


ORIGINAL ARTICLE

INTERNATIONAL LAW AND PRACTICE

Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers?

Xin Wang 

School of Law, Guangdong University of Foreign Studies, Guangzhou, China
Email: vivianwang_336@hotmail.com

Abstract

This article studies how ‘cybercrime’ is framed under the pre-existing regional prohibition regimes and how it would be reshaped under the auspices of the UN. This article adopts a sociolegal approach by integrating transnational criminal law (TCL) and the conceptual framework of recursivity. Observations and analyses show that (i) only the *Budapest Convention* has institutional capacity to shape ‘cybercrime’, while state behaviour of framing ‘cybercrime’ is actually subject to human rights instruments; (ii) states reach an exceptional compromise in transforming ‘cybercrime’ at the global level during the negotiations under the UN; and (iii) protection from cybercrime is emerging as a common interest. This author proposes that the normative changes of framing ‘cybercrime’ reflect the competition of states for normative power on the international plane; therefore, a pursuit of a universalist formula for countering cybercrime would not succeed owing to a lack of a global commitment to what basic norms and rules govern state behaviour in cyberspace. Lastly, this author proposes that transnational criminalization of cybercrime should seek a minimum public order at the first place because it is premature to provide any real global regulation at this moment.

Keywords: cybercrime; common interest; competing normative power; minimum public order; transnational criminalization

1. Introduction

Cybercrime has become a global concern due to its transnational character and evolving nature.¹ According to the 2024 *Cyberthreat Defense Report* issued by CyberEdge Group, cybercrimes such as data breach, identity theft, and others not only plague 72 per cent of organizations around the world, but also afflict almost everyone accessible to Internet services.² In response, 156 countries (80 per cent) have enacted cybercrime legislation at the domestic level,³ and 128 states (65.64 per

¹W. Capeller, ‘Not Such a Neat Net: Some Comments on Virtual Criminality’, (2001) 10(2) *Social & Legal Studies* 229, at 239; P. Arnell and B. Faturoti, ‘The Prosecution of Cybercrime – Why Transnational and Extraterritorial Jurisdiction should be Resisted’, (2023) 37(1) *International Review of Law, Computers & Technology* 29, at 29. This article does not distinguish ‘cybercrime’ from ‘Internet crime’ and other terms describing illegal activities in the digital environment.

²2024 Cyberthreat Defense Report, available at cyberedgegroup.com/wp-content/uploads/2024/05/CyberEdge-2024-CDR-Report-v1.0.pdf, at 10, 19.

³Six countries (5%), namely Congo, Georgia, Iraq, Yemen, Myanmar, and Cambodia are proposing draft legislation. Seventeen countries (13%), namely Suriname, Guyana, Bolivia, Guinea Bissau, Liberia, Namibia, Gabon, Equatorial Guinea, Democratic Republic of Congo, Central African Republic, Chad, Libya, Belgium, Belarus, Syria, Somalia, and Eritrea have neither legislation nor proposed draft legislation. See unctad.org/page/cybercrime-legislation-worldwide.

cent) have acceded to eight treaties on cybercrime under six regional organizations since 2001.⁴ These efforts have facilitated international co-operation of countering cybercrime by ‘rules and procedures that . . . guide, steer, and constrain the actions (or nonactions) and conditions of existence of others’,⁵ but are not enough to produce global collective action.

Pre-existing studies have had diverse discussions on countering cybercrime at the transnational level.⁶ First, pre-existing studies show that ‘cybercrime’ is an open-ended concept. Early scholars have had extensive discussions on classifying ‘cybercrime’, and they have largely agreed on a tripartite classification that has depended on the role of technology in the commission of crime.⁷ Nevertheless, more recent studies indicate that the boundary of ‘cybercrime’ is not clear.⁸ For example, incitement to commit genocide on the Internet may both constitute transnational cybercrime and one of the ‘core crimes’ subject to the International Criminal Court.⁹ Also, some scholars have implied that ‘cybercrime’ could entail cyberattacks and cyber espionage not committed by a state actor.¹⁰

⁴The eight treaties on cybercrime are: the Budapest Convention on Cybercrime (the Budapest Convention), and the two protocols under the Council of Europe (CoE) in 2001, 2006 and 2022 respectively; the 2018 Agreement on Cooperation Between Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Information Technology (CIS Agreement on Cybercrime) under the Commonwealth of Independent States (CIS); the 2009 Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization (ACEIIS) under The Shanghai Cooperation Organization (SCO); the 2010 Arab Convention on Combating Information Technology Offences (ACCITO) under the League of Arab States (LAS); the 2011 Directive on Fighting Cybercrime within Economic Community of West African States (DFC) under the Economic Community of West African States (ECOWAS); the 2012 African Union Convention on Cyber Security and Personal Data Protection (CCSPDP) under the African Union (AU). For the sake of relevance, the Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence will not be substantially observed in the following sections. Also, the article does not include the 2013 Directive on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA (the EU Directive) by the EU is that the EU ‘has legal personality and as such its own legal order which is separate from international law,’ although ‘where international agreements are concluded by the European Union they are binding upon its institutions and, consequently, they prevail over acts of the European Union’. In this regard, the EU Directive is not ‘governed by international law’. *Air Transport Association of America and Others v. Secretary of State for Energy and Climate Change*, Case C-366/10, [2011] ECR I-13755, at 50. The states parties of the Budapest Convention are available at www.coe.int/en/web/cybercrime/the-budapest-convention. The states parties of Protocol I are available at www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=189. Section 3 will provide further details of the treaties. Some scholars have referred to treaties that address crimes across borders as ‘prohibition regimes’. This article will also use this term. See E. A. Nadelmann, ‘Global Prohibition Regimes: The Evolution of Norms in International Society’, (1990) 44(4) *International Organization* 479.

⁵M. Barnett and R. Duvall, ‘Power in International Politics’, (2005) 59 *International Organization* 39, at 51.

⁶Parker’s *Crime by Computer* in 1976 is one of the earliest literatures concerning cybercrime. See D. B. Parker, *Crime by Computer* (1976).

⁷J. Clough, *Principles of Cybercrime* (2010), at 9–10; P. Kleve, R. De Mulder and K. van Noortwijk, ‘The Definition of ICT Crime’, (2011) 27 *Computer Law & Cybersecurity Review* 162, at 163–4. Wall’s classification is different from the tripartite one; instead, Wall classified ‘cybercrime’ into ‘cyber-trespass’, ‘cyber-deception/theft’, ‘(cyber-)pornography/obscenity’, ‘cyber-violence’, and ‘cyber-stalking’. D. Wall, ‘Cybercrimes and the Internet’, in D. Wall (ed.), *Crime and the Internet* (2001), 1, at 3–7.

⁸Goodman and Brenner have regarded ‘cybercrime’ as ‘consensus crime’, while Podgor has mentioned that offences in cyberspace can be both transnational and international crimes. See M. D. Goodman and S. W. Brenner, ‘The Emerging Consensus on Criminal Conduct in Cyberspace’, (2002) 10 *International Journal of Law and Information Technology* 139, at 175–215; E. S. Podgor, ‘Cybercrime: National, Transnational, or International’, (2004) 50 *Wayne Law Review* 97, at 102–6.

⁹M. Vagias, ‘The Territorial Jurisdiction of the ICC for Core Crimes Committed through the Internet’, (2016) 21 *Journal of Conflict & Security Law* 523, at 534.

¹⁰D. L. Speer, ‘Redefining Borders: The Challenges of Cybercrime’, (2000) 34 *Crime, Law and Social Change* 259, at 269–71; D. Weissbrodt, ‘Cyber-Conflict, Cyber-Crime, and Cyber-Espionage’, (2013) 22(2) *Minnesota Journal of International Law* 347, at 368–70; K. Kraszewski, ‘Classification of Cyber Operations under International Law’, (2015) 25 *Finnish Yearbook of International Law* 141, at 170; B. A. Walton, ‘Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law’, (2017) *Yale Law Journal* 1460, at 1474; C. Le Nguyen and W. Golman, ‘Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: “Law on the Books” vs “Law in Action”’, (2021) 40 *Computer Law & Security Review* 1, at 8; L. Yao-Chung Chang and J. Whitehead, ‘What the

Second, scholars recognize that regulatory divide attributable to economic and institutional factors of states is a major obstacle to transnational lawmaking on cybercrime.¹¹ For example, some states such as Cambodia and Ethiopia apply a paternalist approach that recognizes national security instead of human rights as the more prevailing ‘good’ that needs to be protected in cyberspace.¹² In contrast, some states such as the United Kingdom (UK) criminalize certain offences facilitated by digital technology, such as hate speech, which positively correlates with offline racially and religiously aggravated crime.¹³ Furthermore, there are contentions on the extension of criminal law to offences like hate speech due to its severe sanction on a certain type of free expression and its potential greater social harm than leaving it outside the criminal law.¹⁴ For example, Irving indicates that the UN Special Rapporteur on Freedom of Opinion and Expression and civil society is reluctant to support state regulation of atrocity speech because domestic criminalization could become an instrument of ‘suppress[ing] political dissent online under the guise of suppressing hate speech and incitement’.¹⁵ In this regard, it is still preferable to channel offences in cyberspace to tort law and other non-criminal law,¹⁶ even when digital technology as a ‘force multiplier’ that facilitates offences ‘to be committed on a scale that could not be achieved in the offline environment’.¹⁷

Third, scholars have diverged on the effective solution, namely by (i) concluding treaties, (ii) customary international law, or (iii) regime complex, to counter cybercrime. Some scholars have praised that treaties concluded between states should be the most effective method of preventing and prosecuting (certain types of) cybercrime by harmonizing the domestic criminal laws.¹⁸ Nevertheless, some scholars have pointed out that even the Budapest Convention cannot mitigate regulatory differences across states because it has not adequately addressed data protection and privacy concerns, provided a clear guidance to identify who should be responsible to prosecute cybercrime, established effective enforcement mechanisms, enabled participation of developing states and others.¹⁹ In this regard, Cody pointed out that any response to cybercrime must be

Hack: Reconsidering Responses to Hacking’, (2022) 17 *Asian Journal of Criminology* 113, at 123; S. Anstis, ‘Regulating Transnational Dissident Cyber Espionage’, (2024) 73 *International & Comparative Law Quarterly* 259, at 263, 270.

¹¹A. Oberdorfer Nyberg, ‘Is All Speech Local - Balancing Conflicting Free Speech Principles on the Internet’, (2004) 92 *Georgetown Law Journal* 663, at 679; N. Kshetri, *Cybercrime and Cybersecurity in the Global South* (2013), at 12–13.

¹²F. Gerry QC and C. Moore, ‘A Slippery and Inconsistent Slope: How Cambodia’s Draft Cybercrime Law Exposed the Dangerous Drift Away from International Human Rights Standards’, (2015) 31 *Computer Law & Security Review* 628, at 639–40; K. M. Yilma, ‘Ethiopia’s New Cybercrime Legislation: Some Reflections’, (2017) 33 *Computer Law & Security Review* 250, at 251–2.

¹³M. L. Williams et al., ‘Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime’, (2020) 60 *British Journal of Criminology* 93, at 111; R. Griffin, ‘New School Speech Regulation as a Regulatory Strategy against Hate Speech on Social Media: The Case of Germany’s NetzDG’, (2022) 46(9) *Telecommunications Policy* 5.

¹⁴A. Ashworth and J. Horder, *Principles of Criminal Law* (2013), at 33; R. K. Helm and H. Nasu, ‘Regulatory Responses to “Fake News” and Freedom of Expression: Normative and Empirical Evaluation’, (2021) 21 *Human Rights Law Review* 302, at 327.

¹⁵E. Irving, ‘Suppressing Atrocity Speech on Social Media’, (2019) 113 *AJIL Unbound* 256, at 260.

¹⁶D. T. Coenen, ‘Freedom of Speech and the Criminal Law’, (2017) 97(4) *Boston University Law Review* 1533, at 1543–80.

¹⁷See Clough, *supra* note 7, at 5.

¹⁸S. L. Marler, ‘The Convention on Cyber-Crime: Should the United States Ratify’, (2002) 37 *New England Law Review* 183, at 215–17; N. W. Cade, ‘An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code’, (2012) 37 *Brooklyn Journal of International Law* 1139, at 1170.

