialized officials who are well-equipped with sufficient knowledge of law, operations, and information technology and are on par with their tasks in

⁵⁰ INTERPOL. <https://www.interpol.int/en>

⁵¹ ASEANAPOL. <http://www.aseanapol.org/home>

⁵² UNODC. <https://www.unodc.org>

⁵³ *INTERPOL Vietnam Office*. <https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/VIET-NAM>.

new, unpredictable situations. The State needs to have reasonable policies to encourage, attract, and recruit officials with high qualifications in science and technology and the ability to fight against high-tech crimes to serve in specialized agencies.

Fourth, it is crucial to equip advanced equipment and technology in the fight and prevention of high-tech crime because their characteristics always use IT equipment and machinery in criminal activities; thus it is required specialized agencies such as the Department of Cyber Security and Hi-tech Crime Prevention⁵⁴ to use high technology, and the Cyber Security Department (Ministry of Public Security) shall invest heavily in modern specialized equipment and build a team of highly qualified officers. Although the Government has paid much attention to investing in equipment and machinery to keep up with the fast changes in applying sciences and technology to prevent high-tech crime, the most updated technical equipment, specialized applications, and advanced instruments shall be utilized. Therefore, the Government needs to continue to promulgate investment projects to purchase equipment for specialized agencies in addition to approving and implementing numerous critical projects under the establishment of the National Cybersecurity Association (NCA).⁵⁵

Fifth, it is a must to establish and maintain different information exchange channels. It shall implement and choose appropriate information exchange mechanisms for each country through the following forms: a hotline, office of crime prevention liaison officer, or representative of the Ministry of Public Security located in the host country. It is crucial to set up and keep a "hotline" or information exchange channel (liaison officer) as a basis for exchanging information between cybercrime prevention forces between Vietnam and several countries that regularly cooperate in the fight against crimes, especially cybercrime quickly exchange information to meet the requirements of the urgent, convenient, and accurate situations.

Sixth, the government shall concentrate on and concisely target international cooperation to combat cybercrimes. Law enforcement bodies shall determine the localization and nationality of the subjects to provide effective and authoritative content in international cooperation to prevent and fight cybercrime. According to mutual agreements, it is necessary to continue to determine a high level of comprehensive cooperation between Vietnam and

⁵⁴ INTERPOL Vietnam Office.

⁵⁵ [https://en.vietnamplus.vn/nca-aims-to-promote-vietnam-as-safe-cyber-secure-country-post268815.vnp#:~:text=Hanoi%20\(VNA\)%20-%20The%20establishment,of%20the%20National%20Cybersecurity%20Association.](https://en.vietnamplus.vn/nca-aims-to-promote-vietnam-as-safe-cyber-secure-country-post268815.vnp#:~:text=Hanoi%20(VNA)%20-%20The%20establishment,of%20the%20National%20Cybersecurity%20Association.)

foreign countries, which is an important content in collaboration to prevent and combat high-tech crimes based on mutual respect, mutual benefit, and equality to contribute to sustainable development and stability of comprehensive strategic cooperative partnerships in signed treaties. It is necessary to continue to increase the exchange of delegations at all levels, from central to local levels, to exchange information and experiences, sign cooperation agreements that relevant parties are interested in, and create a legal ground to support and help improve coordination to improve the efficiency and firmly protect the security of each country. Besides, it is essential to effectively organize alternate bilateral meetings between cyber-security prevention units annually.

Finally, Vietnam has tried its utmost to confer and propose the best initiatives and feasible solutions so that the police forces of ASEANAPOL member countries and partners can promote closer and more comprehensive collaboration in preventing and combating all types of crimes, especially cybercrime in the spirit of responsibility, solidarity, and mutual trust to ensure the area to be increasingly safer. Police between countries need to strengthen cooperation in information sharing and carry out campaigns and programs to fight transnational crimes, including crimes using high technology. They shall flexibly apply legal regulations to make coordination in investigating and discovering specialized projects and cases more effective. At the same time, the police forces of ASEANAPOL member countries and partners shall collaborate closely and support each other at other international forums to demonstrate solidarity and unity in the true spirit of mutual ASEAN community.

