DECOUPLING TRADE AND CYBERSECURITY: A WAY TO RECALIBRATION?

Xin Wang[*]

ABSTRACT

This article aims at providing an alternative explanation to cybersecurity conundrum in trade. This article takes a systemic and holistic stance to observe cybersecurity by applying an institutionalist approach to analyze the cybersecurity provisions in free trade agreements (hereinafter "FTAs") and the norm-making processes on cybersecurity under the auspice of the United Nations (hereinafter "UN"). The observations indicate that the cybersecurity provisions in FTAs may serve as implicit diversions from the trade commitments, while the norm-making processes on cybersecurity under the UN produce a minimum public order. This represents a shared understanding of states that international law falls short in the context of cybersecurity, although it is necessary to give greater attention. As the shared understanding may incentivize interactions between decision-making processes, the trade rules may further have less constraint on state behavior in the context of cybersecurity. In this regard, cybersecurity "decouples" from trade disciplines, which enables the states to recalibrate the multilateral trading system. Furthermore, this article considers that the "decoupling" arises from receiving and reconstructing the mercantilist practices pertaining to cybersecurity. Finally, this article considers that institutional linkages would be a way to recouple trade and cybersecurity, although there would still be a long march.

[*] Xin Wang is a Lecturer at School of Law, Guangdong University of Foreign Studies (GDUFS). The author can be reached at: vivianwang_336@hotmail.com.

臺灣大學學術期刊資料庫

KEYWORDS: *cybersecurity, FTAs, the UN, legalization, institutions, institutional linkages*

臺灣大學學術期刊資料庫

Table of Content

I. Introduction 41
II. The Preliminaries 45
A. The Institutionalist Approaches: Legalization and Rational Design (RD) 45
B. An Integrated Approach 49
III. Cybersecurity Under the Multilateral Trading System: A Partial Diversion 52
A. An Overview 52
B. The Substance: Shallow Commitments and Exception-Normality Transition 56
1. Shallow Commitments 56
2. Delegation as Law-Making Processes 58
C. Appraisal 61
IV. The Norm-Making Processes on Cybersecurity Under the UN: An Emerging Minimum Order 63
A. An Overview 63
B. Non-Legalized Obligations as Emerging Custom 65
C. Embedded Mechanisms of Delegation 67
D. Appraisal 69
V. Soft Legalization as Recalibration? 72
A. An Appraisal 72
B. Will Institutional Linkages Be a Way to Recoupling? 75
VI. Conclusion 76

I. INTRODUCTION

On May 8th, 2022, the new President of Costa Rica, Rodrigo Chaves Robles, declared a state of national security emergency due to Conti ransomware attacks that infiltrated twenty-seven governmental institutions. The attacks significantly affected foreign trade in Costa Rica because they paralyzed customs and tax systems.[1] Such kinds of cybersecurity incidents are prevalent nowadays. In the last two decades, the number of cyber-attacks has increased exponentially: according to the Center for Strategic and International Studies (CSIS), there was only one reported case of significant cybersecurity incidents in 2003, but the number surged to 118 in 2022.[2]

[1] Joe Tidy, *President Rodrigo Chaves Says Costa Rica Is at War with Conti Hackers*, BBC NEWS (May 18, 2022), https://www.bbc.com/news/technology-61323402.

[2] *Significant Cyber Incidents Since 2006*, CSIS, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/230207_Significant_Cyber_Incidents.pdf?VersionId=f3TcDDNQ0YCzPY72D_AdhyuYY21ifK_h (last visited Feb. 13, 2023).

臺灣大學學術期刊資料庫

Rising cybersecurity incidents dampen "the security of socio-technical dynamics related to the impact of the information revolution on pre-existing mechanisms of human interaction the world over."[3] Therefore, states are more regulatory towards cyberspace. Nevertheless, increasing domestic regulation has created a conundrum in the multilateral trading system which is interconnected with "the application of the principle of least restrictive regulations."[4]

Cybersecurity is a trade-related issue which triggers contentions and debates. Firstly, scholars have contentions on whether trade rules can effectively regulate state behavior pertaining to cybersecurity. Some scholars recognize that the trade rules including free trade agreements (hereinafter "FTAs") and the reformed disciplines of the World Trade Organization (hereinafter "WTO") can contribute to handling cybersecurity issues.[5] Nevertheless, some scholars consider that the trade rules may address those issues, but they cannot regulate them in substance. The reason is that shallow commitments in the trade rules are not sufficient enough to harmonize domestic regulation without universal consensus on how to protect cybersecurity.[6] Secondly, scholars have contentions on whether general/essential security exceptions in the trade rules may defend state behavior of protecting cybersecurity. Henckels recognizes that general/essential security exceptions are applicable to state behavior pertaining to cybersecurity, but they should be applied to justify the inapplicability of the trade rules instead of being applied in a way to defend allegedly inconsistent state behavior.[7] Conversely, some scholars are negative to this issue owing to technical and political concerns. For example, some scholars questioned if a dispute settlement body (hereinafter "DSB") established by the trade rules can solve complex technical issues to balance (cyber-)security and free trade[8] without the engagement of technological

[3] CHRISTOPHER WHYTE & BRIAN MAZANEC, UNDERSTANDING CYBER WARFARE: POLITICS, POLICY AND STRATEGY 11 (2019).