¹⁹A. N. Kitchen, ‘Go to Jail - Do Not Pass Go, Do Not Pay Civil Damages: The United States’ Hesitation towards the International Convention on Cybercrime’s Copyright Provisions’, (2002) 1 *John Marshall Review of Intellectual Property Law* 364, at 377; M. Keyser, ‘The Council of Europe Convention on Cybercrime’, (2003) 12 *Journal of Transnational Law & Policy* 287, at 324–6; A. M. Weber, ‘The Council of Europe’s Convention on Cybercrime’, (2003) 18 *Berkeley Technology Law Journal* 425, at 444–5; E. O’Herlihy, ‘The Cybercrime Convention: A Pioneering Text of International Legal Scope’, (2003) 4 *Hibernian Law Journal* 145, at 176; E. S. Podgor, ‘Cybercrime: National, Transnational, or International’, (2004) 50 *Wayne Law Review* 97, at 107; N. Seitz, ‘Transborder Search: A New Perspective in Law Enforcement’, (2004) 7 *Yale Journal of Law & Technology* 23, at 47–8; A. A. Cottim, ‘Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on

flexible and evolving; therefore, customary international law along with principles borrowed from economics to align interests of states should be the most efficient and effective means.²⁰ Also, the engagement of private actors in countering cybercrime has long deemed necessary to respond to cybercrime due to the incremental effects on behaviour in cyberspace in a society.²¹ For example, Mačák and other scholars have indicated that the engagement of non-state actors is not to replace decision-making processes of sovereign states but to provide an alternative solution to global governance of cybercrime by meeting the needs of states for highly specialized knowledge and direct control of information systems.²² Nevertheless, this proposal is not without problems unless there is a stable legal framework to allocate roles and functions of private actors in law enforcement.²³ In particular, it is recognized that ‘cybercrime may yet—and should—cause transformations in how transnational criminal justice is configured, with more focus on the people affected as suspects and witnesses, and less focus on nation states’.²⁴

The pre-existing studies contribute to explaining that (i) evolving nature of cybercrime; (ii) national disparities; (iii) policy preferences at the transnational level are the main obstacles to global collective action against countering cybercrime. Nevertheless, the pre-existing studies have taken ‘cybercrime’ as *ipso facto* without observing (i) how ‘cybercrime’ has been framed under the pre-established treaties; (ii) if and how ‘cybercrime’ is evolving at the transnational level; and (iii) how evolution of ‘cybercrime’ enlightens potential strategies for global co-operation in countering cybercrime. Notwithstanding, the clarifications are essential to understand (i) how international co-operation of countering cybercrime has been operating; (ii) to what extent limits of international law to national power could be accepted in the international society; (iii) how inherent weakness of international law may affect global collective action against countering cybercrime. In this regard, this article will fill in the gaps. Methodologically, a socio-legal approach which is interdisciplinary by bringing Transnational Criminal Law (TCL) into dialogue with the conceptual framework of recursivity will be adopted.²⁵ TCL, which reveals obscurity in international criminal law and crimes of international concern, contributes to contextualizing ‘cybercrime’ in the pre-existing regional prohibition regimes, while recursivity helps illuminate

Cybercrime’, (2010) 2 *European Journal of Legal Studies* 55, at 78–9; M. Gercke, ‘10 Years Convention on Cybercrime: Achievements and Failures of the Council of Europe’s Instrument in the Fight against Internet-related Crimes’, (2011) 5 *Computer Law Review International* 142, at 145–6; J. Clough, ‘A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation’, (2014) 40(3) *Monash University Law Review* 698, at 734–6.

²⁰J. A. Cody, ‘Derailing the Digitally Depraved: An International Law & (and) Economics Approach to Combating Cybercrime & (and) Cyberterrorism’, (2002) 11 *Michigan State University-Detroit College of Law’s Journal of International Law* 231, at 252–9.

²¹See Clough, *supra* note 7, at 8; Podgor, *supra* note 8, at 101–5; G. Allan, ‘Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative’, (2005) 2005 *New Zealand Law Review* 149, at 168–78; J. P. Jurich, ‘Cyberwar and Customary International Law: The Potential of a “Bottom-up” Approach to an International Law of Information Operations’, (2008) 9 *Chicago Journal of International Law* 275, at 292–5; L. Y. C. Chang, L. Y. Zhong and P. N. Grabosky, ‘Citizen Co-Production of Cyber Security: Self-Help, Vigilantes, and Cybercrime’, (2018) 12(1) *Regulation & Governance* 101, at 110; M. Yar, ‘Transnational Governance and Cybercrime Control: Dilemmas, Developments and Emerging Research Agendas’, in T. Hall and V. Scalia (eds.), *A Research Agenda for Global Crime* (2019), 91, at 99.

²²A. P. Jakobi, ‘Non-State Actors and Global Crime Governance: Explaining the Variance of Public-Private Interaction’, (2016) 18(1) *British Journal of Politics and International Relations* 72, at 82, 85–6; K. Mačák, ‘From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers’, (2017) 30(4) *LJIL* 877, at 894.

²³N. Purtova, ‘Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships’, (2018) 8(1) *International Data Privacy Law* 52, at 67.

²⁴D. Brodowski, ‘The Emerging History of Transnational Criminal Law Relating to Cybercrime’, in N. Boister, S. Gless and F. Jessberger (eds.), *Histories of Transnational Criminal Law* (2021), 236, at 247–8.

²⁵The sociolegal approach adopted in this article has its root in Jessup’s transnational law. Also, Halliday and Shaffer as well as other scholars have expanded scopes of studies on transnational law. See P. C. Jessup, *Transnational Law* (1956); T. C. Halliday and G. Shaffer, ‘Transnational Legal Orders’, in T. C. Halliday and G. Shaffer (eds.), *Transnational Legal Orders* (2015), 3, at 64; T. Halliday, M. Levi and P. Reuter, ‘Why Do Transnational Legal Orders Persist?: The Curious Case of Money-Laundering Controls’, in G. Shaffer and E. Aaronson (eds.), *Transnational Legal Ordering of Criminal Justice* (2020), 51, at 75–80.

legal changes emerging from the UN negotiating processes on formulating a scheme for global collective action against cybercrime.²⁶ This article argues that normative changes in transnational criminalization of ‘cybercrime’ reflect that a common interest is crystallizing without common understanding. Therefore, this author proposes that states should maintain a minimum public order to avoid stagnation of international co-operation in countering cybercrime. The structure of this article goes as specified: following the Introduction, Section 2 presents how TCL and recursivity as the conceptual frameworks will methodologically contribute to contextualizing concepts in prohibition regimes and illuminating legal changes under the international legal system; Section 3 analyses how the pre-existing treaties shape ‘cybercrime’ and what the implications of the framing are; Section 4 presents and analyses different positions of states in negotiations on framing cybercrime under the UN. In particular, the observations serve determination of state practice and *opinio juris*, which further helps define rights and obligations of states in cyberspace under international law;²⁷ Section 5 discusses implications of the normative changes by arguing that global ‘denationalization’ and ‘renationalization’ of ‘cybercrime’ is unlikely in the international society without central enforcement mechanism, when states are still working on adapting human and sovereignty in cyber governance by expanding old regulation and creating new rules to deal with law in computation;²⁸ Section 6 concludes this article.

2. The conceptual frameworks for framing transnational crime

2.1 Transnational criminalization: A conceptual construct

Transnational criminalization is a constructive set of processes that ‘locate, perceive, identify, and label’ certain activities ‘transcending international borders, transgressing the laws of several states or having an impact on another country’ as crimes.²⁹ Essentially, transnational criminalization does not ‘criminalize’ but seeks common ground on prosecuting criminals at a levelling playing field across states.³⁰ In other words, only ‘the indirect suppression by international law through domestic penal law of criminal activities’³¹ is created to aim at ‘fending off harmful behaviour . . . necessarily geared to protection of what are legitimate interests’.³² In practice, states always need to persuade domestic and foreign audiences to accept that international intervention in the

²⁶N. Boister, ‘Further Reflections on the Concept of Transnational Criminal Law’, (2015) 6 *Transnational Legal Theory* 9, at 24. Some scholars have proposed that TCL should not confine to treaties on countering crimes across borders. This article agrees that domestic law and soft law contribute to transnational prosecution of crimes, but it is more practical to start with the treaties because sovereignty still reigns international law. See P. Kotiswaran and N. Palmer, ‘Rethinking the International Law of Crime: Provocations from Transnational Legal Studies’, (2015) 6 *Transnational Legal Theory* 55; T. C. Halliday, ‘Recursivity of Global Normmaking: A Sociolegal Agenda’, (2009) 5 *Annual Review of Law and Social Science* 263; E. Aaronson and G. Shaffer, ‘Defining Crimes in a Global Age: Criminalization as a Transnational Legal Process’, (2021) 46(2) *Law & Social Inquiry* 455, at 457, 461–4. This article will solely focus on the aspect of transnational criminalization for the sake of scope and length.

²⁷This author is enlightened by Pomson’s work and considers that observations on the UN negotiating processes on cybercrime help determine *opinio juris* of states. See O. Pomson, ‘Methodology of Identifying Customary International Law Applicable to Cyber Activities’, (2023) 36(4) *LJIL* 1023, at 1042.

²⁸See Boister, *supra* note 26, at 26–7; K. C. Yoon Onn, ‘The Prosecutor’s New Policy on “Cyber Operations” before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections’, *EJIL:Talk!*, 15 September 2023, available at www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-the-international-criminal-court-and-its-implications-for-ukraine-some-preliminary-reflections/; T. DoCarmo et al., ‘The Law in Computation: What Machine Learning, Artificial Intelligence, and Big Data Mean for Law and Society Scholarship’, (2021) 43(1) *Law & Policy* 170, at 188–92.

²⁹E. Goffman, *Frame Analysis: An Essay on the Organization of Experience* (1986), 21; G. O. W. Mueller, ‘Transnational Crime: Definitions and Concepts’, in P. Williams and D. Vlassis (eds.), *Combating Transnational Crime: Concepts, Activities and Responses* (2001), 13, at 13; Boister, *supra* note 26, at 9; Aaronson and Shaffer, *supra* note 26, at 457.

³⁰See Clough, *supra* note 7, at 18; D. Husak, *Overcriminalization: The Limits of the Criminal Law* (2008), 94.

³¹N. Boister, ‘“Transnational Criminal Law”?’, (2003) 14(5) *European Journal of International Law* 953, at 955.

³²N. McCormick, *Legal Right and Social Democracy: Essays in Legal and Political Philosophy* (1982), at 30.

internal affairs of other states should be justifiable and legitimate.³³ Therefore, transnational criminalization by no means produces ‘a neutral system of disincentives that convey no disapproval’³⁴ but only sets ‘a base line of criminalization and punishment’ without obstructing discretion and autonomy of states to create offences with broader scopes or more severe punishments.³⁵ For example, the US Supreme Court ruled that forcible abduction of Alvarez-Machain, a Mexican, by agents of the Drug Enforcement Administration (DEA) to the US after failing ‘to gain respondent’s presence in the United States through informal negotiations with Mexican officials’ was not a shield from being tried ‘in a court in the United States for violations of the criminal laws of the United States’.³⁶

Generally, transnational criminalization can produce two effects. One is that a state has justifications to police extraterritorially and/or render adjudication with extraterritorial effects by ‘establish[ing] their jurisdiction over persons, property, and acts outside their territory, limited only in certain cases by pre-existing “prohibitive rules” of international law’.³⁷ For example, the ICJ indicates in the *Immunities and Criminal Proceedings* case that a requirement of double criminality under ‘Article 6 (2)(c) of the Palermo Convention does not provide for the exclusive jurisdiction of the State on whose territory such an offence was committed’.³⁸ The other is to reshape domestic criminal law, which will be re-uploaded to alter international lawmaking processes and further influence other national laws.³⁹ For instance, some developing states such as China and Brazil are also influencing the process of transnational criminalization, which was historically subject to the crime control policies of the developed states, to block criminal flows originating in developing states.⁴⁰ Notwithstanding, transnational criminalization does not necessarily mitigate jurisdictional conflicts which could result in international discord as it is long recognized that the best place of punishment should be the place where the crime was committed.⁴¹

2.2 Transforming transnational criminalization in plurality

Undoubtedly, plural sources of legal normativity with heterogeneity of interests coexist in the international legal sphere without either complete autonomy or dependency: states operate through the balance of power, producing (i) actor mismatch; (ii) diagnostic struggles; (iii) contradictions; and (iv) indeterminacy of law, as four incentives that change the course of international decision-making processes including transnational criminalization.⁴²

First, actor mismatch arises from normative interactions when stakeholders are excluded from law-making processes: the excluded actors may marginalize the laws, which would frustrate the

³³P. Andreas and E. Nadelmann, *Policing the Globe: Criminalization and Crime Control in International Relations* (2006), at 19.

³⁴A. P. Simester and A. von Hirsch, *Crimes, Harms, and Wrongs: On the Principles of Criminalisation* (2011), at 12.

³⁵N. Boister, ‘The Concept and Nature of Transnational Criminal Law’, in N. Boister and R. J. Currie (eds.), *The Routledge Handbook of Transnational Criminal Law* (2015), 11, at 16, 19; N. Boister, *An Introduction to Transnational Criminal Law* (2018), at 23.

³⁶*United States v. Alvarez-Machain*, 504 U. S. 655 (9th Cir. 1992), at 657, 670.

³⁷See Boister (2018), *supra* note 35, at 247.

³⁸*Immunities and Criminal Proceedings (Equatorial Guinea v. France)*, Preliminary Objections, Judgment of 6 June 2018, [2018] ICJ Rep. 292, at 327, para. 116.

³⁹See Boister (2018), *supra* note 35, at 20.

⁴⁰*Ibid.*, at 20; V. Mitsilegas, ‘The Global Governance of Transnational Crime: Implications for Justice and the Rule of Law’, in V. Mitsilegas et al. (eds.), *Transnational Crime: European and Chinese Perspectives* (2019), 5, at 16.

⁴¹C. Beccaria, *An Essay on Crimes and Punishments* (1899), 111; N. Passas, ‘Globalization and Transnational Crime: Effects of Criminogenic Asymmetries’, in P. Williams and D. Vlassis (eds.), *Combating Transnational Crime: Concepts, Activities and Response* (2001), 22, at 26. See also *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (Sup. Ct. 1991).