For the INTERPOL Vietnam Office, it is necessary to effectively support professional units at the Central Government and police units in localities throughout the country to coordinate investigations and resolve many severe cases. There are critical foreign factors related to security and order. In particular, it is necessary to improve the guidance and direct implementation of many requests for mutual legal assistance in criminal matters and extradition by domestic and foreign authorities, ensuring success in the fight against high-tech crimes and enhancing the position of the People's Public Security force in the international arena. INTERPOL Vietnam Office's activities must focus on collecting, analyzing, and processing information about cybercrimes to advise on strategies and plans for international cooperation in the fight against crime. They need to conduct primary research to forecast the transnational crime situation as well as propose specific measures to strengthen international cooperation in preventing and combating cybercrimes and implement specific coordination activities in handling requests for investigation of cases, tracing and arresting criminals and issues of mutual legal assistance in criminal matters

and extradition in cases, especially with countries where Vietnam has not signed the mutual legal assistance Agreements in criminal matters, Extradition Agreement, Agreement on Cooperation in Crime Prevention and Control.

Conclusion

It can be argued Industry 4.0 is not simply an inevitable trend, but it has far-reaching consequences for almost every country in the world. Besides its tremendous benefits, countries have to confront significant non-traditional security challenges due to the impact of Industry 4.0. Unlike previous revolutions, Industry 4.0 demands each individual, country or institution to change themselves to keep updated if they do not want to be left behind or become a victim of cybercrime. Many novel cybercrimes have come into existence in accordance with the unpredictable development of Industry 4.0, and it is hard to forecast the growth of this trend in the coming time. As a consequence of the lack of single legal sanctions to control the dark side of the development of Industry 4.0, cybercrime is likened to a “product” of the era that every country has to accept in return for its prosperity and growth. Until now, there is only one international treaty regulating cybercrime; that is the 2001 Budapest Convention (ETS No. 185) and its Protocols (commonly referred to as the Budapest Convention) on a global scale.

In addition, international treaties on criminal legal assistance, extradition, and transfer of convicted persons signed between countries are the direct legal grounds for carrying out these actions at the bilateral level. Mutual assistance activities occur between countries in the process of resolving criminal cases in general and criminal cases related to high-tech crimes in particular. Confronting the complexity and negative consequences of cybercrimes, countries have recognized the urgent need for one harmonized legal sanction in collaboration with fighting and preventing high-tech crimes. It is commented that international law is taken as the legislative basis for countries to conduct these cooperative activities through cooperation approaches, such as forming international agencies and institutions to prevent high-tech crimes, harmonizing laws, providing criminal justice assistance and extradition, and conducting coordinated investigations. It has characterized a common legal mechanism at different levels, from bilateral, regional to global scales to collaborate mutual activities between countries to reduce the potential risks of cybercrimes. Based on the provisions of international law, Vietnam has been conducting many international cooperation activities to combat high-tech crimes.

In practice, Vietnam has coordinated to detect, prevent, investigate and handle many criminals using high technology with foreign elements in Vietnamese territory or those living abroad but harming the interests of foreign countries, benefits of individuals and organizations in Vietnam or cases of fraud targeted at appropriating property and high-tech gambling in Vietnam. Legally, Vietnam has signatory with many international treaties and agreements on cooperation in fighting high-tech crimes. Vietnam has issued a system of general and specialized legal documents to directly regulate the content of cooperation in combatting high-tech crimes, such as the Law on Information Technology 2006 and the Law on Cyber Information Security 2015, Cyber Security Law 2018, Criminal Code 2015, Criminal Procedure Code 2015, Decree No. 25/2014/ND-CP regulating crime prevention and other violations of law using high technology, Joint Circular No. 10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC September 10, 2012 of the inter-sectoral Ministry of Public Security, Ministry of National Defense, Ministry of Justice, Ministry of Information and Communications, Supreme People's Procuracy, Supreme People's Court, guiding the implementation of several provisions of the criminal code on many crimes including cybercrime. Therefore, in addition to amending the legal system and strengthening cooperation with countries around the world, Vietnam shall continuously update knowledge and new advanced high-tech equipment from international organizations and developed countries to protect its sovereignty against the potential threats of high-tech crime.

References

- Abbott, Ryan, and Alex F. Sarch. "Punishing artificial intelligence legal fiction or science fiction." *University of California, Davis* 53, no. 1 (2019): 323-384. <http://dx.doi.org/10.2139/ssrn.3327485>
- Aldoseri, Abdulaziz, Khalifa N. Al-Khalifa, and Abdel Magid Hamouda. "Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges." *Applied Sciences* 13, no. 12 (2023): 7082. <https://doi.org/10.3390/app13127082>
- Alexander, P. Sukhodolov, Artur, V. Bychkov, and Anna, M. Bychkova. "Criminal policy for crimes committed using artificial intelligence technologies: State, problems, prospects." *Journal of Siberian Federal University, Humanities & Social Sciences* 13, no. 1, (2020). <https://doi.org/10.17516/1997-1370-0542>