[4] GATT Secretariat, *Analytical Summary of Information Exchanged Among Contracting Parties*, ¶ 160, GATT Doc. MDF/7/Rev.2 (Nov. 25, 1985). Pertinent discussions include: Alan O. Sykes, *The Least Restrictive Means*, 70(1) U. CHI. L. REV. 403 (2003); Jeremy C. Marwell, *Trade and Morality: The WTO Public Morals Exception After Gambling*, 81(2) N.Y.U. L. REV. 802 (2006).

[5] Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22(3) J. INT'L ECON. L. 389, 405 (2019).

[6] Susan Aaronson, *Why Trade Agreements Are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14(4) WORLD TRADE REV. 671, 695 (2015).

[7] Caroline Henckels, *Permission to Act: The Legal Character of General and Security Exceptions in International Trade and Investment Law*, 69(3) INT'L & COMPAR. L.Q. 557, 582-84 (2020).

[8] Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18(2) J. INT'L ECON. L. 449, 476-78 (2015); Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19(3) WORLD TRADE REV. 341, 364 (2020) [hereinafter Mishra, *Privacy, Cybersecurity, and GATS Article XIV*]; Neha Mishra, *The Trade: (Cyber)Security Dilemma and Its Impact on Global Cybersecurity Governance*, 54(4) J. WORLD TRADE 567, 574-86 (2020) [hereinafter Mishra, *The Trade: (Cyber)Security Dilemma*].

臺灣大學學術期刊資料庫

experts[9] as cyberspace is a highly-structured and complex four-layered domain.[10] Simultaneously, DSB may constrain from deliberating serious cybersecurity issues that amount to international emergency because it is always contentious whether the essential security exception is self-judging:[11] recent cases such as *Russia — Measures Concerning Traffic in Transit* indicated that "the evaluation of whether the invoking Member has satisfied the requirements of the enumerated subparagraphs of Article XXI(b) [should] be made objectively rather than by the invoking Member itself."[12] Nevertheless, "the political discontentment . . . could arise if and when a Panel adjudicates on a cybersecurity-related measure under GATS [A]rt. XIVbis,"[13] which may accelerate the disintegration of the multilateral trading system.[14] Thirdly, it is questionable whether "security" in the trade rules may accommodate "cybersecurity" from a technical perspective: the trade rules adopt traditional and military-focused notions of security,[15] while "cybersecurity" is "a grab-bag concept for a heterogeneous set of threats and practices . . . . [It is] hard to make general claims about the entire range of sub-issues it contains."[16] In particular, the trade rules are based on the goods-service dichotomy, but cybersecurity issues are on the borderline between goods and services.[17] Additionally, scholars have proposed three solutions to the cybersecurity conundrum in trade:

1. To establish a new trade regime to deal with issues concerning cybersecurity in digital trade;[18]

---

[9] Mishra, *Privacy, Cybersecurity, and GATS Article XIV, supra* note 8, at 350, 363-64.

[10] NAZLI CHOUCRI & DAVID D. CLARK, INTERNATIONAL RELATIONS IN THE CYBER AGE: THE CO-EVOLUTION DILEMMA 35 (2019).

[11] Researches indicating "essential security interest" as self-judging include: Roger P. Alford, *The Self-Judging WTO Security Exception*, 2011(3) UTAH L. REV. 697, 749 (2011); Raj Bhala, *National Security and International Trade Law: What the GATT Says, and What the United States Does*, 19(2) U. PA. J. INT'L ECON. L. 263, 267 (1998). Some scholars indicated that it is not. *See* Peter Lindsay, *The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure?*, 52(6) DUKE L.J. 1277, 1303-04 (2003); Tsai-fang Chen, *To Judge the "Self-Judging" Security Exception Under the GATT 1994 – A Systematic Approach*, 12(2) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 311, 321-22 (2017); Jaemin Lee, *Commercializing National Security: National Security Exceptions' Outer Parameter Under GATT Article XXI*, 13(2) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 277, 290-301 (2018).

[12] Panel Report, *Russia — Measures Concerning Traffic in Transit*, ¶ 7.100, WTO Doc. WT/DS512/R (adopted Apr. 26, 2019).

[13] Mishra, *The Trade: (Cyber)Security Dilemma, supra* note 8, at 586.

[14] Daria Boklan & Amrita Bahri, *The First WTO's Ruling on National Security Exception: Balancing Interests or Opening Pandora's Box?*, 19(1) WORLD TRADE REV. 123, 135-36 (2020); Tatiana Lacerda Prazeres, *Trade and National Security: Rising Risks for the WTO*, 19(1) WORLD TRADE REV. 137, 145-48 (2020).

[15] J. Benton Heath, *Trade and Security Among the Ruins*, 30(2) DUKE J. COMPAR. & INT'L L. 223, 227-28, 234-39 (2020).

[16] Myriam Dunn Cavelty, *Cybersecurity Between Hypersecuritization and Technological Routine*, *in* ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY 11, 16 (Eneken Tikk & Mika Kerttunen eds., 2020).

