The Trans-National Cybercrime Court: Towards a New Harmonisation of Cyber Law Regime in ASEAN

Prepared for "Legal Co-operation, Harmonisation and Unification: An ASEAN Perspective" Conference

Kwan Yuen IU[1] & Vanessa Man-Yi WONG[2]

Abstract

Legal Harmonisation is necessary to combat the transnational nature of cybercrimes. However, this is a difficult task in ASEAN as it requires all ASEAN member states to agree on a uniform cybercrime regulatory framework. The rapid evolution of cybercrime also undermines a static convention. This leads to the question: How to design a harmonised regulatory framework to tackle the rapid evolution of cybercrime? Regrettably, the Budapest Convention failed to facilitate the legal harmonisation in ASEAN with its inability to reach universal consensus.

In this paper, it is submitted that a regional cybercrime court, namely, the ASEAN Cybercrime Court can be an alternative approach to achieving legal harmonisation with the prevalence of cybercrimes. The theoretical framework is based on the concept of international common law articulated by Andrew Guzman and Timothy Meyer, in which certain members unable to agree on a broad agreement can instead agree to shallow rules to create an institution with authority to promulgate rules. In effect, it reduces the transaction costs for reaching a consensus. This paper also analyses the feasibility and merit of the ASEAN Cybercrime Court from three aspects: jurisdiction, independent prosecutor office and legal interpretation. Although the solution is not a perfect answer to legal harmonisation, it serves as a starting point in a progress path ultimately leading to the conclusion of a binding multilateral treaty.

Keywords: International Law, ASEAN, Legal Harmonisation, Cybercrime, Cybercrime Court, International Common Law, International Soft Law, ASEAN Cybercrime Court

[1] LL.M. (UChicago), J.D./M.S.Sc. (CUHK), MSc. (LSE), B.Sc. (QMUL); Email: kwanyueniu@gmail.com

[2] J.D. (CUHK), M.A. (HKU), B.A. (EdUHK); Email: vanessa.my.wong@gmail.com

Introduction

> "The effects of cybercrime can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response."
>
> -- United Nations Office of Drugs and Crime[3]

Given the rapid growth of digital economies in ASEAN, ASEAN member states have become prime targets for cyberattacks.[4] With the huge impact of the Covid-19 pandemic on technology-facilitated human trafficking, there is a pressing need for the ASEAN countries to harmonise the law in order to regulate cybercrimes to safeguard the development of E-Commerce, Electronic Data Interchange, and, most importantly, to rectify the paucity of the reliable internet system. Nonetheless, the progress of legal harmonisation in cybercrimes is slow and stagnant within the ASEAN countries, and the ASEAN countries are yet to articulate a satisfactory regional framework for Cybercrime regulation.

Despite the prevalence of cybercrime in ASEAN and the transnational nature of cybercrime, there is limited related literature to offer solutions for legal harmonisation. This paper aims to analyse the possibility of establishing a trans-national cybercrime court in ASEAN ("ASEAN Cybercrime Court") with jurisdiction to hear cybercrime cases to get around the state consent requirement for creating international obligations.

In this paper, the theoretical framework is based on the concept of international common law articulated by Andrew Guzman and Timothy Meyer, in which certain members who were unable to reach a consensus on a broad agreement can instead agree to shallow rules to create an institution with authority to promulgate rules. Further, the ASEAN Cybercrime Court should have its leading advantages in responding to the technological evolution via judicial interpretation without pending the states to update the convention.

This paper is divided into four parts. Part I of this paper will explain the prevalence of cybercrimes in ASEAN. Part II will analyse the challenge of the harmonisation of cybercrime

---

[3] United Nations Office on Drugs and Crime (UNODC), 'Darknet Cybercrime Threats to Southeast Asia 2020' (2021) <https://www.unodc.org/documents/southeastasiaandpacific/darknet/index.html> accessed 1 October 2022, 5.

[4] Interpol, 'ASEAN Cyberthreat Assessment 2021' (22 January 2021) <https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia> accessed 18 September 2022 (hereinafter "**Interpol's Report**") 13.

regulations. Part III will discuss why the Budapest Convention is not a workable solution for ASEAN. We further advocate the establishment of the ASEAN Cybercrime Court as an effective solution to stimulate legal harmonisation in Part IV.

I. Cybercrime in ASEAN

The 2020 Global Digital Report showed that Southeast Asia had witnessed rapid growth in internet penetration over the past few years with an average internet penetration rate of 66% in 2020.[5] The growth did not decelerate post-2020 as the Covid-19 pandemic became a catalyst in accelerating digitisation.[6] The work-from-home measures have facilitated the traffic and frequency of online transactions.[7]

Unfortunately, cybercriminals are also exploiting the opportunity to their advantage.[8] In particular, the ASEAN member states reported significant use of COVID-19 themes for phishing and online fraud. In Malaysia, the reported cases of cyber fraud increased from 4,691 cases in the first eight months of 2019 to 5,697 cases for the same period in 2020.[9]

Another raising concern is the intersection between cybercrime and human trafficking. For example, the news revealed that foreign nationals are being trafficked to Cambodia through online scams, and some of them are subject to torture or even death.[10] The victims came from various countries in Asia such as Malaysia and Taiwan.[11] The transnational and intersectional natures of cybercrime complicate the cybercrime regulatory framework.

---

[5] Simon Kemp, 'Digital 2020: Global Digital Overview' (*DataReportal*, 30 January 2020) <https://datareportal.com/reports/digital-2020-global-digital-overview> accessed 27 September 2022; Interpol's Report (n 4) 8.
[6] ibid.
[7] ibid 25.
[8] ibid 12.
[9] ibid 25.
[10] Enno Hinz, 'Cambodia: Human trafficking crisis driven by cyberscams' (*Deutsche Welle*, 12 September 2022) <https://www.dw.com/en/cambodia-human-trafficking-crisis-driven-by-cyberscams/a-63092938> accessed 29 September 2022.
[11] The Associated Press, '24 more Malaysians rescued from Cambodia human traffickers' (*ABC News*, 9 September 2022) <https://abcnews.go.com/International/wireStory/24-malaysians-rescued-cambodia-human-traffickers-89589335> accessed 29 September 2022.