- Almailubi, Arwa Nassar. "Adaptation of Metadata as Supporting Evidence in Digital Criminal Investigation Processes: Proposed Model." *Arab Journal of Criminal Evidences and Forensic Sciences* 3, no. 2, (2021): 3060-3077. <https://doi.org/10.26735/FPF13820>
- Čerka, Paulius, Jurgita Grigienė, and Gintarė Sirbikytė. "Is it possible to grant legal personality to artificial intelligence software systems?" *Computer Law & Security Review* 33, no. 5, (2017): 688-699. <https://doi.org/10.1016/j.clsr.2017.03.022>
- Council of Europe. *The Budapest Convention (ETS No. 185) and its Protocols* (2001). <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- Dakalbab, Fatima, Manar Abu Talib, Omnia Abu Waraga, Ali Bou Nassif, Sohail Abbas, and Qassim Nasir. "Artificial intelligence & crime prediction: A systematic literature review." *Social Sciences & Humanities Open* 6, no. 1, (2022): 100342. <https://doi.org/10.1016/j.ssaho.2022.100342>
- Dongmei, Pang, and Nikolay V. Olkhovik. Criminal liability for actions of artificial intelligence: Approach of Russia and China. *Journal of Siberian Federal University, Humanities & Social Science* 15, no. 8, (2022): 116-122. <https://doi.org/10.17516/1997-1370-0542>
- El-Din, Eman Ahmad Alaa. "Artificial Intelligence in Forensic Science: Invasion or Revolution?" *Egyptian Society of Clinical Toxicology Journal* 10, no. 2, (2022): 20-32. https://escj.journals.ekb.eg/article_272046.html
- Ellamey, Yasser, and Amr Elwakad. "The criminal responsibility of artificial intelligence systems: A prospective analytical study." *Corporate Law & Governance Review* 5, no. 1, (2023): 92-100. <https://doi.org/10.22495/clgrv5i1p8>
- Esposito, Massimiliano, Francesco Sessa, Giuseppe Cocimano, Pietro Zuccarello, Salvatore Roccuzzo, and Monica Salerno. "Advances in Technologies in Crime Scene Investigation." *Diagnostics* 13, no. 20, (2023): 3169. <https://doi.org/10.3390/diagnostics13203169>
- Galante, Nicola, Rosy Cotroneo, Domenico Furci, Giorgia Lodetti, and Michelangelo Bruno Casali. "Applications of artificial intelligence in forensic sciences: Current potential benefits, limitations and perspectives." *International journal of legal medicine* 137, no. 2, (2023): 445-458. <https://doi.org/10.1007/s00414-022-02928-5>
- Gunawan, Widjaja, Sridevi J, S. Rama Sree, A. Jasmine, and Melanie Lourens. "Implementing AI Techniques for Combating Cybercrimes in Political Science and Management." *European Chemical Bulletin* 12, no. 8, (2023): 8807-8819.

<https://www.eurchembull.com/uploads/paper/54d70fb93b54381ecaaab4fdb4976600.pdf>

- Hall, W. Stuart, Amin Sakzad, and Kim-Kwang Raymond Choo. "Explainable artificial intelligence for digital forensics." *WIREs Forensic Science* 4, no. 2, (2021): 1-11. <http://dx.doi.org/10.1002/wfs2.1434>
- Harbinson, Erin, and Nicole Selzer. "The risk and needs of cyber-dependent offenders sentenced in the United States." *Journal of Crime and Justice* 42, no. 5 (2019): 582-598. <https://doi.org/10.1080/0735648X.2019.1692422>
- Jim A. M. Schiks, Steve G. A. van de Weijer, and Rutger E. Leukfeldt. "High-tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals." *Computers in Human Behavior* 126, no. 1, (2022): 106985. <https://doi.org/10.1016/j.chb.2021.106985>
- International Telecommunication Union (ITU). *Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity*. <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx#:~:text=Committed%20to%20connecting%20the%20world&text=Cybersecurity%20is%20the%20collection%20of,and%20organization%20and%20user's%20assets>.
- Kim, Chris, Barrie Newberger, and Brian Shack. "Computer Crimes." *American Criminal Law Review* 49, no. 2, (2012): 443-488. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7>
- Kshetri, Nir. "Diffusion and Effects of Cyber-Crime in Developing Economies." *Third World Quarterly* 31, no. 7, (2010): 1057-1079. <http://www.jstor.org/stable/27896600>
- Kranenbarg, Marleen, Weulen, Stijn Ruiter, Jean-Louis van Gelder, and Wim Bernasco. "Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison." *Journal of Developmental and Life-Course Criminology* 4, no. 1, (2018): 343-364. <https://doi.org/10.1007/s40865-018-0087-8>
- Kharbanda, Varun, Seetharaman A, and Maddulety K. "Application of Artificial Intelligence in Cyber security." *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)* 15, no. 1, (2013): 1-13. <http://doi.org/10.4018/ijspcc.318676>
- Long-Sutehall, Tracy, Magi Sque, and Julia Addington-Hall. "Secondary analysis of qualitative data: a valuable method for exploring sensitive issues with an elusive population?." *Journal of Research in Nursing* 16, no. 4, (2010): 335-344. <https://doi.org/10.1177/1744987110381553>