[17] Shin-yi Peng, *A New Trade Regime for the Servitization of Manufacturing: Rethinking the Goods-Services Dichotomy*, 54(5) J. WORLD TRADE 699, 699 (2020).

[18] *Id*. at 721-24.

臺灣大學學術期刊資料庫

2. to propose new rules under the WTO; and
3. to use non-trade rules under other international forums to complement trade disciplines owing to linkages between international trade law and internet governance and policy.[19]

This article considers that the pre-existing studies have made great contributions to enlightening what the cybersecurity conundrum is and how it should be addressed in trade. Nevertheless, the pre-existing studies leave a gap as most of them only assessed the conundrum under the scrutiny of the trade rules: what if states actually do not acknowledge that cybersecurity as the pursuit of legitimate policy goals should be subject to "[t]he purpose and objective of the general and specific obligations applicable according to the GATS in relation to non-discrimination and market access and a level playing field?"[20] There are a few studies that have nearly touched upon this topic. For example, Mishra indicated that approaches outside the WTO dispute settlement mechanism, including diplomatic dialogues, international regulatory cooperation/coordination on cybersecurity and others are better instruments to resolve cybersecurity issues.[21] Nevertheless, she does not further explore how these approaches proceed to influence the cybersecurity conundrum in trade. This article does not intend to simply observe cybersecurity in the ambit of the trade rules. Instead, this article will systematically assess how states deliberate on cybersecurity vis-à-vis trade by observing the cybersecurity provisions in the FTAs and the norm-making processes on cybersecurity under the United Nations (hereinafter "UN"). The reason to put the trade rules on a par with the norm-making processes under the UN is that "general law . . . provides the normative background that comes in to fulfil aspects of the regime's operation not specifically provided by the regime . . . [and] also come[s] into operation if the special regime fails to function properly."[22] In this regard, lawmaking under the UN has residual/default applicability vis-à-vis the trade rules, especially when particular objectives of the trade rules have no prioritization over others[23] and the lawmaking under the UN involves codification of customary international law (hereinafter "CIL") and/or fundamental ethical principles.[24] This article believes that a holistic observation on trade and cybersecurity

[19] Henckels, *supra* note 7, at 579-82; Mishra, *Privacy, Cybersecurity, and GATS Article XIV, supra* note 8, at 361; Victoria Conrad, *Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data*, 10(1) WILLIAM & MARY BUS. L. REV. 295, 335-36 (2018).

[20] Rolf H. Weber & Rainer Baisch, *Revisiting the Public Moral/Order and the Security Exceptions Under the GATS*, 13(2) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 375, 380 (2018).

[21] Mishra, *The Trade: (Cyber)Security Dilemma, supra* note 8, at 586.

[22] Martti Koskenniemi, *Rep. of the Study Grp. of the Int'l L. Comm'n*, U.N. Doc. A/CN.4/L.682, Add.1, ¶ 192 (Apr. 13, 2006).

[23] Danae Azaria, *Trade Countermeasures for Breaches of International Law Outside the WTO*, 71(2) INT'L & COMPAR. L.Q. 389, 417 (2022).

[24] BRIAN D. LEPARD, CUSTOMARY INTERNATIONAL LAW: A NEW THEORY WITH PRACTICAL APPLICATIONS 208-17 (2010).

臺灣大學學術期刊資料庫

will further enable "appraisals of the quality of any existing or prospective legal arrangement [to] not focus exclusively on that arrangement but locate it in context so that its aggregate effects on other arrangements and in terms of other principles and goals can be taken into account."[25] This article is structured into six parts. Following the introduction, Part II presents the analytical framework of this study. Part III empirically observes and analyzes the provisions of cybersecurity in the FTAs. The purpose is to assess their distribution and how states structure "cybersecurity" under the multilateral trading system. Part IV observes and analyzes the UN's norm-making processes to see whether and to what extent they may guide state behavior. Part V appraises how these two types of decision-making processes may influence the multilateral trading system and discusses factors that induce the soft legalization of cyberspace. Simultaneously, this article also proposes a potential solution to recouple trade and cybersecurity under the multilateral trading system. Part VI concludes this study.

II. THE PRELIMINARIES

This article recognizes that "international institutions" are "explicit arrangements, negotiated among international actors, that prescribe, proscribe, and/or authorize behavior." [26] Simultaneously, this article recognizes that these arrangements reflect "actor expectations converg[ing] in a given issue-area."[27] Section 2.1 will present two analytical frameworks of the institutional and rational approaches. Then, Section 2.2 will introduce the analytical framework of this study.

A. The Institutionalist Approaches: Legalization and Rational Design (RD)

Scholars have developed several analytical/conceptual frameworks, including legalization, Raustiala's legality,[28] Rational Design (hereinafter

[25] W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY 357-58 (2012).

[26] Barbara Koremenos et al., *The Rational Design of International Institutions*, 55(4) INT'L ORG. 761, 762 (2001). Haggard and Simmons distinguished "institution" from "regime" because they saw "institution" in a wider context, arguing that "regime" instead of "institution" required organizational form. This article only uses the analytical frameworks to facilitate forthcoming observations and analyses without more in-depth theoretical enquiries. Therefore, this article equals "regime" to "institution." *See* Stephan Haggard & Beth A. Simmons, *Theories of International Regimes*, 41(3) INT'L ORG. 491, 495-97 (1987).