II. Cybercrime and Harmonisation: Three challenges of Cybercrime Regulation

Prevention, regulation, and punishment of transactional cybercrimes require co-operation among governments and law enforcement agencies. Similar to the dispute resolution settlement mechanism developed by the ASEAN,[12] the co-operation mechanisms among the ASEAN countries will need to be further strengthened in order to increase regional capacity in law enforcement and sanctions.

Regrettably, legal harmonisation is challenging in the context of cybercrime regulation. Three main challenges have been identified as follows: (i) lack of a territorial jurisdictional boundary; (ii) inadequacies of uniform cybercrime regulatory frameworks; and (iii) rapid evolution of cybercrime.

2.1 Lack of a Territorial Jurisdictional Boundary

First, cyberspace is an extraterritorial space,[13] and cybercriminals are no longer confined to the broad and general meaning of individual hackers. Before and with the start of the Covid-19 pandemic, there have been national organised criminal groups with infrastructures operating on a global scale.[14] For traditional cybercrimes such as financial fraud or domestic cyber-attacks, the domestic criminal legislations are generally sufficient for regulation as the cybercriminals are within the reach of State's police power.[15] However, since cybercriminals often operate in judication other than domestic ones, the judiciary and police forces need to acquire evidence in other jurisdictions.[16] This can be seen as an albatross which could take such a long time to proceed with the case. In particular, certain electronic data such as "cloud storage" is often transnational in nature. It may not be connected to the state where the crime has been committed.[17]

[12] ASEAN, 'ASEAN Protocol on Enhanced Dispute Settlement Mechanism' (2012) <https://asean.org/asean-protocol-on-enhanced-dispute-settlement-mechanism/> accessed 30 September 2022.
[13] Nicohlas W. Cade, 'An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code' (2012) 37(3) Brooklyn J Int'l L 1139, 1147-1148.
[14] Filippo Spiezia, 'International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) 23(1) ERA Forum 101, 102.
[15] Alexandra Perloff-Giles, 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 Yale J Int'l L 191, 204.
[16] Spiezia (n 14) 103.
[17] ibid.

If some specific conducts of cybercrime are only criminalised in some member states of ASEAN but not others, the "legal black hole" will then exist in the relevant states that failed to criminalise cybercrime without any relevant legislation. In the absence of dual criminality, evidence gathering and extradition are almost impossible.[18] This will be a serious impediment to combating transactional cybercrime. As such, legal harmonisation is vital for effective prosecution and law enforcement among the ASEAN member states.

2.2 Inadequacies of Uniform Cybercrime Regulatory Frameworks

Without doubt, the cybercrime issue has been addressed since 2013 or earlier as reflected in the ASEAN Documents Series on Transnational Crime.[19] Common regional collaborative activities such as the ASEAN Computer Emergency Response Teams ("**CERTS**") have also been developed.[20] Yet, the framework is yet to be "solid", "stable" and "clear".[21] To briefly illustrate, the ASEAN Declaration to Prevent and Combat Cybercrime states:--

> '1. ACKNOWLEDGE the importance of harmonisation of laws related to cybercrime and electronic evidence;
> 2. ENCOURAGE ASEAN Member States to explore the feasibility of acceding to existing regional and international instruments in combating cybercrime;
> 3. ENCOURAGE the development of national plans of actions in addressing cybercrimes;'[22]

Despite the importance of ASEAN in having consensus for combating cybercrime is showcased, the development lacks legal clarity for enforcement. At this moment, only serious situation arrives at a certain level raising deep concerns over security. As it has dealt with human trafficking, the ASEAN member states have established a consolidated framework to cooperate and agree on legally binding instruments. For instance, the 2015 ASEAN Convention

---

[18] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2nd International Serious and Organised Crime Conference, Brisbane, July 2013) 698, 701.
[19] ASEAN, *ASEAN Documents Series on Transnational Crime: Terrorism and Violent Extremism; Drugs; Cybercrime; and Trafficking in Persons* (Jakarta: ASEAN Secretariat 2017).
[20] Hitoshi Nasu and others, *The Legal Authority of ASEAN as a Security Institution* (CUP 2019) 143.
[21] Iqbal Ramadhan, 'ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia' (the 1st International Conference on Contemporary Risk Studies, Jakarta, March-April 2022) 2.
[22] ASEAN Declaration to Prevent and Combat Cybercrime (adopted 13 November 2017).

Against Trafficking in Person, Especially Women and Children.[23] Indeed, cybercrime regulation requires solid coordination but not "situations in which states wish to work together and simply need to agree on how to do so".[24] There shall be a practical framework with the establishment of a uniform regulation to incriminate.

2.3 Rapid Evolution of Cybercrime

Laws can never keep the same pace with technology. Nicholas Cade opined that the legislative efforts to fight cybercrime have been largely inefficient as the legislation is outpaced by dynamic criminal tactics and the mutation of cyberspace.[25] For example, the emergence of crypto-currencies complicates the prevention of fraudulent transactions.[26]

As aforementioned, a further difficulty is the intersections between cybercrimes and other substantial areas of law such as human trafficking. Apart from cyber grooming, human traffickers have kept pace with the development of technology by using social media to attract and recruit victims for false job opportunities[27] or pseudo romance.

It remains to be seen, however, the ASEAN member states are still expanding the meaning of the term 'precaution' rather than 'combating'. This leads to the question: How to design a harmonised regulatory framework to tackle the rapid evolution of cybercrime? It is questionable whether the "ASEAN way" of the decision-making process can promptly respond to the dynamic nature of cybercrimes as the consensus decision-making mechanism is slow.[28]

III. Budapest Convention and ASEAN

[23] ASEAN Convention Against Trafficking in Person, Especially Women and Children (adopted 23 November 2015)
[24] Andrew T. Guzman, 'Against Consent' (2012) 52 Virginal J Int'l L 747, 764.
[25] Cade (n 13) 1139.
[26] Europol and Eurojust Public Information, 'Common challenges in combating cybercrime' (2019) <https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf> accessed 10 September 2022, 12.
[27] ASEAN-Australia Counter Trafficking, 'The use and abuse of technology in human trafficking in Southeast Asia' (30 July 2022) <https://www.aseanact.org/story/use-and-abuse-of-technology-in-human-trafficking-southeast-asia/> accessed 1 October 2022.
[28] Ralf Emmers, 'ASEAN minus X: Should This Formula Be Extended?' (2017) RSIS Commentary Nanyang Technology University <https://hdl.handle.net/10356/86219> accessed 10 October 2022.