⁴²A-C. Martineau, ‘The Rhetoric of Fragmentation: Fear and Faith in International Law’, (2009) 22(1) *LJIL* 1, at 26; D. Burchardt, ‘Intertwinement of Legal Spaces in the Transnational Legal Sphere’, (2017) 30(2) *LJIL* 305, at 306, 313–14.

regulatory goals.⁴³ One example is the Rome Statute of the International Criminal Court (the Rome Statute) which has not embodied China's stance of rejecting automatic jurisdiction and preferring an opt-in system; therefore, the Rome Statute has lost its goal of inviting universal participation due to China's final opposing vote.⁴⁴ Second, disagreements with the scope of the conduct or 'over whether a social problem should be addressed through criminal law measures or alternative policies' in crime controls would trigger diagnostic struggles.⁴⁵ For example, both China and the UK criminalize sexual offences, but China does not criminalize 'forced sodomy on other men or young boys older than age fourteen'.⁴⁶ In practice, the struggles would drive domain expansion that produces new conceptualization of social problems and stretch the definitional boundaries of the targeted phenomenon.⁴⁷ Third, unresolved tensions in and between norms may lead to contradictions which 'seek simultaneously to satisfy competing ideologies in the same law without resolving ... to the mutual satisfaction of the conflicting parties to lawmaking'.⁴⁸ A tension between drug control and guarantees of the right to liberty and security of person under the Single Convention on Narcotic Drugs which allows deprivation of liberty as penal sanctions on drug abuse without clearly setting a limit to sovereign prerogative can be an example.⁴⁹ Operationally, contradictions strengthen the norms when contestor(s) can reconstruct the pre-existing authorit(ies), and vice versa.⁵⁰ Fourth, an intention of states to compete for interpretative authority would cause indeterminacy of law.⁵¹ Developing countries often adopt such a strategy in formulating regional trade agreements with higher flexibilities to adapt diverse interests and preferences.⁵² Nevertheless, indeterminacy would dampen a regime's ability to operate as 'a system of rules coordinating the freedom of actors who behave in line with a purposive rationality'.⁵³

In practice, whether a cycle of normative changes may end up modifying pre-existing rules depends on persuasiveness which is conditioned by (i) support of multiple great powers; (ii) consistency with dominant epistemic justification in the international legal order; and (iii) sufficiency of normative bases.⁵⁴ Simultaneously, conceptual and/or operational internalization at the domestic level decide whether transformation would be successful.⁵⁵ Otherwise, states would

⁴³See Halliday, *supra* note 26, at 269; Aaronson and Shaffer, *supra* note 26, at 464.

⁴⁴B. Jia, 'China and the International Criminal Court: The Current Situation', (2006) 10 *Singapore Yearbook of International Law* 87, at 88–90.

⁴⁵See Halliday, *supra* note 26, at 278; Aaronson and Shaffer, *supra* note 26, at 461–3.

⁴⁶W. Luo, 'China', in K. Jon Heller and M. D. Dubber (eds.), *The Handbook of Comparative Criminal Law* (2011), 137, at 167; A. J. Ashworth, 'United Kingdom', in K. Jon Heller and M. D. Dubber (eds.), *The Handbook of Comparative Criminal Law* (2011), 531, at 550–1.

⁴⁷E. Aaronson and G. Shaffer, 'The Transnational Legal Ordering of Criminal Justice', in G. Shaffer and E. Aaronson (eds.), *Transnational Legal Ordering of Criminal Justice* (2020), 3, at 12.

⁴⁸S. Liu and T. C. Halliday, 'Recursivity in Legal Change: Lawyers and Reforms of China's Criminal Procedure Law', (2009) 34(4) *Law & Social Inquiry* 911, at 914.

⁴⁹R. Lines, J. Hannah and G. Girelli, '"Treatment in Liberty" Human Rights and Compulsory Detention for Drug Use', (2022) 22(1) *Human Rights Law Review* 1, at 25–31.

⁵⁰J. Mende, 'The Contestation and Construction of Global Governance Authorities: A Study from the Global Business and Human Rights Regime', (2021) 10(3) *Global Constitutionalism* 377, at 381.

⁵¹See Boister (2015), *supra* note 35, at 16, 19; T. M. Franck, *The Power of Legitimacy among Nations* (1990), 52; Liu and Halliday, *supra* note 48, at 914; G. Hernández, 'Law's Determinability: Indeterminacy, Interpretative Authority, and the International Legal System', (2022) 69 *Netherlands International Law Review* 191, at 198–201, 213. 'Indeterminacy of law' in this article is not confined to linguistic indeterminacy. See C. A. Miles, 'Indeterminacy', in J. D'Aspremont and S. Singh (eds.), *Concepts for International Law: Contributions to Disciplinary Thought* (2019), 447, at 447–58.

⁵²D. K. Elms, 'Getting RCEP across the Line', (2021) 20(3) *World Trade Review* 373, at 374–5; T. Schöfer, 'From Developing Country Leader to Flexible Negotiator: New Directions in Brazilian Trade Strategy', (2023) 22(5) *World Trade Review* 629, at 641.

⁵³K. Gunther, 'The Pragmatic and Functional Indeterminacy of Law', (2011) 12 *German Law Journal* 407, at 408.

⁵⁴W. Sandholtz, *Prohibiting Plunder: How Norms Change* (2007), at 23.

⁵⁵M. Finnemore and K. Sikkink, 'International Norm Dynamics and Political Change', (1998) 52(4) *International Organization* 887, at 902–5.

be prompted to retreat and to resort to opportunistic alliance/partnership to reap profits at the expense of institutional capacity and longevity.⁵⁶ Currently, stagnation in multilateral law-making is general due to asymmetric power structures arising from great power rivalry and a shifting distribution of global power under weakened multilateral institutions.⁵⁷

3. Transnational criminalization of cybercrime in the fragmented world

3.1 The regional regimes as clubs

The eight treaties on cybercrime as noted in the Introduction have uneven distribution with modest overlaps as specified in Figure 1.⁵⁸

Evidently, the treaties have been club goods with different leveraging power: the Budapest Convention, with all member states of the EU, 11 American countries including the US, five African states, five Asian states, and two Oceanian states, not only has the greatest institutional power but also has significant productive power to diffuse knowledge and discursive practices as many Pacific Island Countries (PICs) that are non-parties have imported its provisions into domestic legislation.⁵⁹ Conversely, the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization (ACEIIS) only share members with the Treaty establishing the Commonwealth of Independent States (CIS Agreement), which has limited the spread of the norms and enabled the states with dual membership to move between the two venues for the sake of convenience and benefits.⁶⁰ Additionally, the Arab Convention on Combating Information Technology Offences (ACCITO) also has scarce intersection with the other treaties probably because the Arabian states intend to be flexible in balancing power in a co-ordinated manner by the identity of Islam.⁶¹ In turn, they are

⁵⁶P. G. Danchin et al., 'Navigating the Backlash against Global Law and Institutions', (2020) 38 *Australian Yearbook of International Law* 33, at 50.

⁵⁷A. Motzfeldt Kravik, 'An Analysis of Stagnation in Multilateral Law-making – and Why the Law of the Sea has Transcended the Stagnation Trend', (2021) 34(4) *LJIL* 935, at 952–3.

⁵⁸The states parties of the Budapest Convention are available at www.coe.int/en/web/cybercrime/the-budapest-convention. The states parties of the Protocol I are available at www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treotypnum=189. The CIS Agreement on Cybercrime has replaced the Agreement on Cooperation Between Member States of the Commonwealth of Independent States in the Fight Against Crimes in the Field of Computer Information concluded in 2001. The states parties of the CIS Agreement on Cybercrime include Azerbaijan, Moldova, Armenia, Russia, Belarus, Tajikistan, Turkmenistan, Kazakhstan, Uzbekistan, Kyrgyzstan, and Ukraine. The text of the CIS Agreement on Cybercrime is available at cis.minsk.by/reestr2/doc/5864#text. The states parties of the ACEIIS include India, Kazakhstan, China, Kyrgyzstan, Russia, Pakistan, Tajikistan, Uzbekistan, and Iran. The text of the ACEIIS is available at eng.sectesco.org/documents/?year=2009. The states parties of the ACCITO include Jordan, the United Arab Emirates (UAE), Bahrain, Tunisia, Algeria, Djibouti, Saudi Arabia, Sudan, Syria, Somalia, Iraq, Oman, Palestine, Qatar, Comoros, Kuwait, Lebanon, Libya, Egypt, Morocco, Mauritania, and Yemen. The text of the ACCITO is available at www.asianlaws.org/gclid/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf. The states parties of the DFC include Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, the Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo. The text of the DFC is available at database.cyberpolicyportal.org/en/entity/9qrgsf640zq?page=3. The states parties of the CCSPDP include Angola, Cape Verde, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Sao Tome & Principe, Togo, and Zambia. The text of the CCSPDP is available at au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf. The status list is available at au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf.

⁵⁹M. Barnett and R. Duvall, 'Power in International Politics', (2005) 59(1) *International Organization* 39, at 51–2, 55; Le Nguyen and Golman, *supra* note 10, at 2.

⁶⁰M. Laruelle and S. Peyrouse, 'Friendship with Moderation: The Central Asian Point of View on the SCO', in M. Fredholm (ed.), *The Shanghai Cooperation Organization and Eurasian Geopolitics: New Directions, Perspectives, and Challenges* (2013), 229, at 232.

⁶¹A. Ehteshami, *Globalization and Geopolitics in the Middle East: Old Games, New Rules* (2007), 56. Some scholars regard the identity of Islam as 'an all-encompassing system of beliefs and principles which regulate all walks of life including economics and politics'. See A. E. Hillal Dessouki and B. Korany, 'Globalization and Arab Foreign Policies: Constraints or

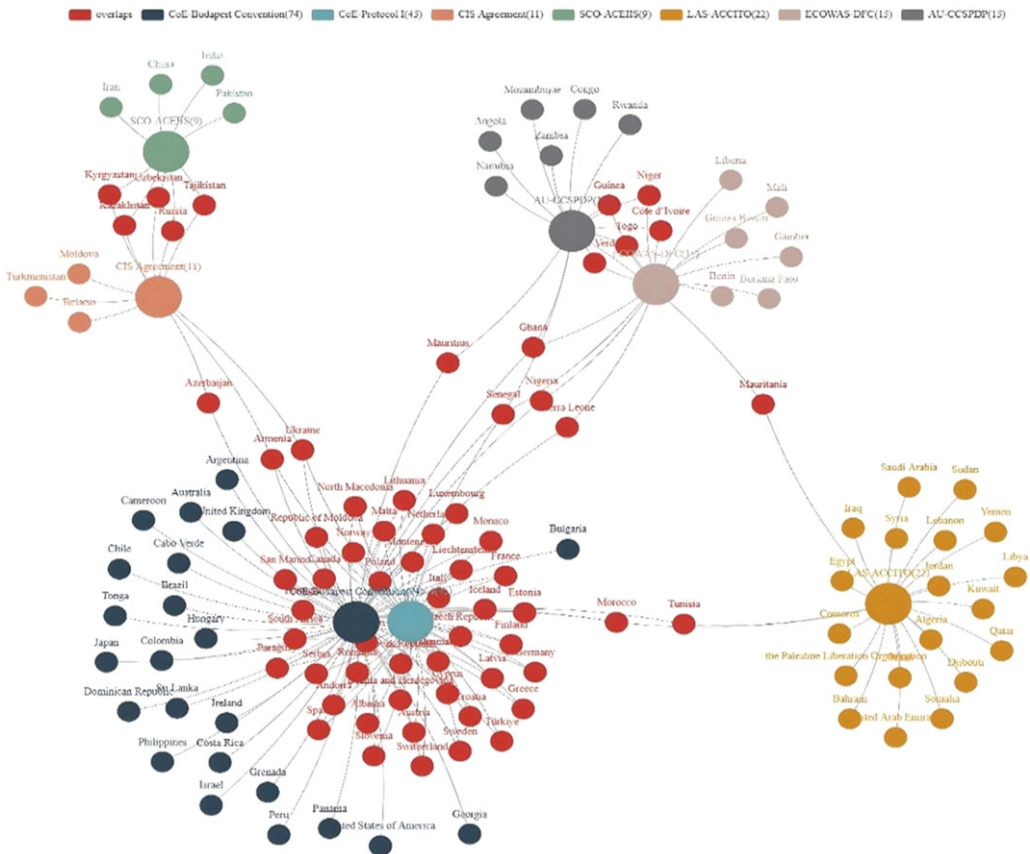


Figure 1. Current multilateral treaties on countering cybercrime and their overlaps

cautious about ‘separat[ing] states who are seriously interested in cooperation from those who have more exploitative motivations’.⁶²

3.2 Criminalizing ‘cybercrime’ in normative plurality: Scopes, liability, and conditions

This section observes the contours of cybercrime under the treaties from three dimensions: (i) the scopes of offences; (ii) the scope of criminal liability; and (iii) the conditions of criminal liability.

3.2.1 Kaleidoscopic ‘cybercrime’

Given the elasticity of ‘cybercrime’ ranging from ‘direct attacks against systems and networks, with the goal of flaunting institutions by crashing systems or causing physical damage’ to ‘the manipulation of social media and the theft or purchase of personal profiles’,⁶³ only the CIS

Marginalization?’, in B. Korany and A. E. Hillal Dessouki (eds.), *Foreign Policies of Arab States: The Challenge of Globalization* (2008), 45, at 46.

⁶²A. Kydd, ‘Trust Building, Trust Breaking: The Dilemma of NATO Enlargement’, (2001) 55(4) *International Organization* 801, at 801.

⁶³A. Alexandrou, ‘Cybercrime’, in M. Natarajan (ed.), *International and Transnational Crime and Justice* (2019), 146, at 151.