[27] Stephen D. Krasner, *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, 36(2) INT'L ORG. 185, 185 (1982).

[28] Kal Raustiala, *Form and Substance in International Agreements*, 99(3) AM. J. INT'L L. 581, 583-84 (2005).

臺灣大學學術期刊資料庫

"RD"), and the Continent of International Law (COIL)[29] since the early 2000s.[30] Legalization and the RD are the main frameworks, while the others are derived from them. Legalization analyzes "a particular set of characteristics that institutions may (or may not) possess"[31] from three dimensions: (1) nature of a commitment; (2) preciseness of a commitment; and (3) how a commitment will be enforced (see Table 1):[32]

TABLE 1: An Integration of Legalization and Legality

	High	Moderate	Low
Obligation	Unconditional ({O})	Conditional (with reservations) or Hortatory ({o})	Non-binding ({o-})
Precision	Determinate and substantial without broad areas of discretion ({P})	Broad areas of discretion or standard-like ({p})	Impossible to determine whether conduct complies ({p-})

[29] *See generally* BARBARA KOREMENOS, THE CONTINENT OF INTERNATIONAL LAW: EXPLAINING AGREEMENT DESIGN (2016).

[30] Barbara Koremenos, *Institutionalism and International Law*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART 59, 61-65 (Jeffrey L. Dunoff & Mark A. Pollack eds., 2013).

[31] Kenneth W. Abbott et al., *The Concept of Legalization*, 54(3) INT'L ORG. 401, 401 (2000).

[32] Raustiala introduced another similar conceptual framework which consists of legality, substance and structure. Legality represents legal bindingness of a commitment. Substance represents the depth of a commitment. Structure represents how a commitment is enforced. *See* Raustiala, *supra* note 28, at 583-86.

臺灣大學學術期刊資料庫

	Adjudication	(Quasi-)Judicial ({D})	Arbitral or mediation-applicable ({d})	Applicable only to negotiation ({d-})
Delegation	Enforcement	Enforceable ({D})	Enforceable based on coordination or monitoring ({d})	Non-enforceable ({d-})

Different combinations of *obligation*, *precision* and *delegation* reflect how states intend to trade off predictability, stability, flexibility and sovereign cost. Technically, most combinations are soft legalized except {O, P/p, D/d}. Generally, hard legalized institutions constrain state behavior because states are at stake of retaliation as well as loss of reputation and reciprocity arising from noncompliance.[33] In other words, states have sent their strongest intention to comply with international legal obligations[34] by developing a hard legalized institution. Nevertheless, it is not easy to bargain for a hard institution when parties need to coordinate on a defined issue to achieve absolute gains on it.[35] For instance, a hard institution of security is difficult to form unless dominant states have such an intention and the participants are like-minded.[36] In contrast, a soft legalized institution may enable states to co-exist side by side while accommodating each other's heterogeneity,[37] but it does not bind states, although it may "create expectations about future conduct."[38]

RD is also an analytical framework to assess an institution, but it starts by observing how cooperation problems (independent variables (hereinafter "IVs")) affect the structure (dependent variables (hereinafter "DVs")) of an institution. The DVs and IVs are either positively or negatively correlated, as specified in Table 2:

[33] ANDREW T. GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 33-48 (2008).
[34] *Id.* at 59.
[35] Asaf Siniver & Scott Lucas, *Understanding Tacit Security Regimes*, 4(4) J. GLOB. SEC. STUD. 510, 513 (2019).
[36] Robert Jervis, *Security Regimes*, 36(2) INT'L ORG. 357, 360-362 (1982).
[37] Prosper Weil, *Towards Relative Normativity in International Law?*, 77(3) AM. J. INT'L L. 413, 418-19 (1983).
[38] Andrew T. Guzman & Timothy L. Meyer, *International Soft Law*, 2(1) J. LEGAL ANALYSIS 171, 174 (2010).

臺灣大學學術期刊資料庫

TABLE 2: Intersections of the DVs and IVs[39]

DVs (horizontal)/ IVs (vertical)	Membership (Who Participates?)	Scope (Coverage)	Centralization (How to administer information dissemination?)	Control (How to make decisions collectively?)	Flexibility (The degree of accommodating new circumstances)
Distribution Problem	+	+	/	/	+
Enforcement Problem	-	+	+	/	/
Number of Actors	/	+	+	- (individual)/ + (asymmetry)	-
Uncertainty about behavior	/	/	+	/	/
Uncertainty about the state of the world	/	/	+	+ (individual)	+
Uncertainty about preferences	-	/	/	/	/

[39] Koremenos et al., *supra* note 26, at 780-99.