One may wonder why Budapest has not been adopted for combatting cybercrimes by ASEAN member states. As argued by Jonathan Clough, cybercrime is distinctive from others because of "the inherently transnational nature of the underlying technology".[29]An international legal regime for the protection of our cyberspace, of course, is ideal. Before turning to the proposal of the trans-national cyber court, consideration must be given to the current legal co-operation. The Convention on Cybercrime of the Council of Europe, the Budapest Convention, is the first international convention on cybercrime which came into effect in 2004.[30]

The Preamble of the Budapest Convention explicitly states that

> "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.
> …
> Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation"[31]

The core objective of the Budapest Convention enshrined in the Preamble is to "by facilitating their detection, investigation and prosecution at both the domestic and international levels". In other words, it harmonises nations by providing a guideline to develop their domestic legislations on cybercrime, and also offers a legal framework for "fast and reliable international co-operation".[32] By June 2022, 66 states, including both member states and non-member states of the Council of Europe were parties to the Budapest Convention.[33] However, only one

[29] Clough (n 18) 700.
[30] The Budapest Convention on Cybercrime (signed 23 November 2001) TIAS 131, ETS 185.
[31] ibid Preamble.
[32] Council of Europe Cybercrime Division DGI, 'Joining the Convention on Cybercrime: Benefits' (16 June 2022) <https://rm.coe.int/cyber-buda-benefits-june2022-en-final/1680a6f93b> accessed 9 September 2022.
[33] ibid.

ASEAN Member State – Philippines has ratified the Budapest Convention. Given the global fragmentation, it is unrealistic to expect the majority of ASEAN member states, or a global consensus will join the Budapest Convention in a short term.[34]

Having said that, it remains questionable in reality whether the Budapest Convention is an appropriate legal solution for tackling cybercrime in ASEAN. Even though the Philippines have already ratified the Budapest Convention, it is unlikely that the other ASEAN countries will follow this path or fastidiously level the regulation due to the issue of state sovereignty.

3.1 Why cannot the Budapest Convention facilitate the legal harmonisation in ASEAN? Challenges of Budapest Convention in ASEAN

3.1.1 A Coordination Dilemma

The ultimate goal of ASEAN is to create a security community which rests upon preserving regional autonomy against foreign intervention.[35] With this aim in mind, the problem with legal harmonisation under the Budapest Convention is all ASEAN member states did not participate in the preparation and negotiation of the Budapest Convention.[36] The chief executive officer of Cybersecurity Malaysia suggested that the domestic legislations in different states remain significant, and it is important that the multilateral treaties shall not be in conflict with national interests and sovereignty.[37] The failure to involve all the parties in the negotiation process results in an uncertainty of a regional autonomy and distributional effect. The state is uncertain as to whether the benefits of participating in the Budapest Convention will outweigh the cost.[38] For example, Russia perceived that national security and sovereignty could be at risk given that paragraph 32 of the Budapest Convention allows trans-border access to stored computer data

[34] Eugenio Benincasa, 'The role of regional organizations in building cyber resilience: ASEAN and the EU' Pacific Forum Issues & Insights Vol. 20, WP 3 6/2020, 1 <https://pacforum.org/wp-content/uploads/2020/06/issuesinsights_Vol20WP3-1.pdf> accessed 9 September 2022.
[35] Hanan Mohamed Ali, '"Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance' (2021) 4(1) The Journal of Intelligence, Conflict, and Warfare 123, 127.
[36] Gabey Goh, 'Cybercrime: Malaysia not lagging but needs to level up' (*Digital News Asia*, 24 September 2014) <https://www.digitalnewsasia.com/security/cybercrime-malaysia-not-lagging-but-needs-to-level-up> accessed 11 September 2022.
[37] ibid.
[38] Guzman (n 24) 756-757.

during cybercrime investigations by the special services of various nations.[39] As a result, in the past decade, Russia had been proposed another convention to counter cybercrime.[40] Russia further submitted a letter to the United Nations advocating a new international convention on cybercrime.[41]

According to Coase Theorem, the transaction costs of reaching an agreement are simply too high given the high number of participants in the Budapest Convention.[42] Indeed, it is infeasible to impose standardised legal measures and mechanisms in every jurisdiction because states have different cultures, values, priorities and organisational structures, which will result in divergent legislations.[43] As such, it is legally complicated to agree on any multilateral treaties on a global scale.[44]

This is a typical problem of prisoner's dilemma. Professor Marco Gercke argued that the Budapest Convention failed to play an important role outside Europe because

> "[t]he list of reasons why the Convention did not succeed at global level is complex. It starts with a missing involvement of developing countries in the drafting process, a more demanding accession procedure compared to UN Conventions, a lack of updates in response to trends, the absence of regulations for electronic evidence and liability of Internet Service Provider (ISP), missing field offices outside Europe and maybe most importantly a lack of supporting capacity building that is especially relevant for developing countries."[45]

[39] Russia & FSU, 'Russia prepares new UN anti-cybercrime convention-report' (*RT*, 14 April 2017) <https://www.rt.com/russia/384728-russia-has-prepared-new-international/> accessed 5 October 2022.
[40] ibid.
[41] UNGA 'Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General' (16 October 2017) UN Doc (A/C.3/72/12)
[42] Guzman (n 24) 759.
[43] Benincasa (n 34) 1.
[44] Goh (n 36)
[45] Marco Gercke, '10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-related Crimes' (2011) 12(5) Computer Law Review International 142; Stein Schjolberg, 'The History of Cybercrime' (2020) 13 Schriftenreihe des Cybercrime Research Institute 96.

In fact, many large States, such as Russia, India, and China, have refused to join the Budapest Convention. As long as one member state in ASEAN is reluctant to become a party to the Budapest Convention, the member state will become a safe haven for cybercriminals.[46]

3.1.2 Evolution of Cybercrimes

The Budapest Convention does not create extraterritorial legislation but only requires the signatories to enact domestic law.[47] The reliance on domestic legislation undermines the process of legal harmonisation because there are no enforceable standards for criminal statutes among the signatories.[48]

Logically, even if all ASEAN member states enact the domestic cybercrime legislation in accordance with the guideline of the Budapest Convention, it is foreseeable that the legal harmonisation will fail in the long run due to the dynamic nature of the cybercrime.