Agreement and ACEIIS define ‘cybercrime’ as ‘a criminal act ... whose encroachment is computer information’⁶⁴ and ‘using information resources and/or influencing them in the information space for illegal purposes’.⁶⁵ Simultaneously, ‘cybercrime’ under the treaties all includes two categories of offences, namely cyber-dependent offences that are ‘malicious activities that would not exist outside of the digital realm’ and cyber-enabled offences that digital technology is leveraging to amplify existing forms of offending.⁶⁶ First, all the treaties recognize (i) unauthorized access to computers or computer systems; (ii) malicious software; and (iii) denial of service attacks as cyber-dependent offences, but states can still have ‘discretion in implementation as to ... [create] an idiosyncratic representation of different features or elements of the conventions in a number of different pieces of national legislation’;⁶⁷ the similarity in cyber-dependent offences may simply represent coincidence in wide abhorrence of harmful behaviour rather than substantive harmonization of domestic criminal law, which is sufficient to enable international co-operation.⁶⁸ For example, unlike the US, the UK does not prescribe a conduct that ‘exceeds authorised access’ to obtain information as illegal access, although both countries are parties to the Budapest Convention.⁶⁹

Second, the treaties diverge greatly on cyber-enabled offences as specified in Table 1:

Essentially, domestic criminal law and culture serve as a pivotal conditioning factor. For example, the CIS Agreement does not require states to proscribe fraud and forgery in cyberspace given disparities in the domestic criminal laws of the CIS member states: Articles 281–282 of the Criminal Code of the Republic of Tajikistan address general forgery without any digital element, while Azerbaijan does not criminalize ‘fraud’ *per se*.⁷⁰ The situation is similar in child pornography because ‘minor’ is an aggravating factor instead of an independent punishable crime under the Russia Criminal Code.⁷¹ Simultaneously, the ACCITO and Directive on Fighting Cybercrime within Economic Community of West African States (DFC) require complete prohibition of pornography which is ‘unethical’ in Islamic norms which pervade both regions.⁷² Furthermore, the scope of cyber-enabled offences would be implicitly enlarged under the ACEIIS, ACCITO, DFC, and the African Union Convention on Cyber Security and Personal Data Protection

⁶⁴Agreement on Cooperation of the Member States of the Commonwealth of Independent States in Combating Crimes in the Field of Computer Science Information, Art.1(a).

⁶⁵Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, Annex 1.

⁶⁶B. Dupont and C. Whelan, ‘Enhancing Relationships Between Criminology and Cybersecurity’, (2021) 54(1) *Journal of Criminology* 76, at 79.

⁶⁷*Ibid.*, at 16, 19.

⁶⁸See McCormick, *supra* note 32, at 30; Boister (2018), *supra* note 35, at 25.

⁶⁹The Computer Misuse Act 1990 (CMA) only addresses unauthorized access, while the Computer Fraud and Abuse Act (CFAA) also includes ‘exceeding authorised access’.

⁷⁰The Criminal Code of the Republic of Tajikistan is available at legislationline.org/sites/default/files/documents/f3/Tajikistan_CC_1998_am2020_en.pdf. The Criminal Code of the Azerbaijan Republic is available at adsdatabase.ohchr.org/IssueLibrary/AZERBAIJAN_Criminal%20Code.pdf. Though this article only resorts to unofficial translations of the laws, they are reliable because they are retrieved from the United Nations Human Rights Office of the High Commissioner (OHCHR) or Office of Democratic Institutions and Human Rights (ODIHR) vested under the Organization for Security and Co-operation in Europe (OSCE).

⁷¹Y. Isakova and E. Millerov, ‘Legal Issues in the Field of Digital Technologies in Russia’, (2021) 273 *E3S Web of Conferences* 1.

⁷²D. Beekers and L. L. Schrijvers, ‘Religion, Sexual Ethics, and the Politics of Belonging: Young Muslims and Christians in the Netherlands’, (2020) 67(1) *Social Compass* 137, at 144–6; B. Saho, ‘Chapter 9: Islam in West Africa: Diffusion and Growth’, in F. Ngom, M. H. Kurfi and T. Falola (eds.), *The Palgrave Handbook of Islam in Africa* (2020), 149, at 156.

Table 1. Types of cyber-enabled offences under the treaties

Title	Computer-related forgery & fraud	Infringements of copyright and related rights	Pornography		Offences against the person		
			All	Child	Against privacy	Racist/ Xenophobic	Terrorist
The Budapest Convention	✓	✓	N/A	✓	N/A	N/A	N/A
Protocol I	N/A	N/A	N/A	N/A	N/A	✓	N/A
CIS Agreement	N/A	✓	N/A	N/A	N/A	N/A	N/A
ACEIIS	✓	✓	N/A	✓	N/A	N/A	N/A ⁷³
ACCITO	✓	✓	✓	N/A	✓	N/A	✓
DFC	✓	✓	✓	✓	N/A	✓	N/A
CCSPDP	✓	✓	N/A	✓	✓	✓	N/A

(CCSPDP) as ‘State Parties shall take the necessary legislative and/or regulatory measures to consider as aggravating circumstances the use of information and communication technologies to commit offences such as . . . money laundering’.⁷⁴ Nevertheless, these proscriptions may result in vague and broad rules that do not ‘satisfy the cumulative conditions of legality, necessity and legitimacy’ at the domestic level.⁷⁵ For example, the Mauritian Information and Communication Technologies Act 2001 provides that ‘in any other manner contravenes this Act or any regulations made under this Act, shall commit an offence’ which brings about ‘a fine not exceeding 1,000,000 rupees and to penal servitude for a term not exceeding 10 years’.⁷⁶

3.2.2 No agreement on when to be accountable for ‘cybercrime’

First, some treaties such as the CIS Agreement and ACEIIS lack proscriptions of attempts and complicity, which suggests that the states lack a co-ordinated standard for constraining risks arising from cybercrime.⁷⁷ attempts and complicity are probabilities that crime would follow upon⁷⁸ and ‘assistance or encouragement someone gives another in the commission of a crime as itself a crime’.⁷⁹ In practice, such an absence would dampen the goal of the treaties ‘to mark out that range of pre-existing (pre-criminal) wrongs that the polity will treat as public wrongs, and for which citizens will therefore be called to account, convicted, and punished by the polity’s criminal

⁷³The ACEIIS also prescribes ‘[d]issemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States’, but it does not clarify whether the states should commit to criminalization.

⁷⁴African Union Convention on Cyber Security and Personal Data Protection, Art. 30, para. 1(b).

⁷⁵Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Note by the Secretariat, UN Doc. A/HRC/38/35 (2018), at 5.

⁷⁶Information and Communication Technologies Act 2001 of Mauritius, Arts. 46 and 47, available at www.icta.mu/documents/2022/04/ict_act.pdf.

⁷⁷G. Yaffe, *Attempts: In the Philosophy of Action and the Criminal Law* (2010), 28; A. P. Simester, *Fundamentals of Criminal Law: Responsibility, Culpability, and Wrongdoing* (2021), at 155.

⁷⁸Y. Hong and W. Neilson, ‘Cybercrime and Punishment’, (2020) 49 *Journal of Legal Studies* 431, at 445.

⁷⁹J. Deigh and D. Dolinko, ‘Introduction’, in J. Deigh and D. Dolinko (eds.), *The Oxford Handbook of Philosophy of Criminal Law* (2011), i, at vii.

courts⁸⁰ because ambiguity in the texts is the room left for later fine-tuning of those unresolved disagreements or uncertainties.⁸¹ Second, only the Budapest Convention and CCSPDP require the states to prescribe ‘intention’ as the central and most grave mental state in constituting ‘cybercrime’,⁸² although most of the treaties except the ACEIIS ascribe ‘the property of bodily-movement-caused-by-a-volition’.⁸³ In other words, there is significant disparity in whether preventive efficacy of public censure at the expense of ‘an essential safeguard against unjust convictions and disproportionate punishment’ should be prioritized.⁸⁴ *mens rea* ‘restrict[s] criminal statutes to conduct that is “inevitably nefarious”⁸⁵ and helps avoid charges of ‘mistaken or careless acts of unauthorized access of a computer or data therein’.⁸⁶ For example, the Supreme Court of the United States in *Rehaif v. United States* provides that the application of *mens rea* ‘helps to separate wrongful from innocent acts’,⁸⁷ although there is always a ‘fit problem’ between intention and harm.⁸⁸

3.3 Appraisal

The aforementioned observations and analyses on ‘cybercrime’ under the treaties demonstrate that states have wide demands for framing ‘cybercrime’ under ‘a multiplicity of domestic legal systems in loose array’⁸⁹ by simple clarification of ‘the general and abstract question whether a crime has been committed’.⁹⁰ Nevertheless, no shared ‘understanding of the nature of particular wrongs and the way these are protected in law’⁹¹ has emerged from the aspirations to help set ‘legal limits that delimit [sovereign] scope of action, that confer power by allocating it’⁹² at the transnational level: even the similarity between the Budapest Convention and CCSPDP may only reflect that the European states have embedded its institutions in Africa through colonization, foreign aid, cultural influence, and political engagement.⁹³ Correspondingly, unavoidable norm conflicts and strategic rivalry may arise, especially when the treaties have different institutional capacities.⁹⁴ For example, Armenia and Azerbaijan by participating in the CyberEast under the Budapest Convention have been recommended to ‘take action against all proceeds of crime involving [virtual assets]’ through measures adapted to domestic circumstances to counter online

⁸⁰R. A. Duff, ‘Political Retributivism and Legal Moralism’, (2012) 1 *Virginia Journal of Criminal Law* 179, at 197.

⁸¹See Franck, *supra* note 51, at 52.

⁸²Compared with the Budapest Convention, *mens rea* requirements in the CCSPDP are incomplete because some offences only include *actus reus*.

⁸³M. S. Moore, *Act and Crime: The Philosophy of Action and its Implications for Criminal Law* (1993), at 169.

⁸⁴S. F. Smith, ‘Overcoming Overcriminalization’, (2013) 102 *Journal of Criminal Law & Criminology* 537, at 568; A. Ashworth and L. Zedner, *Preventive Justice* (2014), at 116–17, 265.

⁸⁵S. F. Smith, ‘Proportional Mens Rea’, (2009) 46 *American Criminal Law Review* 127, at 127.

⁸⁶M. Dan-Cohen, ‘Decisions Rules and Conduct Rules: On Acoustic Separation in Criminal Law’, (1984) 97 *Harvard Law Review* 625, at 663.

⁸⁷*Rehaif v. United States*, 139 S. Ct. 2191 (2019), at 2197.

⁸⁸See Clough, *supra* note 7, at 348.

⁸⁹See Boister (2018), *supra* note 35, at 39.

⁹⁰R. N. Gooderson, ‘Similar Facts and Actus Reus’, (1959) 17 *Cambridge Law Journal* 210, at 212.

⁹¹L. Farmer, *Making the Modern Criminal Law: Criminalization and Civil Order* (2016), at 28, 30.

⁹²M. Köpcke, ‘Law and the Limits of Sovereign Power’, (2021) 66(1) *American Journal of Jurisprudence* 115, at 115.

⁹³A. A. Mazrui, *Africa’s International Relations: The Diplomacy of Dependency and Change* (1977), 85–7; B. E. Whitaker and J. F. Clark, *Africa’s International Relations: Balancing Domestic & Global Interests* (2018), 288; F. Plank, *Evaluating the Africa-EU Partnership on Peace and Security: Interregional Cooperation in Peace Operations* (2022), at 5–7.

⁹⁴L. A. Schuette, ‘Shaping Institutional Overlap: NATO’s Responses to EU Security and Defence Initiatives since 2014’, (2023) 25(3) *The British Journal of Politics and International Relations* 423, at 425–8; W. Neal, ‘Russia Slips from Center Stage as UN Cybercrime Treaty Negotiations Forge Ahead’, *OCCRP*, 15 September 2022, available at www.occrp.org/en/daily/16769-russia-slips-from-center-stage-as-un-cybercrime-treaty-negotiations-forge-ahead.

fraud,⁹⁵ but there is no resolution device to clarify whether the recommendations are compatible with the commitments under the CIS Agreement.⁹⁶ Otherwise, ‘undue encroachment on a jurisdiction more properly appertaining to, or more appropriately exercisable by, another State’ would still occur.⁹⁷ What the Supreme Court of Norway has suggested in *Tidal Music AS v. The public prosecution authority* about the exercise of investigative power is a good example: ‘Tidal [as] a group of companies domiciled among other places in the USA and several European countries’ is not preconditioned on state consent because

it is not easy to tell on which server a Norwegian user’s data is stored, and the storage place may be changed over time without the user knowing or being able to control it. Although one agrees that the physical storage place is not in Norway, the state in which the data is stored at any given time may – as demonstrated in this case – be unknown.⁹⁸

Correspondingly, a gap between ‘the extent of international law’s claim to legitimate authority and the effective scope of its legitimacy’⁹⁹ may arise: just as Bianchi writes that ‘in a highly complex normative system without any centralized authority, issues of coordination and conflict among its different components are likely to arise and their solution may not be immanent’, states may resort to ‘a transparent disguise for instrumentalism based on domestic criminal law models’ as an alternative until ‘the drifting of the discipline towards a higher degree of specialization’.¹⁰⁰ In response, the human rights instruments are de facto exercising public authority, although some of the treaties that expand the scope of cyber-enabled crimes are resisting human rights inflation.¹⁰¹ For example, the European Court of Human Rights (ECtHR) in *K.U. v. Finland* indicates that the state has a positive obligation to protect a teenager who was the victim of online child pornography even when ‘any legislative shortcoming should be seen in its social context at the time’ and ‘freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected’.¹⁰² Also, the ECOWAS Court of Justice indicates in *The Incorporated Trustees of Laws and Rights Awareness Initiatives v. The Federal Republic of Nigeria* that Section 24 of the Cybercrime Act is ‘not necessary in a democratic society and disproportionately violate[s] the right to freedom of expression’ by ‘plac[ing] restrictions on freedom of expression to protect the rights of others, has established penal

⁹⁵CyberEast Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region, ‘Guidelines on the Prevention and Control of Online Fraud and Criminal Money Flows Eastern Partnership’, *Council of Europe*, 12 August 2022, available at rm.coe.int/guidelines-on-the-prevention-and-control-of-online-fraud-and-criminal-/1680a956df. Moldova has initiated withdrawal from the CIS in May 2023, but the recommendations were adopted before initiating the withdrawal. B. Eryugur, ‘Moldova to Initiate Withdrawal Procedure from CIS Parliamentary Assembly’, *Anadolu Agency*, 15 May 2023, available at www.aa.com.tr/en/asia-pacific/moldova-to-initiate-withdrawal-procedure-from-cis-parliamentary-assembly/2897842; FATF (2021), ‘Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers’, FATF, Paris, para. 111, available at www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html.