臺灣大學學術期刊資料庫

The RD considers that variations of the DVs are purposeful choices of states to advance joint interests and to reap future gains.[40] For example, states use exceptions as escape clauses to accommodate uncertainty and to lower the difficulty in concluding an agreement.[41] For another instance, states use one centralized focal point to reduce uncertainty by increasing transparency and to tilt asymmetry between participants with the purpose of enhancing adherence.[42] The Trade Policy Review Mechanism (TPRM) under the WTO is one typical exemplar: the Trade Policy Review Mechanism Division under the WTO Secretariat periodically review the trade policies and practices of the WTO members, improving transparency of the multilateral trading system.[43]

B. An Integrated Approach

This article considers that the two analytical frameworks are complementary because the RD can complement the formal approach adopted in Legalization. Simultaneously, Legalization can compensate for the RD's neglect of form, which may lead to subjectivity. In this regard, this article will integrate both to analyze the FTAs and the UN norm-making processes. The integrated approach starts by analyzing *obligation* and *delegation*. Simultaneously, the DVs of the RD will be incorporated in explaining the substances of *obligation* and *delegation*.[44]

First, membership, scope and flexibility in the RD serve as the substance of *obligation* in Legalization because the three factors are oftentimes calculations of policy preferences as well as cost and benefit.[45] {O} represents that states treat a commitment as a legal obligation. Nevertheless, the compliance pull of {O} can be reduced, if there is linguistic indeterminacy that blurs the scope of the commitment.[46] For example, some scholars indicate that the United States (hereinafter "US") indirectly conveys its intentions to expand its military role in cybersecurity by using implicit metaphorical language in its military strategy and doctrine concerning cybersecurity. The purpose of using metaphorical language is to avoid inconsistency with the obligation to maintain international peace and security

[40] *Id.* at 781-82.
[41] B. Peter Rosendorff & Helen V. Milner, *The Optimal Design of International Trade Institutions: Uncertainty and Escape*, 55(4) INT'L ORG. 829, 831-32 (2001).
[42] Koremenos et al., *supra* note 26, at 771-72.
[43] 2 PETROS C. MAVROIDIS, THE REGULATION OF INTERNATIONAL TRADE (VOL. 2: THE WTO AGREEMENTS ON TRADE IN GOODS) 692-94 (2016).
[44] This article appraise *precision* from the perspective of *obligation*.
[45] G. JOHN IKENBERRY, LIBERAL LEVIATHAN: THE ORIGINS, CRISIS, AND TRANSFORMATION OF THE AMERICAN WORLD ORDER 99-102 (2011).
[46] Thomas M. Franck, *Legitimacy in the International System*, 82(4) AM. J. INT'L L. 705, 714 (1988).

臺灣大學學術期刊資料庫

under the Charter of the United Nations (hereinafter "the UN Charter").[47] {o} often represents an intention of states to balance predictability and flexibility because exceptions allow states to mitigate unforeseeable risks arising from compliance.[48] It is believed that states may not necessarily abuse exceptions by being opportunistic as long as the design of exceptions is not unlimited or subject to full discretion.[49] {o-} means that a commitment is only with "political or moral weight" because it does not constrain states from exercising the sovereign right to regulate.[50] Therefore, {o-} produces less predictable state behavior than {O}/{o} because "[i]ndeterminate normative standards not only make it harder to know what conformity is expected, but also make it easier to justify noncompliance."[51] Nevertheless, {o-} may serve as evidence of emerging customary law in transition of hard law, although judicial recognition is unlikely.[52] In practice, states oftentimes make soft commitments, when a subject-matter is premature to harder legalization.[53] Furthermore, rewarding of compliance with international law will also be an essential incentive for states to choose one from the other:[54] states may not seek {O}/{o}, when joint gains do not increase in accordance with risks.[55] Additionally, the depth of *obligation* can affect its bindingness. From a substantive perspective, shallow commitments "assure the coexistence of different interests which are worthy of legal protection,"[56] which enables states to "pursue Pareto-improving agreements with minimum cost."[57] In practice, states will not make a deep commitment unless it reflects the genuine expectations of the community or the value of future gains outweighs risks of paying high sovereign costs or of constraining sovereign autonomy because deep commitments may (re)shape a community.[58]

---

[47] Jordan Branch, *What's in a Name? Metaphors and Cybersecurity*, 75(1) INT'L ORG. 39, 50-55 (2020).

[48] KRZYSZTOF J. PELC, MAKING AND BENDING INTERNATIONAL RULES: THE DESIGN OF EXCEPTIONS AND ESCAPE CLAUSES IN TRADE LAW 11 (2016).

[49] Martti Koskenniemi, *The Mystery of Legal Obligation*, 3(2) INT'L THEORY 319, 323 (2011).

[50] Oscar Schachter, *The Twilight Existence of Nonbinding International Agreements*, 71(2) AM. J. INT'L L. 296, 302 (1977).

[51] Franck, *supra* note 46, at 714.

[52] Hugh Thirlway, *Reflections on* Lex Ferenda, 32 NETH. Y.B. INT'L L. 3, 13-17 (2001).

[53] Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54(3) INT'L ORG. 421, 423 (2000).

[54] Anne van Aaken & Betül Simsek, *Rewarding in International Law*, 115(2) AM. J. INT'L L. 195, 196-97 (2021).

[55] Brandon J. Kinne, *Defense Cooperation Agreements and the Emergence of a Global Security Network*, 72(4) INT'L ORG. 799, 808-09 (2018).

[56] Island of Palmas Case (Neth. v. U.S.), 2 R.I.A.A. 870 (Perm. Ct. Arb. 1928).