It is practically infeasible to obtain the consensus of all the member countries in the Budapest Convention to agree on the amendment to tackle a mutated form of cybercrime in a short period of time. Thus, the only possible solution for cybercrime enforcement would be to stretch the existing provisions by the form of legal interpretation. However, legal interpretation of certain provisions would not be harmonised across different jurisdictions due to legal practices and systems differences. This becomes a major obstacle to cybercrime prevention.

3.1.3 Lack of Enforcement Mechanism

Similarly, the lack of enforcement mechanisms is another issue of the Budapest Convention. Andrew Guzman and Timothy Meyer argued the assumption that the parties in an international agreement would honour their commitment under the threat of coercive enforcement is incorrect.[49] The enforcement measures in international law are not sufficient to secure efficient

[46] Cade (n 13) 1155.
[47] ibid 1154.
[48] Cade (n 13) 1155.
[49] Andrew T. Guzman & Timothy L. Meyer, 'International Soft Law' (2010) 2(1) Journal of Legal Analysis 171, 182.

levels of compliance.[50] Under the Budapest Convention, there is an absence of retaliation and sanction against the party who fails to comply with the agreement.

In addition, the harmonisation of the laws in ASEAN *per se* would be futile without the member states' effective application. Without the judiciary exercising the interpretative and contentions competence, the legislation of a country is merely a legal framework.

IV. The ASEAN Cybercrime Court and International Common Law in ASEAN

Given that Budapest Convention may not be a feasible solution for ASEAN, ASEAN will need to find an alternative solution to tackle cross-border cybercrime. The scholarship of Jonathan Clough shows that despite each ASEAN member state did show certain national efforts in combating cybercrime, the greatest danger is the fragmentation of effort.[51] The development of a harmonised legal regime for cybercrime is complicated because it is not purely a legal matter. It involves a question of national policy and interest.[52] In particular, this is a question of proportionality in balancing the interests of legal enforcement and precision.

The reality is that it is infeasible for all ASEAN member states to develop a detailed convention promptly to tackle the prevalence of cybercrime, especially when the cybercrime regulation needs to be specific and clear enough in order to create a criminal regime.[53] In this section, it is submitted that the establishment of the ASEAN Cybercrime Court can be a practically innovative approach to achieving legal harmonisation.

4.1 Theoretical basis: International Common Law

Andrew Guzman and Timothy Meyer introduced the concept of international common law ("**ICL**") as a form of soft law. They defined the ICL as "a nonbinding gloss that international institutions, such as international court, put on binding legal rules".[54] They argued that the

[50] ibid.
[51] Clough (n 18) 700.
[52] Andrew T. Guzman & Timothy L. Meyer, 'Explaining Soft Law' (Latin American and Caribbean Law and Economics Association (ALACDE) Annual Papers, UC Berkeley, 2010)
[53] Judge Stein Schjolberg, 'Peace and Justice in Cyberspace: Potential new global legal mechanisms against global cyberattacks and other global cybercrimes' (EWI Worldwide Cybersecurity Summit Special Interest Seminar, New Delhi, October 2012) 6.
[54] Guzman & Meyer (n 49) 171.

cooperation-minded states could establish an international court with the authority to create international common law to get around the state consent requirement for establishing international obligations.[55]

It is no doubt that ASEAN member states are cooperation-minded states, which can be ascertained from the key provisions in the ASEAN declaration. That said, the first three aims and purposes of ASEAN are:--

> "(1) To accelerate economic growth, social progress and cultural development in the region.
> (2) To promote regional peace and stability through abiding respect for justice and the rule of law in the relationship among countries in the region and adherence to the principles of the United Nations Charter.
> (3) To promote active collaboration and mutual assistance on matters of common interest in the economic, social, cultural, technical, scientific and administrative fields."[56]

The cultural connections and the ASEAN declaration have made it achievable for the ASEAN member states to agree on certain vague rules on cybercrimes under the ICL framework.[57] The beauty of ICL is manifold.

First, it is recognised that even the cooperation-minded states, like the ASEAN member states are difficult to reach unanimous consent on broad and detailed rules on a legal problem.[58] Reaching consensus by searching for an auspice among the ASEAN member states do more harm than good. However, under the ICL framework, the cooperation-minded states only need to agree on shallow, vague or flexible rules to a certain degree in order to establish a tribunal with limited jurisdiction to hear disputes.[59] This will conceivably make it more attractive and acceptable to the ASEAN members states in reaching consensus for having a framework.

Second, although the judgment of the tribunal is non-binding to the states other than the parties before it, it shapes the expectation of all states bound by the underlying obligation.[60] The ICL,

[55] ibid 178.
[56] The ASEAN Declaration (Bangkok Declaration) (signed 8 August 1967).
[57] Guzman (n 24) 761-762.
[58] Guzman & Meyer (n 49) 202.
[59] ibid.
[60] ibid 178.

as a form of soft law, may be evidence of existing law, formative of the *opinio juris* or a new form of customary law.[61] For example, Guzman and Meyer observed that the *Nicaragua v United States of America*[62] had an extensive effect on shaping the expectations of what constitutes compliant behaviour, such as the understanding of the law of self-defence.[63] Another notable example is the United Nations Human Rights Council ("**UNHRC**"). The view delivered by UNHRC is non-binding, but the States would often take the view in considering the underlying obligations.[64]

As such, Guzman and Meyer concluded that

> "[e]stablishing a tribunal with limited jurisdiction to hear disputes arising under a legal rule can thus be a strategy for cooperation-minded states to deepen co-operation even with those states that would not consent to deeper co-operation in a negotiation […] they also create a body of soft legal rules that constrain, to some extent, the behavior of states not party to the creation of the tribunal or IO [International Organization]."[65]

This will make it easier to acknowledge when they have a shared understanding. An example of such legal rule for cooperation-minded states is found in the E-ASEAN Framework Agreement. Even though the agreement was not in force, most member states enacted their domestic legislations to "create a regulatory space where existing national security concerns are projected".[66]