⁹⁶V. Jeutner, *Irresolvable Norm Conflicts in International Law: The Concept of a Legal Dilemma* (2017), at 33–4.

⁹⁷*Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)*, Judgment of 5 February 1970, [1970] ICJ Rep. 3, at 105 (Judge Sir Gerald Fitzmaurice, Separate Opinion).

⁹⁸*Tidal Music AS v. The Public Prosecution Authority*, [2019] HR-2019-610-A (Case No. 19-010640STR-HRET), paras. 2, 41.

⁹⁹S. Besson, ‘The Authority of International Law - Lifting the State Veil’, (2009) 31 *Sydney Law Review* 343, at 345.

¹⁰⁰A. Bianchi, ‘Looking ahead: International Law’s Main Challenges’, in D. Armstrong (ed.), *The Routledge Handbook of International Law* (2009), 392, at 404; Boister (2018), *supra* note 35, at 37.

¹⁰¹J. T. Theilen, ‘The Inflation of Human Rights: A Deconstruction’, (2021) 34(4) *LJIL* 831, at 834–5.

¹⁰²*K.U. v. Finland*, Judgment of 2 December 2008, [2008] ECHR, paras. 48–49.

punishment for conducts that it considers offensive to honor, consideration, reputation, morals, etc., with high penalties of fine . . . and imprisonment . . .¹⁰³ In a sense, the reasonings imply a move to ‘frame the issue either as a special kind of politics or as above politics’ to respond to negative effects arising from rapid advancement of digital technologies¹⁰⁴ given ‘the operative part of the final judgment [extends] far beyond the individual case identifying structural problem, [which] request[s] the respondent state party to adopt specific general and/or individual measures’.¹⁰⁵

Nevertheless, what if such a political morality for states to prioritize protection of human rights as an assumed legal ideal is simply a demand of liberal democracy for ‘an alignment of law and morality around the model of individual choice and responsibility’?¹⁰⁶ Judge Oda stated in the Separate Opinion of the *Legality of the Use by a State of Nuclear Weapons in Armed Conflict* that ‘the WHO lack the competence to submit a request for advisory opinion to the Court on the above-mentioned question, which appears not to arise “within the scope of [its] activities”’, but originates from lobbying of some non-governmental organizations (NGOs).¹⁰⁷ In this regard, constraints on sovereign power of countering cybercrime in the name of human rights protections would not necessarily resolve normative conflicts but act as ‘Western domination over the making of international law’.¹⁰⁸ let alone the Universal Declaration of Human Rights (UDHR) requires states to ‘strive . . . by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction’, heterogeneity does not obstruct ‘a harmony of interests which has a basis more real and tangible than the illusions of the sentimentalist or the hypocrisy of those satisfied with the existing *status quo*’.¹⁰⁹ Otherwise, it would be impossible to answer the question about individual duties owed to sovereignty when economic globalization directed by Western liberalism has made non-state actors instead of sovereignty the major violators of human rights.¹¹⁰

4. Global framing of ‘cybercrime’

4.1 Global incremental law-making on countering cybercrime

The current negotiating processes on cybercrime under the UN are not the first attempt of states to form a guarantee mechanism in relation to obligations and situations arising from transnational prosecution of cybercrime.¹¹¹ As early as 1998, states considered ‘developing international principles that would . . . help to combat information terrorism and criminality’ under the UN First Committee, but the decision-making processes have grown into a non-legislative act which mainly focuses on crystallizing norms that stipulate minimum standards for state behaviour in

¹⁰³*The Incorporated Trustees of Laws and Rights Awareness Initiatives v. The Federal Republic of Nigeria*, Judgment of 10 July 2020, Court of Justice of the Economic Community of West African States, No. ECW/CCJ/JUD/16/20, paras. 163–164.

¹⁰⁴B. Buzan, O. Wæver and J. de Wilde, *Security: A New Framework for Analysis* (1998), at 23.

¹⁰⁵M. Fynys, ‘Expanding Competences by Judicial Lawmaking: The Pilot Judgment Procedure of the European Court of Human Rights’, (2011) 12(5) *German Law Journal* 1231, at 1244.

¹⁰⁶I. Dennis, ‘The Critical Condition of Criminal Law’, (1997) 50(1) *Current Legal Problems* 213, at 215; A. Norrie, *Punishment, Responsibility, and Justice: A Relational Critique* (2000), 2; U. Linderfalk, ‘The Legal Consequences of Jus Cogens and the Individuation of Norms’, (2020) 33(4) *LJIL* 893, at 902–3; M. J. Perry, *Interrogating the Morality of Human Rights* (2023), 12.

¹⁰⁷*Legality of the Use by a State of Nuclear Weapons in Armed Conflict*, Advisory Opinion of 8 July 1966, [1996] ICJ Rep. 66, at 96 (Judge Oda, Separate Opinion).

¹⁰⁸C. Ryngaert, *Jurisdiction in International Law* (2015), at 205.

¹⁰⁹H. Lauterpacht, *International Law: Collected Papers* (1970), vol. 2, at 26.

¹¹⁰D. Shelton, ‘Protecting Human Rights in a Globalized World’, (2002) 25 *Boston College International & Comparative Law Review* 273, at 279.

¹¹¹This idea is enlightened by Professor Crawford’s work. J. Crawford, *Multilateral Rights and Obligations in International Law* (2007), at 364.

cyberspace.¹¹² Precisely, states did not ‘invite the Commission on Crime Prevention and Criminal Justice [CCPCJ] . . . to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations’¹¹³ until the Eleventh United Nations Congress on Crime Prevention and Criminal Justice (UNCCPCJ) in 2005. At the Twelfth UNCCPCJ, states further recognized that the United Nations Office on Drugs and Crime (UNODC) should help states ‘improve national legislation and build the capacity of national authorities . . . to deal with cybercrime’ upon request, while mandating the CCPCJ to:

consider convening an open-ended intergovernmental expert group [OEIEG] to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector . . . with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.¹¹⁴

In 2012, the Global Programme on Cybercrime (GPC) was established ‘to provide technical assistance and capacity-building on cybercrime’¹¹⁵ in response to problems specified in the Comprehensive Study on Cybercrime, including uneven criminalization of cybercrime across the countries.¹¹⁶ These activities have laid a solid foundation for the UN General Assembly to ‘establish an open-ended *ad hoc* intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes’.¹¹⁷ Up until the completion of this article, the Open-Ended Ad Hoc Intergovernmental Committee of Experts (the AHC) has held the concluding session from 29 January to 9 February 2024, but a reconvened concluding session will be held on the proposal of Mexico from 29 July to 9 August 2024.¹¹⁸

4.2 Reshaping transnational criminalization of cybercrime

4.2.1 Actor mismatch in whether a global convention on cybercrime should be shaped

Generally, the states parties to the Budapest Convention have not intended to formulate a global convention on cybercrime in contrast to those under the CIS Agreement, ACEIIS and ACCITO as specified in Figure 2.¹¹⁹

¹¹²United Nations General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/RES/53/70 (1999), at 2. Works under the First Committee have turned out to crystallize norms that stipulate minimum standard for state behaviour in cyberspace. The latest achievement under the decision-making processes is a consensus report adopted on 28 May 2021. See United Nations General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Note by the Secretary-General, UN Doc. A/76/135 (2021).

¹¹³Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.203/18 (2005), at 4.

¹¹⁴United Nations General Assembly, Annex: Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, UN Doc. A/C.3/65/L.6 (2010), at 11.

¹¹⁵United Nations Office on Drugs and Crime, Promoting Technical Assistance and Capacity-Building to Strengthen National Measures and International Cooperation Against Cybercrime, UN Doc. Res 22/8 (2013).

¹¹⁶United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (February 2013), at 77, available at www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

¹¹⁷United Nations General Assembly, Countering the Use of Information and Communications Technologies for Criminal Purposes, UN Doc. A/RES/74/247 (2020), at 1.

¹¹⁸United Nations General Assembly, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, available at www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Documents/GA_78_549_ACH_reconvened_session.pdf.

¹¹⁹Seventy-nine states voted for the proposal, 60 states voted against the proposal, 33 abstained, and 21 states did not vote. Available at digitallibrary.un.org/record/3841023.

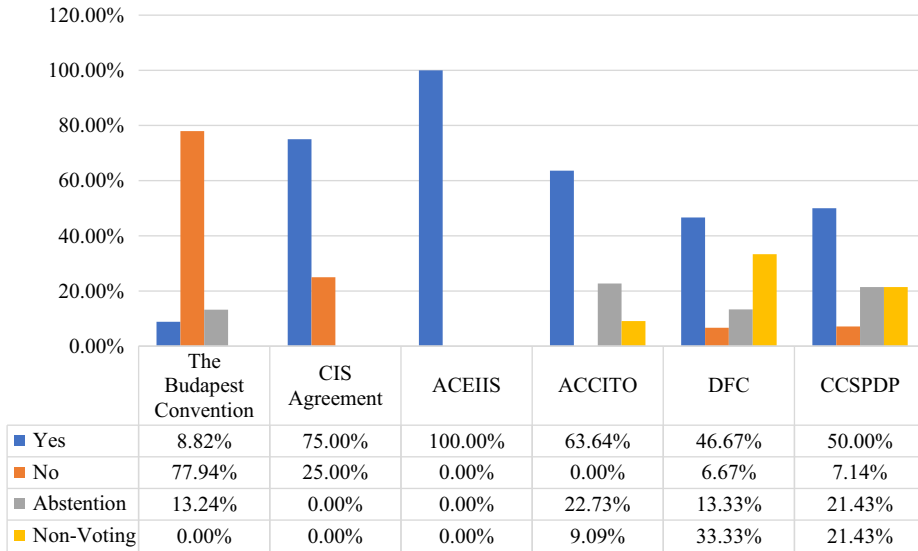


Figure 2. Voting

The unwilling participation has indicated an intention of the states to maintain the *status quo* which enables mobilization of interest groups for political advantages while preventing the proponent states from ‘legitimis[ing] and disseminat[ing] [their] foreign policy values and interests’.¹²⁰ Nevertheless, the states parties to the Budapest Convention have had a shift of position in the negotiating processes: proactive participation in different sessions may help the states to accommodate ‘pluralities of competing interests and institutional checks and balances’.¹²¹ Furthermore, lacks of political, staff, and ideational capacities have barred the states parties to the ACCITO, DFC and CCSPDP from being substantially involved in the negotiating processes, although a majority of them have recognized the necessity to formulate a global treaty on countering cybercrime:¹²² only six non-voting states – Côte d’Ivoire, El Salvador, Ghana, Mexico, Turkey, and Uruguay – have made submissions during the sessions, but they have actively participated in the inter-sessional consultations.¹²³ Additionally, diverse IOs and non-state actors have also been intensively involved in identifying what appropriate rules should be; therefore, even the less competent states may obtain information about the past and make estimates of the future for the guidance of decisions from the negotiating processes, though norm contestations could be

¹²⁰J. M. Brown and J. Urpelainen, ‘Picking Treaties, Picking Winners: International Treaty Negotiations and the Strategic Mobilization of Domestic Interests’, (2015) 59(6) *Journal of Conflict Resolution* 1043, at 1045; C. J. Fung and S-Hon Lam, ‘Mixed Report Card: China’s Influence at the United Nations’, *Lowy Institute Analysis*, 18 December 2022, available at www.lowyinstitute.org/publications/mixed-report-card-china-s-influence-united-nations. This echoes what D’Aspremont’s work which regards naming as a weapon for competing for interpretative authority: J. D’Aspremont, ‘Wording in International Law’, (2012) 25(3) *LJIL* 575.

¹²¹S. Brazys and D. Panke, ‘Why do States Change Positions in the United Nations General Assembly?’, (2017) 38(1) *International Political Science Review/Revue internationale de science politique* 70, at 79.

¹²²D. Panke, ‘Absenteeism in the General Assembly of the United Nations: Why Some Member States Rarely Vote’, (2014) 51(6) *International Politics* 729, at 745.

¹²³The lists of the states that have participated in the intersessional consultations are available at www.unodc.org/documents/Cybercrime/AdHocCommittee/First_intersessional_consultation/List_of_Participants_REV_06.04.2022_1.pdf; www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/LOP_AHC_ISC2_rev.pdf; www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_intersessional_consultation/LOP_3ISC_AHC_08112022.pdf; www.unodc.org/documents/Cybercrime/AdHocCommittee/Fourth_intersessional_consultation/LOP_4ISC_AHC_1.pdf; www.unodc.org/documents/Cybercrime/AdHocCommittee/Fifth_intersessional_consultation/LOP_-_5ISC_AHC_1.pdf.

provoked: it is still likely to culminate in a commitment through facilitating ‘those who are targets of manipulation [to] have access to information about their predispositions obtained by the agents of manipulation’.¹²⁴

4.2.2 Wrestling with framing ‘cybercrime’

According to the three consolidated negotiating documents (CNDs) produced by the AHC, states still intend to not define ‘cybercrime’ but to categorize cyber-dependent offences, cyber-enabled offences, and cyber-assisted offences.¹²⁵ First, there are diagnostic struggles across states as to whether ‘cybercrime’ must have a phenomenological transnational ‘hook’:¹²⁶ states have general consensus on proscribing illegal access, illegal interception, interference with digital system/information/devices, misuse of devices, computer-related forgery, and use of forged data in domestic criminal law, but the states parties to the Budapest Convention have insisted that those offences should be completely virtual.¹²⁷ For example, Austria indicates that transnational cyber-trespass offences should not include ‘the interception of telephone landlines that work without computers’ because ‘[s]uch an offence has no international dimension that would justify its inclusion in a UN Convention’.¹²⁸ In contrast, Russia, Iran, Belarus, Burkina Faso, Venezuela, and Egypt deem a mere transnational normative hook enough as ‘cybercrime’ should comprise a mandate to ‘establish as an offence under its domestic law the intentional creation, distribution and/or use of software or other digital information knowingly designed to interfere unlawfully with critical information infrastructure’.¹²⁹

Second, contradictions are prominent between the major states parties to the Budapest Convention and the ACEIIS/CIS Agreement in reshaping offences against the person and whether cyber-assisted offences should be established under the future global convention as specified in Table 2.¹³⁰

Most of the contentions arise from concerns that states may extend criminal penalties that exclusively serve domestic needs for addressing moral issues to the international legal system because any commitments to apply ‘criminal laws to punish the spread of [information disorder]

¹²⁴H. D. Lasswell and M. S. McDougal, *Jurisprudence for a Free Society: Studies in Law, Science and Policy* (1992), at 1175, 1187–9; T. C. Halliday and B. G. Carruthers, ‘The Recursivity of Law: Global Norm Making and National Lawmaking in the Globalization of Corporate Insolvency Regimes’, (2007) 112(4) *American Journal of Sociology* 1135, at 1152; J. D’Aspremont, ‘Non-State Actors and the Social Practice of International Law’, in M. Noortmann, A. Reinisch and C. Ryngaert (eds.), *Non-State Actors in International Law* (2015), 11, at 14.