[57] KOREMENOS, *supra* note 29, at 29; Abbott & Snidal, *supra* note 53, at 430-33; Rosendorff & Milner, *supra* note 41, at 831; Laurence R. Helfer, *Flexibility in International Agreements*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART 175, 179 (Jeffrey L. Dunoff & Mark A. Pollack eds., 2012).

[58] Koremenos et al., *supra* note 26, at 775-76; Adeno Addis, *Authority and Community*, 18(1) ASIA PAC. L. REV. 63, 66-67 (2010).

臺灣大學學術期刊資料庫

Second, *delegation* connects with centralization and control in the RD. {D} means that an institution has administrative or adjudicatory mechanisms for monitoring and enforcing performance, but an administrative mechanism is not designed to "determine authoritatively and effectively what is regarded as international law" in a contentious case.[59] Comparatively, an adjudicatory mechanism circumscribes "the controversial subject to remain altogether outside the sphere of law" or "out of express legal regulation."[60] In practice, {O} is toothless without adjudicatory {D} or {d} because "[p]rimary rules of obligation that lack adherence to a system of secondary rules of process are mere ad hoc reciprocal arrangements."[61] For example, most scholars and practitioners lament the malfunction of the WTO's dispute settlement mechanism (hereinafter "DSM") because many issues leave open-ended without resolutions.[62] However, {D}/{d}, particularly an adjudicatory one, imposes great constraints on sovereignty; therefore, there would be challenges to its legitimacy. For example, there was a call for internal legitimation of the WTO DSB to counter power shift and ideological frictions arising from increasing diversity in the first decade of the WTO's establishment.[63] {d-} means that an institution operates in the shadow of power because few independent procedural rules are available for participants to have access to mediate conflicting interests.[64]

This article considers that an institution is legalized when an institution has {O/o, D/d}, and the commitment(s) should not be only "process commitments".[65] Ideologically, a legalized institution reflects a liberal approach that uses the law to steer state behavior.[66] Notwithstanding, a legalized institution may risk ending cooperation if it ends up with punishment.[67] Conversely, {o-, d-} means that an institution is softly legalized. From a functional perspective, a softly legalized institution can not only supplement and clarify pre-existing rules, but also signals institutional change as it serves as "the first step of the codification and progressive

[59] GERNOT BIEHLER, PROCEDURES IN INTERNATIONAL LAW 37 (2008).
[60] SIR HERSCH LAUTERPACHT, THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY 85 (2011).
[61] Franck, *supra* note 46, at 752.
[62] PETROS C. MAVROIDIS, THE WTO DISPUTE SETTLEMENT SYSTEM: HOW, WHY AND WHERE? 62 (2022).
[63] *Id.* at 10-19; Joseph H.H. Weiler, *The Rule of Lawyers and the Ethos of Diplomats Reflections on the Internal and External Legitimacy of WTO Dispute Settlement*, 35(2) J. WORLD TRADE 191, 193 (2001).
[64] Robert O. Keohane et al., *Legalized Dispute Resolution: Interstate and Transnational*, 54(3) INT'L ORG. 457, 458 (2000).
[65] IKENBERRY, *supra* note 45, at 112.
[66] Laurence R. Helfer, *Overlegalizing Human Rights: International Relations Theory and the Commonwealth Caribbean Backlash Against Human Rights Regimes*, 102(7) COLUM. L. REV. 1832, 1848-49 (2002).
[67] KOREMENOS, *supra* note 29, at 231.

臺灣大學學術期刊資料庫

development of certain sectors of international law . . . ."[68] Therefore, a softly legalized institution seeks "the acceptability of approximate implementations" that "do not preclude subsequent improvements which may lead to a closer approximation of a satisfactory arrangement."[69] Nevertheless, a soft-legalized institution is in the midst of political struggles because a subject-matter is not in the legal domain.[70]

III. CYBERSECURITY UNDER THE MULTILATERAL TRADING SYSTEM: A PARTIAL DIVERSION

A. An Overview

This article uses data from the Trade Agreements Provisions on Electronic-commerce and Data (TAPED) database and the WTO Regional Trade Agreements Database (WTO RTA Database) as the dataset for this study:[71] 50 (25%) of the 200 FTAs with e-commerce provisions or an e-commerce chapter have one or more cybersecurity provisions. The limited number does not mean that states lack cybersecurity cooperation in trade. Instead, it means that states may be tacit in cybersecurity cooperation in trade; therefore, they may not tend to set boundaries of their promises and/or specify their intentions *ex ante*.[72] Furthermore, statistics indicate that "cybersecurity" is more frequently addressed after the 2010s as indicated in Figure 1:

[68] TULLIO TREVES, THE EXPANSION OF INTERNATIONAL LAW 284 (2015).
[69] REISMAN, *supra* note 25, at 359.
[70] Jeffrey L. Dunoff, *The Death of the Trade Regime*, 10(4) EUR. J. INT'L L. 733, 755 (1999).
[71] *TAPED: A New Dataset on Data-Related Trade Provisions*, UNIV. OF LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/ (last visited Feb. 8, 2023). The reason to use the WTO Regional Trade Agreements Database as a supplement is because Trade Agreements Provisions on Electronic-commerce and Data [hereinafter TAPED] does not contain free trade agreements [hereinafter FTAs] effective after 2021. Additionally, UK–Singapore Digital Economy Agreement is also counted with the purpose of being consistent with the criteria adopted by TAPED.
[72] Charles Lipson, *Why Are Some International Agreements Informal?*, 45(4) INT'L ORG. 495, 498-99 (1991).