From this perspective, legal harmonisation can be achieved by legal approximation. Jonathan Clough recognised the difficulty of legal harmonisation for cybercrime regulation at both domestic and international levels, and he argued that "harmonisation" does not mean "identical". The key part of the framework is "complementarity" which enables enforcement

[61] Alan Boyle, 'Soft Law in International Law-Making' in Malcolm D. Evans (ed) *International Law* (OUP 2010) 118.
[62] *Nicaragua v United States of America* (Merits) ICJ Rep 1986.
[63] Guzman & Meyer (n 49) 202-203.
[64] ibid 211.
[65] ibid 178.
[66] Nasu (n 20) 151.

mechanisms to work effectively while respecting national and regional differences.[67] The approximately harmonised legal regime is sufficient to attract foreign investment.[68]

Third, soft law can also act as a starting point in a progress path ultimately leading to the conclusion of a binding multilateral treaty.[69] By nature, soft law is non-binding. This makes the member states easier to accept, example being the Universal Declaration of Human Rights. It was a non-binding instrument adopted by the United Nations General Assembly in 1948 and was intended by the Human Rights Commission that future binding agreements would be made based on that later.[70] The influence of it and soft law has therefore formed the basis for the more than 70 human rights instruments hereinafter.[71]

Likewise, an ICL institution can facilitate consensual co-operation among states as the ASEAN cybercrime court can provide a forum for capacity building which reduces the transaction costs for reaching consensus.[72] For example, the International Criminal Tribunal for the former Yugoslavia actively engaged in the capacity building via working visits, training seminars, workshops and other activities.[73] It is therefore anticipated that the ICL institution would facilitate the establishment of a detailed binding treaty for cybercrime regulations.

From a practical perspective, Judge Stein Schjolberg, an international expert on cybercrime, is a strong advocate for creating an International Criminal Tribunal for Cyberspace ("ICTC") to handle "the most serious cybercrimes of global concern".[74] He opined that the international criminal court lies in the promise of universal justice, and most serious cybercrimes would go unpunished without an international criminal court because of the multi-jurisdictional nature of cybercrime. ICTC will take action when national courts or prosecutors fail to act on the most serious global cybercrimes.[75]

---

[67] Clough (n 18) 701.
[68] Visoot Tuvayanond, 'The Role of the Rule of Law, the Legal Approximation and the National Judiciary in ASEAN Integration' (2001) 6(1) Thammasat Review 74, 82.
[69] Boyle (n 61) 123.
[70] ibid.
[71] Universal Declaration of Human Rights (adopted on 10 December 1948).
[72] Guzman (n 24) 781.
[73] International Criminal Tribunal for the former Yugoslavia, 'Overview of Capacity Building Activities' <https://www.icty.org/en/outreach/capacity-building/overview-activities> accessed 26 September 2022.
[74] Judge Stein Schjolberg, 'Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes' EWI Cybercrime Legal Working Group 3/2012, 17.
[75] ibid.

Again, the practicality of ICTC might raise similar concerns to the ASEAN member states given this may be compounded by a conflation of other questions such as the exercise of jurisdiction and the standard of failure to prosecute.

4.2 The ASEAN Cybercrime Court: The Feasibility and the Founding Treaty

4.2.1 Regional co-operation as the Starting Point

Closely linked to the above challenges, the initial issue faced by all ASEAN member states is the difficulty of agreeing on a broad and detailed convention. Instead, the member states can first agree to shallow or vague rules in extenso.

Generally speaking, neighbouring countries are likely to share greater common interests and similarities when they are more likely to have interconnected infrastructures and economics.[76] These commonalities make it easier to develop a common cybercrime regulatory framework.[77] The example of the Budapest Convention is a successful model of regional co-operation, albeit not a suitable model for global co-operation.

However, it will be difficult to transplant a similar convention in ASEAN because ASEAN has no strong unifying governance or legal frameworks like E.U.[78] and the potential problem of violating state sovereignty. The capacity for coordination would be relatively different under the ASEAN model. Given consensus has already accorded to the urgency of the issues, the Declaration to Prevent and Combat Cybercrime in 2017 proved that consensus has already accorded to the urgency of the issues.[79] The declaration encourages the ASEAN member states to explore the feasibility of acceding to the existing regional and international instruments in combating cybercrimes and it supports the common framework for capacity building. [80]As such, there is much plausibility for the ASEAN member states to set out a new regional code of cybercrime for a regional court in order to achieve legal harmonisation.

[76] Benincasa (n 34) 2.
[77] ibid.
[78] ibid.
[79] ASEAN Declaration to Prevent and Combat Cybercrime (n 22)
[80] ibid.

Further, it may also be possible for the majority of ASEAN member states to reach a consensus through the 'ASEAN minus X' voting formula, as recognised in the 2007 ASEAN Charter. 'ASEAN minus X' refers to that each country can adopt the agreement on its own based on its own consideration without having to extend concessions to nonparticipating members.[81] This formula is able to balance the interests of the member states by promoting efficiency to the majority states and enabling the minority states to catch up later. In other words, this framework allows a mode of flexible participation and speeds up legal harmonisation for cybercrime regulations.[82] Therefore, the 'ASEAN minus X' formula should be extended to assist the cybercrime regulatory regime.

Regional co-operation is the starting point with a core objective for the protection of society against cybercrime with "comprehensive security and collective responsibility",[83] and a legal authority for effectively combating such criminal offences. Subsequent conventions shall therefore be constructed upon the principle above. In view of the establishment of the ASEAN Cybercrime Court, three areas, namely jurisdiction, independent prosecutor office and legal interpretation shall be evaluated for the feasibility of the Court.

4.2.2 Jurisdiction

First and foremost, ASEAN member states can confer jurisdiction to the ASEAN Cybercrime Court to deal with transnational cybercrime within ASEAN. However, jurisdiction remains the most contentious and difficult part as it involves the assertion of sovereignty and "tends to inhere in States for the purpose of protecting their own interests".[84]

The application of jurisdiction on cybercrimes is inherently complicated because of the fact that cyberspace is another space and the cybercrimes conducted usually involved offenders located in more than one or multiple states. So, in which ways the jurisdiction may be asserted?