¹²⁵Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalization and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Note by the Chair, UN Doc. A/AC.291/16 (2022).

¹²⁶See Boister, *supra* note 26, at 12; Kotiswaran and Palmer, *supra* note 26, at 70; J. Świątkowska, ‘Tackling Cybercrime to Unleash Developing Countries’ Digital Potential’, *Pathways for Property Commission*, 2020, available at pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf, at 19.

¹²⁷Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft text of the Convention, 1 September 2023, at 6–10; Statement by the Representative of Japan at the Fourth Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Agenda Item 4), available at www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Statements/Japan_4_EN.pdf.

¹²⁸Permanent Mission of Austria to the United Nations in Vienna, Statement by Austria at the Fourth Negotiating Session of the Ad-hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 10 January 2023, available at www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Statements/Austria_4_EN.pdf.

¹²⁹See Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, *supra* note 125, at 8.

¹³⁰*Ibid.*, at 18.

Table 2. Contradictions

Offences	Supporting States	Opposing States
Encouragement of or coercion to suicide	Russia, Mali, Belarus, Nicaragua, Eritrea, Venezuela, Sudan, Cuba, Burundi, DPRK, Iran, Sierra Leone.	US, Georgia, Norway, UK, Liechtenstein, Switzerland, Australia, EU, New Zealand, Israel, Lebanon.
Incitement to subversive or armed activities	The same as above plus Burkina Faso, Sudan, Egypt, Iran.	The same as above plus Canada, Dominican Republic and Guatemala, but except Switzerland.
Extremism-related offences	The same as above plus Nigeria.	
Denial, approval, justification or rehabilitation of genocide or crimes against peace and humanity	The same as above except Nigeria, Egypt, Iran.	
Terrorism-related offences	The same as above plus Egypt, Türkiye.	
Offences related to the distribution of narcotic drugs and psychotropic substances	The same as above except Türkiye.	
Offences related to arms trafficking	The same as above.	
Illegal distribution of counterfeit medicines and medical products	The same as above.	
Other unlawful acts	The same as above except Egypt and plus Iran.	
Acts threatening public safety	China, Eritrea, Russia, Venezuela, Sudan, DPRK, Lao PDR, Sierra Leone.	UK, New Zealand, US, EU, Lebanon, Norway, Liechtenstein.
Online trafficking of drugs	The same as above plus Egypt.	

... can have a chilling effect on freedom of expression'.¹³¹ For instance, the UN Human Rights Committee (UNHRC) pointed out in *Jong-Kyu Sohn v. Republic of Korea* that the state should not have applied criminal law to the persons who 'issued a statement supporting the [labour] strike and condemning the Government's threat to send in troops' because they 'w[ere] exercising [their] right to impart information and ideas within the meaning of article 19, paragraph 2, of the Covenant'.¹³² Nevertheless, attempts to expand the scopes of offences against the person and cyber-assisted offences may enable states to seek global legitimacy for using criminal law to compensate for institutional incapacity to respond to lesser cybercrime with low penalties at the domestic level, although potential duplication with other international rules and norms could come about.¹³³ In this regard, the critical issue does not lie in whether states may apply criminal law to those offences but concerns how to make state interventions 'become fully effective'¹³⁴ without 'put[ting] in jeopardy the right itself'.¹³⁵ digital technology has been reshaping the ability of individuals worldwide to exercise their freedom of expression, which has multiplied commitments on human rights protection through coercion and persuasion.¹³⁶ Notwithstanding, what if states are using human rights law to disguise accommodation of political agendas such as election interference, which 'would undermine the rights of others or the ability of States to protect legitimate national security or public order interests'?¹³⁷ For example, the UNHRC reasoned that the criminal conviction of a journalist who disclosed political opinion polls for the 23-day period running up to and including election day was not excessive.¹³⁸ After all, criminal law is the last

¹³¹See Ashworth and Horder, *supra* note 14, at 29; Human Rights Council, *supra* note 75, at 10–11.

¹³²Human Rights Committee, *Jong-Kyu Sohn v. Republic of Korea*, Communication No. 518/1992, UN Doc. CCPR/C/50/D/518/1992 (Decision on admissibility, dated 18 March 1994), paras. 2.1, 10.3.

¹³³See Ashworth and Horder, *supra* note 14, at 29; Australia, Japan, and Mexico have made arguments like that. See Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Compilation of Proposals and Contributions Submitted by Member States on the Provisions on Criminalization, the General Provisions and the Provisions on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/9 (2022), at 4, 36, 45; Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Compilation of Proposals and Contributions Submitted by Member States on the Provisions on Criminalization, the General Provisions and the Provisions on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, A/AC.291/9/Add.2 (2022), at 32.

¹³⁴Office of the High Commissioner for Human Rights, CCPR General Comment No. 11: Article 20 Prohibition of Propaganda for War and Inciting National, Racial or Religious Hatred, 29 July 1983, para. 2.

¹³⁵Human Rights Committee, General Comment No.34 on Article 19: Freedom of Opinion and Expression, UN Doc. CCPR/C/GC/34 (2011), at 5.

¹³⁶Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Note by the Secretariat, UN Doc. A/HRC/38/35 (2018), at 19; E. M. Hafner-Burton, *Making Human Rights a Reality* (2013), at 60–6.

¹³⁷S. J. Barela and J. Duberry, 'Understanding Disinformation Operations in the Twenty-First Century', in D. B. Hollis and J. David Ohlin (eds.), *Defending Democracies: Combating Foreign Election Interference in a Digital Age* (2021), 41, at 42–8; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Note by the Secretariat, A/HRC/38/35 (2018), at 15. Barrie Sander proposes that international human rights law should not insist on the negative obligation of states to refrain from unjustifiably interfering with the right to freedom of expression but on the positive obligation to protect freedom of expression and on balancing power asymmetry between individuals, social media platforms and states. Nevertheless, this proposal is workable when a state has strong regulatory regime and robust digital capacity, but most of the developing countries lack these two conditions. See B. Sander, 'Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law', (2021) 32(1) *European Journal of International Law* 159, at 192–3.

¹³⁸*Kim Jong-Cheol v. Republic of Korea*, Communication No. 968/2001, UN Doc. CCPR/C/84/D/968/2001 (2005), para. 8.3.

resort for a state to undertake its positive obligation to obstruct ‘hostility, violence, discrimination, or exclusion by others’¹³⁹ arising from ‘the soul-shriveling humiliation that a discriminatory rebuff can give rise to’.¹⁴⁰

4.2.3 Decreasing indeterminacy in criminal liability and condition of cybercrime

In general, states have mitigated the significant divide in prescribing the liability and condition of ‘cybercrime’ under the pre-existing treaties during the negotiations: states have agreed on the necessity to criminalize ‘attempt’ and ‘complicity’ as well as prescribe ‘intent’ in committing cybercrime at the domestic level, although the broad expressions such as ‘the participation in any capacity’ and ‘any attempt’ as well as a demand for not ‘imposing an unnecessary burden of translation and explanation’ to *mens rea*¹⁴¹ provide little guidance for states to substantively harmonize a requirement of ‘evil mind’ as well inchoate and derivative liabilities in domestic criminal law.¹⁴² For example, Niger, Malaysia, Indonesia, Vietnam, and Tanzania propose that ‘[k]nowledge, intent or purpose required as an element of an offence established in accordance with this Convention may be inferred from objective factual circumstances’.¹⁴³ In practice, the convergences could facilitate assertion of criminal jurisdiction over regulating cybercrime without resolving jurisdictional conflicts, especially in terms of jurisdictional overreach where ‘different sovereigns may bring successive prosecutions for ... different offences’ arising from one incident:¹⁴⁴ improvement in semantic determinacy does not necessarily resolve structural indeterminacy which emerges from tensions between a quest for common values and the basic need to maintain independence in the international society.¹⁴⁵ For example, the US District Court for the Eastern District of New York in the *United States v. Augustine* case reasoned that prosecution of the defendant for attempting to provide personnel to a Federal Terrorist Organization (FTO) after prior prosecution by the Tunisian court proceedings has been justifiable by ‘the dual sovereignty principle’.¹⁴⁶ In this regard, over-criminalization could happen, especially when circumstantial evidence may justify actions against or even punishment of conducts tangential to serious and organized crimes in cyberspace.¹⁴⁷

4.3 Appraisal

The aforementioned analyses suggest that states have certain consensus on operational rules for taking joint action on cybercrime in the midst of ‘pluralities of competing interests and

¹³⁹J. Waldron, *The Harm in Hate Speech* (2012), at 4.

¹⁴⁰*Ibid.*, at 84. Professor Husak recognizes that ‘the criminal law should be used only as a last resort to prevent given kinds of conduct. If non-criminal means to prevent the conduct in question as well or better, the criminal sanction should not be employed’. See D. Husak, ‘The Criminal Law as Last Resort’, (2004) 24(2) *Oxford Journal of Legal Studies* 207, at 217.

¹⁴¹Supreme Court of Canada, *R. v. Legare*, 2009 SCC 56, [2009] 3 S.C.R. 551 (2009).

¹⁴²M. T. Cahill, ‘Inchoate Crimes’, in M. D. Dubber and T. Hörnle (eds.), *The Oxford Handbook of Criminal Law* (2014), 641, at 641; J. G. Stewart, ‘Complicity’, in *ibid.*, at 682.

¹⁴³Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Consolidated Negotiating Document on the General Provisions and the Provisions on Criminalization and on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Status as of 21 January 2023), Art. 37.

¹⁴⁴J. Hörnle, *Internet Jurisdiction: Law and Practice* (2021), at 82, 108.

¹⁴⁵M. Koskeniemi, *From Apology to Utopia: The Structure of International Legal Argument* (2005), at 59–70.

¹⁴⁶*United States v. Augustine*, 18 CR 393 (SJ) (RML) (E.D.N.Y. 2021).

¹⁴⁷A. Ashworth, ‘Conceptions of Overcriminalization’, (2008) 5 *Ohio State Journal of Criminal Law* 407, at 413; The Secretary of State for the Home Department, *Serious and Organised Crime Strategy* (November 2018), available at assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752850/SOC-2018-web.pdf.

institutional checks and balances'.¹⁴⁸ Nevertheless, the diagnostic struggles and contradictions suggest that the pre-existing treaties have failed to nurture a wide agreement among states to couch the disputed issues concerning cybercrime in certain specific terms due to a lack of principled foreign policy to prevent states from 'us[ing] their control of implementation to undermine and subvert legal changes'.¹⁴⁹ In this respect, the negotiations may not go beyond cultivating an exceptional and extended compromise resting on the prior treaties as justifications for countering cybercrime transnationally as the UN may only enable states to strategically get to the best outcome out of irreconcilable issues.¹⁵⁰ just as Professor Crawford writes that 'treaties are time-bound promises or propositions that generally reflect a perspective at the time of being made. But we know that over time custom may actually be employed to "mould and even modify" the content of otherwise static treaties',¹⁵¹ it is likely that states would reach acceptable trade-offs concerning most of the cyber-dependent offences and certain cyber-enabled offences, such as child pornography, by continuous inquiry that may 'help each party understand the realities the other is working with'.¹⁵² In particular, Australia, Mexico, China, the UK, and others have agreed that private actors play a significant role in addressing cybercrime, although China favours hierarchical governance by underlining that states should 'clarify the responsibilities of the private sector' while the UK appreciates co-governance by 'reach[ing] inter-subjective understanding' of collaboration.¹⁵³ Therefore, it is likely to persuade or provide alternative policy options for Austria to accept that 'the interception of telephone landlines that work[s] without computers' is culpable given that the affinal relationship between cybercrime and ICT has been well recognized.¹⁵⁴

Nevertheless, global collective action against cybercrime will still be a slim chance unless 'both the identity and preferred distribution pattern of basic goal values, and implementing institution' are well allocated to balance sovereign prerogatives and the need to maintain co-existence of states.¹⁵⁵ First, does a demand for global collective action against cybercrime justify a need for observing a universal set form of calculus for determining what degree of reducing harms is required and what socially acceptable levels of risk are?¹⁵⁶ The answer is substantially 'no' because even a common concern does not *ipso facto* prevail over a state's entitlements. The ECtHR's ruling in *Al-Adsani v. The United Kingdom* is one example: a state's right to enjoy 'immunity from civil suit in the courts of another State where acts of torture are alleged' remains intact, even when the

¹⁴⁸S. Brazys and D. Panke, 'Why do States Change Positions in the United Nations General Assembly?', (2017) 38(1) *International Political Science Review/Revue internationale de science politique* 70, at 79; A. Stimmer, 'Beyond Internalization: Alternate Endings of the Norm Life Cycle', (2019) 63 *International Studies Quarterly* 270, at 272.