- Matthew N. O. Sadiku, Omobayode I. Fagbohunbe, and Sarhan M. Musa. "Artificial Intelligence in Cybersecurity." *International Journal of Engineering Research and Advanced Technology* 6, no. 5, (2020): 1-7. <https://doi.org/10.31695/IJERAT.2020.3612>
- McGuire, Mike, and Samantha Dowling. *Cyber crime: A review of the evidence*. (October, 2013) <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5e089b9bac3cdba577724cf0cd23f648a4f952d9>
- John, McCarthy. "From here to human-level AI." *Artificial Intelligence* 171, no. 18, (2007): 1174-1182. <https://doi.org/10.1016/j.artint.2007.10.009>
- Mijwil, Maad, Mohammad Aljanabi, and ChatGPT. "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime." *Iraqi Journal for Computer Science and Mathematics* 4, no. 1, (2023): 65-70. <https://doi.org/10.52866/ijcsm.2023.01.01.0019>
- Raed, S. A. Faqir. "Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview." *International Journal of Cyber Criminology* 17, no. 2, (2023): 77-94. <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/189>
- Rajasekharaiah, K. M., Chhaya, S. Dule, and Sudarshan, E. "Cyber Security Challenges and its Emerging Trends on Latest Technologies." *IOP Conference Series: Materials Science and Engineering* 981, (2020): 022062. <http://dx.doi.org/10.1088/1757-899X/981/2/022062>
- Smith, Chris, Brian McGuire, Ting Huang, and Gary Yang. *The History of Artificial Intelligence*. University of Washington: Washington, DC, USA. (2006).
- Schwab, Klaus. *The Fourth Industrial Revolution*. Crown Publishing Group, New York, 2017.
- Senthil, C. Selvi, Ramesh N. Sripada, Gunawan Widjaja, Radha, T, and Auadhati Datta. "Impact and limitations of artificial intelligence in cyber security awareness." *European Chemical Bulletin* 12, no. 8, (2023): 8820-8829. <https://www.eurchembull.com/uploads/paper/76fef900d1ca70965feb53dd886529a.pdf>
- Sessa, Francesco, Massimiliano Esposito, Giuseppe Cocimano, Sara Sablone, Michele Ahmed Antonio Karaboue, Mario Chisari, Davide Giuseppe Albano, and Monica Salerno. "Artificial Intelligence and Forensic Genetics: Current Applications and Future Perspectives." *Applied Sciences* 14, no. 5, (2024): 2113. <https://doi.org/10.3390/app14052113>

- United Nations (A/CONF.187/15). *Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. Vienna, 10-17 April 2000. <https://digitallibrary.un.org/record/404748?ln=en&v=pdf>
- Verma, Shivangi, and Neetu Gupta. "Application of Artificial Intelligence in Cybersecurity". In H. S. Saini, R. Sayal, R. Buyya, & G. Aliseri (Eds.), *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE* (pp. 65-72). Springer Singapore, 2020. https://doi.org/10.1007/978-981-15-2043-3_9
- Wang, XiaoLing. "Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime." *Journal of Physics: Conference Series* 1533, (2020): 032014. <http://dx.doi.org/10.1088/1742-6596/1533/3/032014>
- Wexler, Chuck. "Crime Has Been Changing, and Police Agencies Need to Catch Up". In *The Changing Nature of Crime and Criminal Investigations* (pp. 4-8). Police Executive Research Forum, (2018). <https://www.policeforum.org/assets/ChangingNatureofCrime.pdf>

Acknowledgment

The authors thanks Hanoi Law University for its encouragement and support to complete this research paper.

Funding Information

This paper is financially supported by Hanoi Law University

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

History of Article

Submitted : March 2, 2024

Revised : May 28, 2024; August 21, 2024

Accepted : September 15, 2024

Published : September 22, 2024