[81] Usanee Aimsiranun, 'Comparative Study on the Legal Framework on General Differentiated Integration Mechanisms in the European Union, APEC, and ASEAN' (2020) ADBI Working Paper 1107 (Tokyo: Asian Development Bank Institute) 5.
[82] Ramadhan (n 21).
[83] Nasu (n 20) 158.
[84] Robert Cryer and others, *An Introduction to International Criminal Law and Procedure* (2nd edn, CUP 2010) 51.

Before turning to the explanation of jurisdiction over cybercrimes, attention must be given to the doctrine of treaty-based jurisdiction and universal jurisdiction. The treaty-based jurisdiction refers to the situation "where States have agreed between themselves that they may exercise jurisdiction on each other's behalf".[85] For instance, the International Criminal Court was established with the adoption of the Rome Statute over a list of treaty crimes. Likewise, it is possible for the ASEAN member states to draft, amend and adopt a convention with the establishment of a trans-national Cybercrime Court, namely the ASEAN Cybercrime Court in ASEAN.

Despite the inadequacies of national efforts in resolving these situations, the ASEAN member states have indeed attempted to develop strategies for the harmonisation of laws: by ministerial meetings within ASEAN such as Kuala Lumpur Declaration Combating Transitional Crime, Kuala Lumpur[86] and ASEAN Declaration to Prevent and Combat Cybercrime, Manila, the Philippines; [87]and ministerial meetings within ASEAN member states plus other counties such as Memorandum of Understanding between ASEAN and the Government of the People's Republic of China on Cooperation in the Field of Non-Traditional Security Issues[88] and Joint Statement of the Fourth ASEAN Plus China Ministerial Meeting on Transnational Crime Consultation.[89] Hence, it is not impossible for the ASEAN member states to prepare, draft, and implement their own treaty fairly representing the objectives of ASEAN in combating transnational cybercrimes and other grave crimes facilitated by technology thereafter.

Regrettably, the main uncertainty that remains is whether the ASEAN member states are willing to relinquish some sovereign power for granting the jurisdictional power to the regional court.[90] Daniel Nserko once commented on the problem of the International Criminal Court was the lack of universal jurisdiction "to track down and try perpetrators of heinous crimes

[85] ibid 46.
[86] Kuala Lumpur Declaration Combating Transitional Crime, Kuala Lumpur, Malaysia (signed on 30 September 2015).
[87] ASEAN Declaration to Prevent and Combat Cybercrime (n 22).
[88] Memorandum of Understanding between ASEAN and the Government of the People's Republic of China on Cooperation in the Field of Non-Traditional Security Issues, Manila, Philippines (signed on 21 September 2017).
[89] Joint Statement of the Fourth ASEAN Plus China Ministerial Meeting on Transnational Crime Consultation (30 September 2015).
[90] Cade (n 13) 20.

irrespective of their nationality and the place where they committed the crimes" rendering the Court became "severe handicap" and "may not accede to the Statute".[91]

Universal jurisdiction, as its name suggests, is "one aspect of a complex framework governing the exercise of extraterritorial jurisdiction by national legal systems".[92] The ASEAN Cybercrime Court can therefore have its own cybercrime jurisdiction with provisions on universal jurisdiction. Article 49 of Geneva Convention I reads that: --

> "[…] Each High Contracting Party shall be under the obligation to search for persons alleged to have committed, or to have ordered to be committed, such grave breaches and shall bring such persons, regardless of their nationality, before its own. […]"[93]

Potentially more contentious is the "forum shopping"[94] problem might then arise. Whether the universal jurisdiction is an appropriate solution? Similar to pirates' indiscriminate acts of depredation, transnational cybercrimes threaten international trade in the sense that the cyber attacks can destroy commercial websites or international corporations' records.[95] Accordingly, Alexandra Perloff-Giles argues that cybercriminals can be considered as *hostis humani generis* in which cyberspace is like "high seas".[96]

Further, the modus operandi of cyber fraudsters has gone beyond the virtual space of social media to human trafficking in the physical world. The list of specific crimes in the founding treaty should be updated from time-to-time depending on the evolution of cyber sphere. The list may also include the most serious global concern offences such as human trafficking. In response, the subsequent revision must therefore consider the evolution of the cybercrime in interpretation.

4.2.3 Independent Prosecutor Office

[91] Daniel, T. Ntanda Nsereko, 'The International Criminal Court: Jurisdictional and Related Issues' (1999) 10 Criminal Law Forum 87, 120.
[92] A. Hays Butler, 'The Doctrine of Universal Jurisdiction: A Review of the Literature' (2000) 11(3) Criminal Law Forum 353, 354.
[93] Geneva Convention I (12 August 1949) art 49.
[94] George Fletcher, 'Against Universal Jurisdiction' (2003) 1 JICJ 580.
[95] Perloff-Giles (n 15) 224.
[96] ibid.

Secondly, the inadequate enforcement mechanisms on cybercrime in ASEAN would be detrimental if there are difficulties in gathering and exonerating evidence to prove the case. Given the increase of human trafficking through infiltrating existing social media, the effect of the cybercrime has gone beyond the cyber sphere, and this would be a serious impediment to combating trans-national cybercrime.

One may suggest that there are already some key platforms namely the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF-ISM on ICTs Security), the ASEAN Telecommunications and IT Minister's meeting (TELMIN), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN Network Security Council (ANSAC), and the Council for Security Cooperation in the Asia Pacific (CSCAP). However, they are more preventative in nature with working groups and forums for exchanging views. Even some views of the ASEAN member states are "diverging […] on some critical matters" that "had impeded the successful implementation".[97] The ASEAN communities have a strong will but insufficient plans to execute.

It is therefore suggested that an independent prosecutor's office should be set up for the purpose of investigation and prosecution.[98] Reference can be taken from the Office of the Prosecutor in the International Criminal Court, the responsibility of the Prosecutor is "examining situations under the jurisdiction of the Court" and "carrying out investigations and prosecutions against the individuals who are allegedly most responsible for those crimes"[99]. The provision-based and independent yet centralised nature of the Independent Prosecutor Office as part of the ASEAN Cybercrime Court will thus create a new landscape in ASEAN with a clearer direction. With reference to Articles 12 and 13 of the Rome Statute, the operation of the Independent Prosecutor Office can either begin through the requests made by any state party to the treaty of the AESAN Cybercrime Court or by an ad hoc basis within the acceptance of jurisdiction.