¹⁴⁹See Halliday and Carruthers, *supra* note 124, at 1152.

¹⁵⁰R. A. Falk, 'The United Nations: Various Systems of Operation', in L. Gordenker (ed.), *The United Nations in International Politics* (1971), 184, at 200; G. Sjostedt, B. I. Spector and I. W. Zartman, 'The Dynamics of Regime-Building Negotiations', in B. I. Spector, G. Sjostedt and I. W. Zartman (eds.), *Negotiating International Regimes: Lessons Learned from the United Nations Conference on Environment and Development (UNCED)* (1994), 3, at 9; R. E. Webber Gaudiosi, J. Leiva-Roesch and Y-M. Wu, *Negotiating at the United Nations: A Practitioner's Guide* (2019), at 71.

¹⁵¹J. Crawford, *Chance, Order, Change: The Course of International Law* (2014), at 143.

¹⁵²See Gaudiosi, Leiva-Roesch and Wu, *supra* note 150, at 27.

¹⁵³Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Compilation of views submitted by Member States on the Scope, Objectives and Structure (Elements) of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Note by the Secretariat, UN Doc. A/AC.291/4 (2021), at 14, 61; J. Kooiman, *Governing as Governance* (2003), at 101, 115–18.

¹⁵⁴C. Grobe, 'The Power of Words: Argumentative Persuasion in International Negotiations', (2010) 16(1) *European Journal of International Relations* 5, at 22.

¹⁵⁵M. S. McDougal and H. D. Lasswell, 'The Identification and Appraisal of Diverse Systems of Public Order', (1959) 53 *American Journal of International Law* 1, at 10; D. Kennedy, 'The Disciplines of International Law and Policy', (1999) 12 *LJIL* 1, at 127; A. Hertogen, 'Letting Lotus Bloom', (2015) 26(4) *European Journal of International Law* 901, at 904, 918–20.

¹⁵⁶See Ashworth and Zedner, *supra* note 84, at 5.

prohibition of torture ‘has achieved the status of a peremptory norm in international law’.¹⁵⁷ Similarly, the ICJ in the *Whaling in the Antarctic* case implied that the exercise of international law should have deference to national disparities by refusing to settle differences about the appropriate policy towards whales and whaling at the domestic level.¹⁵⁸ In this regard, either criminalization of hate speech or reconstruction of conventional crimes as ‘cybercrime’ should still be *domaine réservé* as long as states observe proportionality when imposing deterrence, although ‘[t]here is no uniformity . . . in the practice or the doctrine as to the formulation of the principle, the strictness or flexibility of the principle and the criteria on the basis of which proportionality should be assessed’.¹⁵⁹ Essentially, liberty is socially embedded and ‘can be evaluated from the perspectives of a variety of normative orders or normative control systems and thus, importantly, can also be justified from a variety of such perspectives’.¹⁶⁰ It is justifiable to subordinate individual interests to the goals of their collective or ingroups with the purpose of preserving a democratic political community and individual rights without sufficient state capacity.¹⁶¹

Second, what is ‘the extent to which and the methods by which states can pursue any national-culturally determined goals in the international society’?¹⁶² The requirements for human rights protection and democratic principles have restrained state autonomy since 1945, but such a constraint does not extend to prescribe how a state should provide a range of acceptable options to achieve individual full potential:¹⁶³ what the *Lotus* case requires has long been a duty of each state to maintain ‘co-existence of independent communities and facilitate the achievement of common aims’.¹⁶⁴ In this respect, the duties discourse as recognized by certain regional human rights regimes should also be well noted.¹⁶⁵ For example, Article 29 of the African Charter on Human and Peoples’ Rights requires that ‘[t]he individual shall have the duty . . . [n]ot to compromise the security of the State whose national or resident he is’. Also, Paragraph 2, Principle 23 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted by the African Commission on Human and Peoples’ Rights (ACHPR)¹⁶⁶ reaffirms that ‘individual rights . . . originate from, and acquire existence, effectiveness and significance in, the context of

¹⁵⁷ *Al-Adsani v. The United Kingdom*, Judgment of 21 November 2001, [2001] ECHR, at 4–6, 19. The ICJ also indicates that ‘the prohibition of torture is part of customary international law and it has become a peremptory norm (jus cogens)’. See *Questions Relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal)*, Judgment of 20 July 2012, [2012] ICJ Rep. 422, at 457.

¹⁵⁸ *Whaling in the Antarctic (Australia v. Japan: New Zealand intervening)*, Judgment of 31 March 2014, [2014] ICJ Rep. 226, at 254.

¹⁵⁹ O. Gross and F. Ni Aoláin, *Law in Times of Crisis: Emergency Powers in Theory and Practice* (2006), 252; see Ashworth and Zedner, *supra* note 84, at 19; Report of the International Law Commission on the Work of its Forty-Seventh Session, 2 May–21 July 1995, Official Records of the General Assembly, Fiftieth session, Supplement No.10, UN Doc. A/50/10 (1995), at 65.

¹⁶⁰ J. Rawls, *A Theory of Justice* (1999), 55–6; J. Klabbbers and To. Piiparinen, ‘Normative Pluralism: An Exploration’, in J. Klabbbers and T. Piiparinen (eds.), *Normative Pluralism and International Law: Exploring Global Governance* (2013), 13, at 14.

¹⁶¹ M. Erez and P. C. Earley, *Culture, Self-Identity, and Work* (1993), 78; E. R. Boot, *Human Duties and the Limits of Human Rights Discourse* (2017), at 30.

¹⁶² W. Levi, ‘International Law in a Multicultural World’, (1974) 18(4) *International Studies Quarterly* 417, at 445–6.

¹⁶³ See Crawford, *supra* note 111, at 389; S. Fredman, *Human Rights Transformed: Positive Rights and Positive Duties* (2008), at 65–6.

¹⁶⁴ *SS Lotus (France v. Turkey)*, PCIJ Rep Series A No 10, at 21; P. Weil, ‘The Court Cannot Conclude Definitively . . . Non Lique Revisited’, (1998) 36 *Columbia Journal of Transnational Law* 109, at 112; A. Hertogen, ‘Letting Lotus Bloom’, (2016) 26(4) *European Journal of International Law* 901, at 912.

¹⁶⁵ United Nations General Assembly, Draft International Declaration of Human Rights–Recapitulation of Amendments to Article 27 of the Draft Declaration (E/800), UN Doc. A/C.3/304 /Rev.2 (1948).

¹⁶⁶ Principle 23 Prohibited Speech: . . . 2. States shall criminalise prohibited speech as a last resort and only for the most severe cases. In determining the threshold of severity that may warrant criminal sanctions, States shall take into account the: a. prevailing social and political context; b. status of the speaker in relation to the audience; c. existence of a clear intent to incite; d. content and form of the speech; e. extent of the speech, including its public nature, size of audience and means of dissemination; f. real likelihood and imminence of harm.

collective rights'.¹⁶⁷ Therefore, a state may discard the idea that 'the individual achieves her full freedom only when untrammelled by State and community regulation'¹⁶⁸ but turn to a rationale that '[t]he fulfilment of duty by each individual is a prerequisite to the rights of all' as long as the state's intention is to sustain human relationships and individual identity.¹⁶⁹ In a word, just as the ICJ in the *Application of the International Convention on the Elimination of All Forms of Racial Discrimination* case refuses to recognize its jurisdiction *ratione materiae* on 'alleged "indirect discrimination" resulting from the effect of the media block on persons of Qatari national origin' on the ground that media corporations are not "institutions" which 'refers to collective bodies or associations . . . [as] individuals or groups of individuals',¹⁷⁰ not any of the ideologies across different cultures but 'the international reaction to the genocide and atrocities committed by National Socialist Germany' should be the only constraint on state behaviour at the universal level.¹⁷¹

5. Positioning 'cybercrime' in the pluralist legal order

This section discusses the implications emerging from the evolution of 'cybercrime' on the international plane. This author will then propose an alternative to mediate the diversity of the international society.

5.1 Is protection from cybercrime an emerging common interest of the international society?

Stepping beyond the unresolved tension between states in the processes of global (re-)framing of 'cybercrime', it is clear that 'a common sense of nations' that protection from cybercrime demands active co-operation beyond the simple precept of coexistence: it is necessary to form a community in law in quest for common values, higher norms, and objective responsibility in terms of countering cybercrime.¹⁷² In other words, states are seeking an *erga omnes partes* obligation in the midst of traditionally bilateralist international law: a state has an obligation of imposing criminal sanctions on offences in cyberspace, which objectively owes to all the other parties under the prospective regime.¹⁷³ Alternatively, a 'general principle' which is logically connected with the phenomenon of 'cybercrime' has emerged to 'establish the existence of a legal principle that has a general scope and may be applied to a situation not initially envisaged by the rules from which it was derived'.¹⁷⁴ In this regard, what contradictory practice reflects is not a lack of 'acceptance as

¹⁶⁷*Sawhoyamaya Indigenous Community v. Paraguay*, Judgment of 29 March 2006, [2006] IACHR, para. 11 (Judge García-Ramírez, Separate Opinion).

¹⁶⁸See Fredman, *supra* note 163, at 62.

¹⁶⁹The Preamble of the American Declaration of the Rights and Duties of Man; see Fredman, *ibid.*, at 65–6.

¹⁷⁰*Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Qatar v. United Arab Emirates)*, Preliminary Objections, Judgment of 4 February 2021, [2021] ICJ Rep. 71, at 106–7.

¹⁷¹J. Mende, 'Are Human Rights Western—And Why does it Matter? A Perspective from International Political Theory', (2021) 17(1) *Journal of International Political Theory* 38, at 40.

¹⁷²M.-C. Cordonier Segger and A. Khalfan, *Sustainable Development Law: Principles, Practices and Prospects* (2004), xi; A. A. Cançado Trindade, *International Law for Humankind: Towards a New Jus Gentium* (2010), 4; R. Wolfrum, 'Identifying Community Interests in International Law: Common Spaces and Beyond', in E. Benvenisti and G. Nolte (eds.), *Community Interests Across International Law* (2018), 19, at 22; S. Thin, 'Community Interest and the International Public Legal Order', (2021) 68 *Netherlands International Law Review* 35, at 43–53.

¹⁷³See *Questions relating to the Obligation to Prosecute or Extradite case*, *supra* note 157, at 449. See also B. Simma, *From Bilateralism to Community Interest in International Law (Volume 250)* (1994), at 230.

¹⁷⁴International Law Commission, Second Report on General Principles of Law by Marcelo Vázquez-Bermúdez, Special Rapporteur, A/CN.4/741 (2020), at 49, 53; C. Voigt, 'Delineating the Common Interest in International Law', in W. Benedek et al. (eds.), *The Common Interest in International Law* (2014), 9, at 14; N. Oral, 'The Global Commons and Common Interests: Is there Common Ground?', in M. Iovane et al. (eds.), *The Protection of General Interests in Contemporary International Law: A Theoretical and Empirical Inquiry* (2021), 13, at 28.

law' about countering cybercrime but about what operationalized regime is appropriate.¹⁷⁵ The developing states are avoiding yielding 'the armed governing apparatus of the sovereign and . . . the rich resources of the state[s]'¹⁷⁶ to increasing inter-dependence,¹⁷⁶ while the developed states have turned to democratizing and humanizing international law to overcome a structural problem inherent in the international society where even commitments to realize common good are essentially contractual.¹⁷⁷ George Abi-Saab indicated that:

the traditional view staunchly held in Western quarters, that a new State is born in a legal universe that binds it . . . [but] the alleged universality and legitimacy of the international legal system [is] a system developed without their participation and used to justify their subjugation; an unjust system, for whilst formally based on sovereign equality and hence reciprocity, in actuality it works in one direction and in favour of one side only; and finally an antiquated system that does not correspond to contemporary conditions and their specific needs.¹⁷⁸

Accordingly, '[t]he interest of the community . . . is [still] . . . the sum of the interests of the several members who compose it':¹⁷⁹ the winner would be able to create an imposed regime which would enable the introduction of "'alien" doctrines . . . [that] require[s] fundamental change of domestic principles of participation and obligations',¹⁸⁰ which could deprive certain other states of 'undertakings possessing their own value and consequently are capable of independent application'.¹⁸¹ Otherwise, conflicts would arise from resistance of the affected states just as China had tried to regain control and ownership of her territory through tactically declaring war on Germany in 1917.¹⁸²

Notwithstanding, a global demand for 'all States can be held to have a legal interest in their protection' still contributes to producing 'transboundary moral impacts':¹⁸³ just as Nardin recognizes that '[d]urable relations among adversaries presuppose a framework of common

¹⁷⁵This is similar with Villalpando's proposition that 'the identification of a rule or mechanism that ensures that the individual interest concerned be sacrificed only in those instances where this is justified by the preservation of the common good' is the core problem of protecting a community interest. See S. Villalpando, 'The Legal Dimension of the International Community: How Community Interests Are Protected in International Law', (2010) 21(2) *European Journal of International Law* 387, at 417.

¹⁷⁶M. Brus, 'Bridging the Gap Between State Sovereignty and International Governance: The Authority of Law', in G. Kreijen et al. (eds.), *State, Sovereignty, and International Governance* (2002), 3, at 10; E. C. Ip, 'Globalization and the Future of the Law of the Sovereign State', (2010) 8(3) *International Journal of Constitutional Law* 636, at 653.