臺灣大學學術期刊資料庫

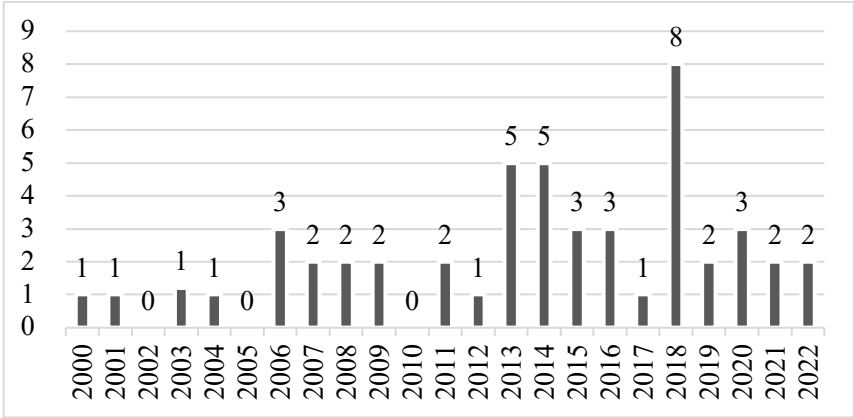


FIGURE 1: Time Span and Distribution

The statistics indicate that the demands for greater attention to cybersecurity issues in trade increased after 2010 (n=37/74%),[73] covering forty-three economies. Additionally, a majority of them engage in more than one FTA,[74] as indicated in Figure 2:

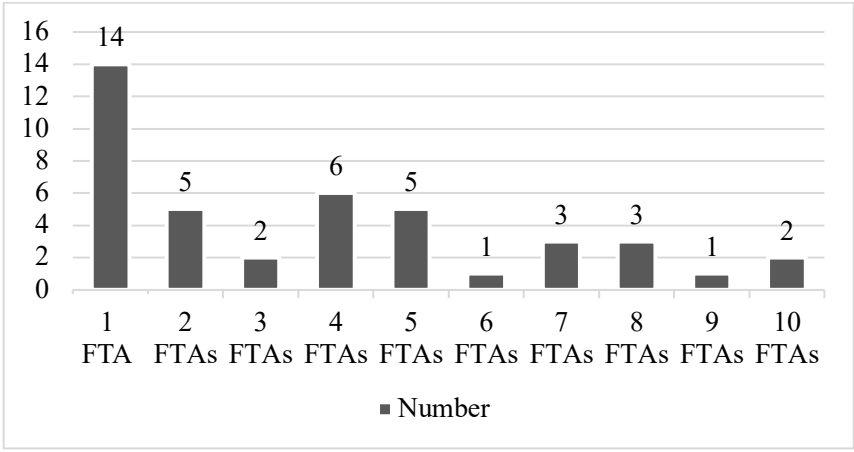


FIGURE 2: Distribution

[73] Statistics support this argument. *See Individuals Using the Internet (% of population)*, THE WORLD BANK, https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&start=1960 & view=chart (last visited Feb. 8, 2023).

[74] Fourteen economies (30%) are parties to only one FTA: Jordan, United Arab Emirates [UAE], Chinese Taipei, India, the Swiss Confederation, Ecuador, Moldova, Mongolia, Turkey, Uruguay, Argentina, Sri Lanka, Brazil and (the People's Republic of) China.

臺灣大學學術期刊資料庫

A closer examination indicates that the distribution is asymmetric: North and South American states are active players because thirty-five FTAs (70%) have at least one state in the Americas as a party. In Asia, Singapore is an active player that is a party to ten FTAs. Australia and New Zealand are also active, engaging in nine and seven FTAs respectively. These states, by concluding the FTAs, are delivering messages that they are willing to cooperate in protecting cybersecurity in trade. One interesting phenomenon is that the EU addressed "cybersecurity" under only five FTAs with Colombia and Peru, Mexico, Moldova, Japan and the United Kingdom (hereinafter "UK"): the number is disproportionate to its influence on data governance. One explanation is that the requirement of coherence in the EU's external actions increases its difficulty in forming a treaty, especially when "[c]ybersecurity is an integral part of Europeans' security."[75] In this regard, the EU also resorts to non-trade and non-institutionalized forums to facilitate and expand cooperation in cybersecurity at the transnational level without affecting the EU's legal autonomy:[76] the U.S.-EU Trade and Technology Council (TTC) that aims at enhancing training and guidance on cybersecurity for small and medium-sized enterprises (SMEs)[77] as well as the EU-South Korea–Singapore Digital Partnership[78] are the good cases. Simultaneously, no African state has addressed cybersecurity through the FTAs: one possible explanation is that participation of the African states in domains other than trade in raw materials is limited.[79] Furthermore, cybersecurity cooperation under the FTAs is largely bilateral because 74% of the FTAs (n=37) are bilateral, while the remaining FTAs are trilateral (2/4%), quadrilateral (4/8%), more than quadrilateral but with less than ten parties (3/6%) and with more than ten parties (4/8%).[80] Notwithstanding, externalities of the FTAs

[75] Joanna Lam & Güneş Ünüvar, *Transparency and Participatory Aspects of Investor-State Dispute Settlement in the EU 'New Wave' Trade Agreements*, 32(4) LEIDEN J. INT'L L. 781, 788 (2019); *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*, at 1, JOIN (2020) 18 final (Dec. 16, 2020).