4.3 Legal Interpretation

[97] Benincasa (n 34) 9.
[98] Schjolberg (n 53) 20.
[99] International Criminal Court, 'Office of the Prosecutor' <https://www.icc-cpi.int/about/otp> accessed 1 October 2022.

Further, a successful legal harmonisation framework must consider the harmonisation of legal interpretation. The ICL institution can tackle the rapid evolution of cybercrimes.[100] As analysed above, the dynamic criminal tactics and the mutation of cyberspace outpace the existing regulatory regime, and hence undermine the effort of legal harmonisation. The ASEAN Cybercrime Court is able to solve this problem with the legal interpretation of the general rule. The ICL institution has the discretion to decide the individual cases based on the facts against the written general and vague rules.[101]

In this process, the ASEAN Cybercrime Court is able to transform the general rule into a specific rule just like the human rights tribunal.[102] In interpreting the law, the common law court won't merely examine the literal meaning of the law. For example, In *Regina v Secretary of State for Health ex parte Quintavalle* (on behalf of Pro-Life Alliance) (2003), the House of Lords expressly used a purposive approach to statutory interpretation in order to consider whether a new technology - cell nuclear replacement is within the ambit of the Human Fertilisation and Embryology Act 1990. Lord Bingham of Cornhill pointed out that

> "…If Parliament, however long ago, passed an Act applicable to dogs, it could not properly be interpreted to apply to cats; but it could properly be held to apply to animals which were not regarded as dogs when the Act was passed but are so regarded now. The meaning of "cruel and unusual punishments" has not changed over the years since 1689, but many punishments which were not then thought to fall within that category would now be held to do so. The courts have frequently had to grapple with the question whether a modern invention or activity falls within old statutory language: see Bennion, *Statutory Interpretation*, 4th ed (2002) Part XVIII, Section 288. A revealing example is found in *Grant v Southwestern and County Properties Ltd* [1975] Ch 185, where Walton J had to decide whether a tape recording fell within the expression "document" in the Rules of the Supreme Court. Pointing out (page 190) that the furnishing of information had been treated as one of the main functions of a document, the judge concluded that the tape recording was a document"

[100] Guzman & Meyer (n 49) 204.
[101] ibid.
[102] ibid.

Following this line of argument, by vesting the jurisdiction over the most serious cybercrime to a single regional institution, the legal interpretation of the cybercrime regulation can be updated and harmonised among the ASEAN member states.[103]

As aforementioned, the evolution of the modus operandi in cybercrimes has operated beyond the cyber sphere. The ASEAN Cybercrime Court can vest with discretion to include other binding instruments of crimes now facilitated by social media such as the 2007 ASEAN Convention on Counter Terrorism and the 2015 ASEAN Convention Against Trafficking in Persons, Especially Women and Children.

In addition, a potential problem is the issue of travaux préparatoires among the ASEAN member states. Given the distinctive features of every language and legal system, instead of focusing on linguistic differences, it is possible to document the consultation and draft material for the future to ensure that ambiguities are resolved peacefully.

[103] Cade (n 13) 1170.

V. Conclusion

This paper put forward an innovative yet practical solution in combating cybercrime in ASEAN. It has been observed that there is an urgent need to establish a harmonised criminal regime for cybercrime in ASEAN. Regrettably, current cyberspace regulation seems to be an ambitious goal with only a strong will without sufficient implementation of law enforcement in remedying the situation. As such, the ASEAN Cybercrime Court is a necessary step for ASEAN to tackle the dynamic nature of cybercrime.

Through the ICL, ASEAN can mobilise a consistent response to complicated transnational cybercrimes. The ICL may not be able to solve the problem in one go. Nevertheless, it is at least the first step toward a more comprehensive multilateral treaty.[104] Even if certain ASEAN member states only agree to the shallow jurisdictional commitment, the soft law under ICL framework will affect all parties to the underlying treaty.[105] Subsequently, similar to what it has done in dealing with human trafficking, ASEAN will have a uniform regulatory framework in advancing "the feasibility of acceding to existing regional and international instruments in combating cybercrime".

In addition, the establishment of the ASEAN Cybercrime Court would also lead to tremendous alterations to cyberspace that it acts as a platform to gather technological experts such as digital forensics, to assist the court in understanding the development and analysis of emerging new technologies. It will be proportionate for the court to identify and resolve the legal issues and to avoid future astounding misuse of technologies.

Nothing can ever be a perfect solution, but at least it is a starting point for capacity building. The ASEAN community shall act in response to the urgent and increasing cyber threats moving beyond the cyber sphere.

[104] Boyle (n 61) 118.
[105] Guzman & Meyer (n 49) 205.

Bibliography

Books

Alan Boyle, 'Soft Law in International Law-Making' in Malcolm D. Evans (ed) *International Law* (OUP 2010).

Hitoshi Nasu and others, *The Legal Authority of ASEAN as a Security Institution* (CUP 2019).

Robert Cryer and others, *An Introduction to International Criminal Law and Procedure* (2nd edn, CUP 2010).

Journal Articles

A. Hays Butler, 'The Doctrine of Universal Jurisdiction: A Review of the Literature' (2000) 11(3) Criminal Law Forum 353.

Alexandra Perloff-Giles, 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 Yale J Int'l L 191.

Andrew T. Guzman, 'Against Consent' (2012) 52 Virginal J Int'l L 747.

Andrew T. Guzman & Timothy L. Meyer, 'International Soft Law' (2010) 2(1) Journal of Legal Analysis 171.

Daniel, T. Ntanda Nsereko, 'The International Criminal Court: Jurisdictional and Related Issues' (1999) 10 Criminal Law Forum 87.

Filippo Spiezia, 'International co-operation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime' (2022) 23(1) ERA Forum 101.

George Fletcher, 'Against Universal Jurisdiction' (2003) 1 JICJ 580.

Hanan Mohamed Ali, '"Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance' (2021) 4(1) The Journal of Intelligence, Conflict, and Warfare 123.

Marco Gercke, '10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-related Crimes' (2011) 12(5) Computer Law Review International 142.

Judge Stein Schjolberg, 'Peace and Justice in Cyberspace: Potential new global legal mechanisms against global cyberattacks and other global cybercrimes' (EWI Worldwide Cybersecurity Summit Special Interest Seminar, New Delhi, October 2012).