¹⁷⁷T. Sato, 'Legitimacy of International Organizations and their Decisions – Challenges that International Organizations Face in the 21st Century', (2009) 37 *Hitotsubashi Journal of Law and Politics* 11, at 15; Y. Tanaka, 'Protection Community Interests in International Law: The Case of the Law of the Sea', (2011) 15 *Max Planck Yearbook of United Nations Law* 329, at 339 et seq; G. Oberleitner, *Human Rights in Armed Conflict: Law, Practice, Policy* (2015), 232; J. von Bernstorff, 'New Responses to the Legitimacy Crisis of International Institutions: The Role of "Civil Society" and the Rise of the Principle of Participation of "The Most Affected" in International Institutional Law', (2021) 32(1) *European Journal of International Law* 125.

¹⁷⁸G. Abi-Saab, 'The Third World Intellectual in Praxis: Confrontation, Participation, or Operation Behind Enemy Lines?', (2016) 37 *Third World Quarterly* 1957, at 1958–9.

¹⁷⁹J. W. Dacyl, 'Sovereignty versus Human Rights: From Past Discourses to Contemporary Dilemmas', (1996) 9(2) *Journal of Refugee Studies* 136, at 158; J. Bentham, *An Introduction to the Principles of Morals and Legislation* (2000), para. IV; R. Domingo, 'The New Global Human Community', (2012) 12(2) *Chicago Journal of International Law* 563, at 583; S. Besson, 'Community Interests in International Law: Whose Interests Are They and How Should We Best Identify Them?', in E. Benvenisti and G. Nolte (eds.), *Community Interests Across International Law* (2018), 36, at 38.

¹⁸⁰See Boister (2018), *supra* note 35, at 26.

¹⁸¹R. Müllerson, *Dawn of a New Order: Geopolitics and the Clash of Ideologies* (2017), 77; *Customs Régime Between Germany and Austria (Protocol of March 19th, 1931)*, PCIJ Series A/B, No 41, 37 at 49.

¹⁸²'China's Declaration of War on Germany and Austria-Hungary, August 14, 1917', (1920) 5 *Chinese Social & Political Science Review* 100; T. E. La Frague, 'The Entrance of China into the World War', (1936) 5(3) *Pacific Historical Review* 222, at 222; S. G. Craft, 'Angling for an Invitation to Paris: China's Entry into the First World War', (1994) 16(1) *The International History Review* 1, at 21.

¹⁸³See *Barcelona Traction, Light and Power Company, Limited* case, *supra* note 97, at 32.

practices and rules capable of providing some unifying bond where shared purposes are lacking',¹⁸⁴ the global negotiations still 'render events or occurrences meaningful and thereby function to organize experience and guide action' against cybercrimes across borders.¹⁸⁵ In a word, what states demand is to be emancipated from 'hierarchical relations of domination and subordination'¹⁸⁶ and to 'accept a range of different and equally legitimate normative choices by national governments and international institutions and tribunals ... within the context of a universal system'.¹⁸⁷ The ICJ articulates in the *Military and Paramilitary Activities in and against Nicaragua* case that '[t]he existence in the *opinio juris* of States of the principle of non-intervention is backed by established and substantial practice. It has moreover been presented as a corollary of the principle of the sovereign equality of States'.¹⁸⁸

5.2 Is seeking a minimum public order a solution?

Eventually, a more profound question arises: what are the more advantageous alternatives to mediate claims and counter-claims in the global framing of 'cybercrime'? The failure of the International Convention Concerning the Use of Broadcasting in the Cause of Peace (ICCUBCP) concluded under the League of Nations in 1936 can provide some enlightenment.¹⁸⁹ During the interwar period, states made deep commitments to regulate information flow to prevent 'the detriment of good international understanding ... as to incite the population of any territory to acts incompatible with the internal order or the security of a territory of a High Contracting Party'.¹⁹⁰ Nevertheless, the International Convention Concerning Use of Broadcasting in the Cause of Peace (ICCUBCP) was barely operative due to a lack of 'a public order system in which the basic values of human dignity are widely produced and widely shared'.¹⁹¹ states such as Spain and the Soviet Union thought it either premature to implement at the domestic level or impossible to apply without like-mindedness.¹⁹² Eventually, the ICCUBCP collapsed without curbing broadcast propaganda which conspired in the outbreak of the Second World War.¹⁹³ Just as Professor Müllerson observes that '[d]ominance is rarely voluntarily accepted',¹⁹⁴ the ICCUBCP's destiny foreshadows potential outcomes of the future global convention on countering cybercrime.

In this regard, any attempts to shape 'cybercrime' at the global level should not go beyond 'the maintenance or re-establishment of minimum order and, then, within the social space created by the maintenance of minimum order, to the optimum ways in which all life opportunities are produced and distributed'.¹⁹⁵ Otherwise, it is unlikely to crystallize 'the highest common

¹⁸⁴T. Nardin, *Law, Morality, and the Relations of States* (1983), 5.

¹⁸⁵R. D. Benford and D. A. Snow, 'Framing Processes and Social Movements: An Overview and Assessment', (2000) 26 *Annual Review of Sociology* 611, at 614.

¹⁸⁶G. J. Ikenberry, *Liberal Leviathan: The Origins, Crisis, and Transformation of the American World Order* (2011), 24.

¹⁸⁷W. W. Burke-White, 'International Legal Pluralism', (2004) 25 *Michigan Journal of International Law* 963, at 977.

¹⁸⁸*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14, at 106.

¹⁸⁹S. J. Potter, 'Broadcasting in the Cause of Peace: Regulating International Radio Propaganda in Europe, 1921–1939', (2023) *International History Review* 1, at 10–11.

¹⁹⁰Inter-Governmental Conference for the Adoption of a Convention Concerning the Use of Broadcasting in the Cause of Peace (Geneva, 17–23 September 1936), 17 League of Nations O. J. 1437 (1936), Art. 1.

¹⁹¹E. Suzuki, 'Self-Determination and World Public Order: Community Response to Territorial Separation', (1976) 16(4) *Virginia Journal of International Law* 779, at 792.

¹⁹²E. A. Downey, 'A Historical Survey of the International Regulation of Propaganda', (1984) 5(1) *Michigan Journal of International Law* 341, at 344.

¹⁹³S. J. Potter, 'Broadcasting in the Cause of Peace: Regulating International Radio Propaganda in Europe, 1921–1939', (2023) *International History Review* 1, at 17.

¹⁹⁴See Müllerson, *supra* note 181, at 59.

¹⁹⁵W. M. Reisman, *The Quest for World Order and Human Dignity in the Twenty-First Century: Constitutive Process and Individual Commitment* (2012), 350.

denominator of relevant rules':¹⁹⁶ it is unrealistic to 'format . . . norms and values coming from different cultures and religions into a common paradigm of legal norms and principles',¹⁹⁷ when dominators seek perpetual domination and the dominated seeks to 'join or replace the dominators'.¹⁹⁸ For example, states such as the US, China, Russia, Iran, and others are abusing public attribution to compete for normative power in cyberspace, which further escalates tension in the international society due to lack of consensus and guidance.¹⁹⁹ Therefore, global framing of cybercrime should head for a satisfactory arrangement through subsequent improvements rather than delimiting the morally permissible range of diversity among states that cannot exercise their right on an equal footing.²⁰⁰ It is more just and practical to require states to observe procedural obligations such as periodical information sharing and reporting of accountability in accordance with agreed rules,²⁰¹ which 'place in juxtaposition quite divergent diagnoses and prescriptions for action . . . [and] allow implementing nations to follow quite divergent courses of action while each appeals to the same global norms'.²⁰² Judge Huber indicated that '[s]overeignty in the relations between States signifies independence . . . [which] is the right to exercise therein, to the exclusion of any other State, the functions of a State',²⁰³ a pressing need to jointly combat cybercrime and the globality of cyberspace does not equate to rendering states 'the right to intervene in the internal or external affairs of another',²⁰⁴ and to compel states to give up *domaine privilégié* that concerns protection of political organizations, internal and external security, and major economic interests.²⁰⁵ After all, consensus is not necessarily preconditioned by institutionalization of power just as Colombia as a non-party still recognizes the relevant provisions of the United Nations Convention on the Law of the Sea concerning the baselines of a coastal state and its entitlement to maritime zones, the definition of the continental shelf and the provisions relating to the delimitation of the exclusive economic zone and the continental shelf as applicable due to their role as customary international law.²⁰⁶ The essential features retained in the public order system of today still underpin new developments in the future and state consent is indispensable to resolve normative conflicts in a highly complex normative system without any centralized authority.²⁰⁷

¹⁹⁶G. Schwarzenberger, *The Fundamental Principles of International Law (Volume 87)* (1955), 195.

¹⁹⁷O. Roy and P. Annicchino, 'Human Rights between Religions, Cultures, and Universality', in A. F. Vrdoljak (ed.), *The Cultural Dimension of Human Rights* (2013), 13, at 24.

¹⁹⁸See Müllerson, *supra* note 181, at 60.

¹⁹⁹H. Lee, 'Public Attribution in the US Government: Implications for Diplomacy and Norms in Cyberspace', (2023) 6(2) *Policy Design and Practice* 198, at 207–12.

²⁰⁰See Reisman, *supra* note 195, at 352; G. E. Sherman, 'Jus Gentium and International Law', (1918) 12(1) *American Journal of International Law* 56, at 58–9; S. R. Ratner, *The Thin Justice of International Law: A Moral Reckoning of the Law of Nations* (2015), 23, 89–90; C. R. Beitz, *Political Theory and International Relations* (1979), 56; B. Barry, 'International Society from a Cosmopolitan Perspective', in D. R. Mapel and T. Nardin (eds.), *International Society: Diverse Ethical Perspectives* (1998), 144, at 154.

²⁰¹C. Voigt, 'The Power of the Paris Agreement in International Climate Litigation', (2023) 32(2) *Review of European, Comparative & International Environmental Law (RECIEL)* 237, at 239.

²⁰²See Halliday, *supra* note 26, at 280.

²⁰³*The Island of Palmas Case (or Miangas) (United States of America v. The Netherlands)*, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4 April 1928, at 8.

²⁰⁴Montevideo Convention on the Rights and Duties of States, 49 Stat. 3097 (1919–1936) (1933), Art. 8.

²⁰⁵T. Moulin, 'Revising the Principle of Non-Intervention in Cyberspace: The Path Forward', (2020) 25(3) *Journal of Conflict & Security Law* 423, at 437.

²⁰⁶*Territorial and Maritime Dispute (Nicaragua v. Colombia)*, Judgment of 19 November 2012, [2012] ICJ Rep. 624, at 666.

²⁰⁷M. S. McDougal, H. D. Lasswell and J. C. Miller, *The Interpretation of Agreements and World Public Order: Principles of Content and Procedure* (1967), 379; see Simma, *supra* note 173, at 230; Boister (2018), *supra* note 35, at 37.

6. Conclusion

This article has observed and analysed transnational criminalization of cybercrime under the treaties and global negotiations under the UN. The observations show that a common interest of preserving peace and security in cyberspace through criminal justice is crystallizing in operation amid divergences of states on framing ‘cybercrime’, but such a global aspiration to develop an optimum public order that promotes the greater production and wider distribution of all values is still utopian.²⁰⁸ Simultaneously, states should secure the duties to co-operate and avoidance of harm first when there is no ‘unified society of states adhering to generally the same norms, rules, identities, and views of moral conduct’:²⁰⁹ a collection of ‘self-contained bod[ies] of law or legal system[s], the sum-total of norms, indicating the proper rules of obligatory conduct, binding on members of a law-governed human society’²¹⁰ is not all about the international legal order for maintaining co-existence of states and upholding human dignity. Therefore, the hope of the states to delegate the League of Nations to maintain peace and international security was doomed to disillusion without paying attention to ‘the possibility of integrating them in a lasting political and economic order’.²¹¹ Analogically, transnational criminalization is not ‘a status quo project of legitimation . . . for those who might otherwise have contributed to a new global politics’²¹² by exercising special privileges upon some states with a limited capacity for rights in international law.²¹³ After all, the UN’s ‘values-based framework’ may not serve other than to ‘ensure . . . all the threats . . . that are distant do not become imminent and those that are imminent do not actually become destructive’.²¹⁴

²⁰⁸M. S. McDougal and F. P. Feliciano, *Law and Minimum World Public Order: The Legal Regulation of International Coercion* (1961), 319.

²⁰⁹D. C. Ellis, ‘On the Possibility of “International Community”’, (2009) 11(1) *International Studies Review* 1, at 4; E. B. Weiss, *Establishing Norms in a Kaleidoscopic World* (2020), at 147.

²¹⁰D. Lee, *The Right of Sovereignty: Jean Bodin on the Sovereign State and the Law of Nations* (2021), 74.

²¹¹C. De Visscher, *Theory and Reality in Public International Law* (1957), 53–5.

²¹²D. Kennedy, ‘The International Human Rights Regime: Still Part of the Problem?’, in R. Dickinson et al. (eds.), *Examining Critical Perspectives on Human Rights* (2012), 19, at 33.

²¹³H. Suganami, ‘Grotius and International Equality’, in H. Bull, B. Kingsbury and A. Roberts (eds.), *Hugo Grotius and International Relations* (1990), 221, at 227.

²¹⁴United Nations General Assembly, Note by the Secretary-General, A/59/565 (2004), at 12. Many works have shown that the UN has shared many ideological traits with the League of Nations which ‘was not a machine for global democracy intended to bring political independence to the rest of the world, or to dismantle the European colonial empires’. See M. Mazower, *No Enchanted Palace: The End of Empire and the Ideological Origins of the United Nations* (2009), 86. See also A. Zimmern, *The League of Nations and the Rule of Law 1918–1935* (1936).

Cite this article: Wang X (2024). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers? *Leiden Journal of International Law*. <https://doi.org/10.1017/S0922156524000402>