Nicohlas W. Cade, 'An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code' (2012) 37(3) Brooklyn J Int'l L 1139.

Stein Schjolberg, ‘The History of Cybercrime’ (2020) 13 Schriftenreihe des Cybercrime Research Institute 96.

Visoot Tuvayanond, ‘The Role of the Rule of Law, the Legal Approximation and the National Judiciary in ASEAN Integration’ (2001) 6(1) Thammasat Review 74.

Conference and Working Papers
Andrew T. Guzman & Timothy L. Meyer, ‘Explaining Soft Law’ (Latin American and Caribbean Law and Economics Association (ALACDE) Annual Papers, UC Berkeley, 2010).

Eugenio Benincasa, ‘The role of regional organisations in building cyber resilience: ASEAN and the EU’ Pacific Forum Issues & Insights Vol. 20, WP 3 6/2020, 1 <https://pacforum.org/wp-content/uploads/2020/06/issuesinsights_Vol20WP3-1.pdf> accessed 9 September 2022.

Jonathan Clough, ‘A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation’ (2nd International Serious and Organised Crime Conference, Brisbane, July 2013).

Judge Stein Schjolberg, ‘Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes’ EWI Cybercrime Legal Working Group 3/2012.

Iqbal Ramadhan, ‘ASEAN Consensus and Forming Cybersecurity Regulation in Southeast Asia’ (the 1st International Conference on Contemporary Risk Studies, Jakarta, March-April 2022).

Ralf Emmers, ‘ASEAN minus X: Should This Formula Be Extended?’ (2017) RSIS Commentary Nanyang Technology University <https://hdl.handle.net/10356/86219> accessed 10 October 2022.

Usanee Aimsiranun, ‘Comparative Study on the Legal Framework on General Differentiated Integration Mechanisms in the European Union, APEC, and ASEAN’ (2020) ADBI Working Paper 1107 (Tokyo: Asian Development Bank Institute).

Cases

Nicaragua v United States of America (Merits) ICJ Rep 1986.

Treaties, UN General Assembly Resolutions and Declaration

ASEAN Convention Against Trafficking in Person, Especially Women and Children (adopted 23 November 2015).

ASEAN Declaration to Prevent and Combat Cybercrime (adopted 13 November 2017).

ASEAN, ‘ASEAN Protocol on Enhanced Dispute Settlement Mechanism’ (2012) <https://asean.org/asean-protocol-on-enhanced-dispute-settlement-mechanism/> accessed 30 September 2022.

ASEAN, *ASEAN Documents Series on Transnational Crime: Terrorism and Violent Extremism; Drugs; Cybercrime; and Trafficking in Persons* (Jakarta: ASEAN Secretariat 2017).

Geneva Convention I (12 August 1949) art 49.

Joint Statement of the Fourth ASEAN Plus China Ministerial Meeting on Transnational Crime Consultation (30 September 2015).

Kuala Lumpur Declaration Combating Transitional Crime, Kuala Lumpur, Malaysia (signed on 30 September 2015).

Memorandum of Understanding between ASEAN and the Government of the People's Republic of China on Cooperation in the Field of Non-Traditional Security Issues, Manila, Philippines (signed on 21 September 2017).

The ASEAN Declaration (Bangkok Declaration) (signed 8 August 1967).

The Budapest Convention on Cybercrime (signed 23 November 2001) TIAS 131, ETS 185.

UNGA 'Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General' (16 October 2017) UN Doc (A/C.3/72/12).

Universal Declaration of Human Rights (adopted on 10 December 1948).

Other Sources

ASEAN-Australia Counter Trafficking, 'The use and abuse of technology in human trafficking in Southeast Asia' (30 July 2022) <https://www.aseanact.org/story/use-and-abuse-of-technology-in-human-trafficking-southeast-asia/> accessed 1 October 2022.

Council of Europe Cybercrime Division DGI, 'Joining the Convention on Cybercrime: Benefits' (16 June 2022) <https://rm.coe.int/cyber-buda-benefits-june2022-en-final/1680a6f93b> accessed 9 September 2022.

Enno Hinz, 'Cambodia: Human trafficking crisis driven by cyberscams' (*Deutsche Welle*, 12 September 2022) <https://www.dw.com/en/cambodia-human-trafficking-crisis-driven-by-cyberscams/a-63092938> accessed 29 September 2022.

Europol and Eurojust Public Information, 'Common challenges in combating cybercrime' (2019) <https://www.europol.europa.eu/cms/sites/default/files/documents/common_challenges_in_combating_cybercrime_2018.pdf> accessed 10 September 2022.

Gabey Goh, 'Cybercrime: Malaysia not lagging but needs to level up' (*Digital News Asia*, 24 September 2014) <https://www.digitalnewsasia.com/security/cybercrime-malaysia-not-lagging-but-needs-to-level-up> accessed 11 September 2022.

International Criminal Court, 'Office of the Prosecutor' <https://www.icc-cpi.int/about/otp> accessed 1 October 2022.

International Criminal Tribunal for the former Yugoslavia, 'Overview of Capacity Building Activities' <https://www.icty.org/en/outreach/capacity-building/overview-activities> accessed 26 September 2022.

Interpol, 'ASEAN Cyberthreat Assessment 2021' (22 January 2021) <https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-charts-top-cyberthreats-in-Southeast-Asia> accessed 18 September 2022.

Russia & FSU, 'Russia prepares new UN anti-cybercrime convention-report' (*RT*, 14 April 2017) <https://www.rt.com/russia/384728-russia-has-prepared-new-international/> accessed 5 October 2022.

Simon Kemp, 'Digital 2020: Global Digital Overview' (*DataReportal*, 30 January 2020) <https://datareportal.com/reports/digital-2020-global-digital-overview> accessed 27 September 2022

The Associated Press, '24 more Malaysians rescued from Cambodia human traffickers' (*ABC News*, 9 September 2022) <https://abcnews.go.com/International/wireStory/24-malaysians-rescued-cambodia-human-traffickers-89589335> accessed 29 September 2022.

United Nations Office on Drugs and Crime (UNODC), 'Darknet Cybercrime Threats to Southeast Asia 2020' (2021) <https://www.unodc.org/documents/southeastasiaandpacific/darknet/index.html> accessed 1 October 2022.