[76] Case C-284/16, Slowakische Republik (Slovak Republic) v. Achmea BV, ECLI:EU:C:2018:158, ¶¶ 32-33 (Mar. 6, 2018).

[77] *U.S.–EU Joint Statement of the Trade and Technology Council* (Annex IX: Conclusions on Working Group 9 – Promoting SME Access to and Use of Digital Tools, ¶ 3), THE WHITE HOUSE 41 (May 16, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf.

[78] *Joint Statement by President von der Leyen and President Yoon on the EU–Republic of Korea Digital Partnership*, EUR. COMM'N (Nov. 28, 2022), https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7232; *Joint Statement by President von der Leyen and Prime Minister Lee on the EU–Singapore Digital Partnership*, EUR. COMM'N (Dec. 14, 2022), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7743.

[79] Souleymane Coulibaly et al., *Overview: Market Access Strategy in a New Trade Environment*, *in* AFRICA IN THE NEW TRADE ENVIRONMENT: MARKET ACCESS IN TROUBLED TIMES 1, 14 (Souleymane Coulibaly et al. eds., 2022).

[80] The Association of Southeast Asian Nations [hereinafter ASEAN] is not counted collectively, but the European Union [hereinafter EU] is counted collectively.

臺灣大學學術期刊資料庫

and the rise of the mega-FTAs may produce a network effect which multilateralizes the cooperation.[81]

Additionally, the states may have a different understanding of cybersecurity because they use different terms to represent cybersecurity as indicated in Figure 3:

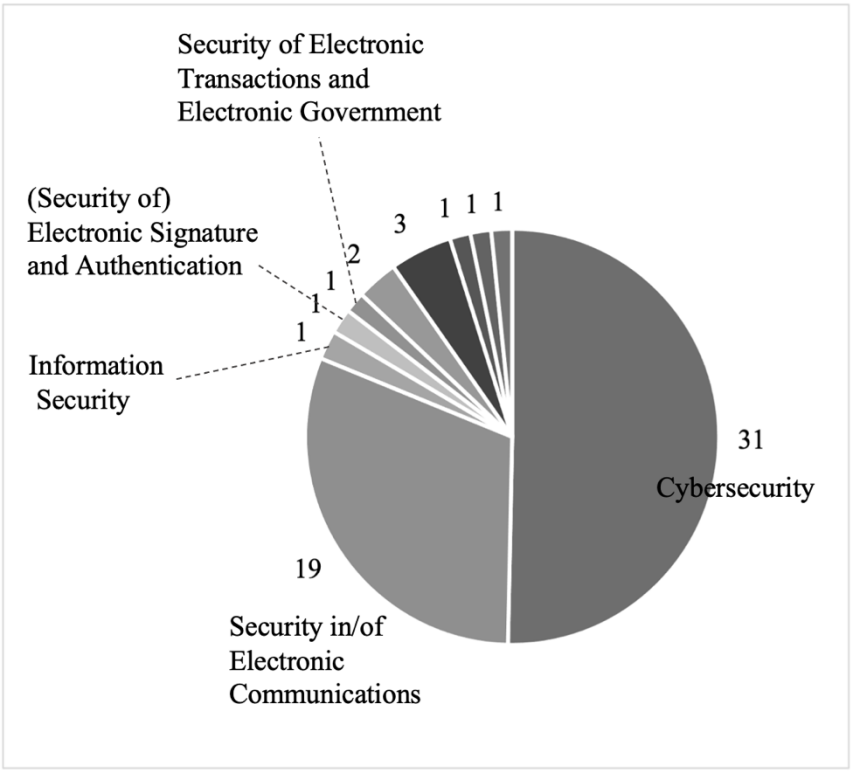


FIGURE 3: The Distribution of the Terms

The diversity in wording implies that the scopes of "cybersecurity" under the FTAs may be different, especially when some of the FTAs concurrently use "cybersecurity" and one of the other terms (22%).[82]

[81] Richard Baldwin et al., *Beyond Tariffs: Multilateralizing Non-Tariff RTA Commitments*, *in* MULTILATERALIZING REGIONALISM: CHALLENGES FOR THE GLOBAL TRADING SYSTEM 79, 80-81 (Richard Baldwin & Patrick Low eds., 2009).

[82] There are ten/eleven FTAs including *Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico*, CPTPP/TPP, *Acuerdo de Libre Comercio entre la República de Chile y la República Oriental del Uruguay*, *Australia–Peru FTA*, *United States–Mexico–Canada Agreement* (USMCA), *Chile–Brazil Bilateral Trade Agreement*, *Indonesia–Australia Comprehensive Economic Partnership Agreement* (IACEPA), *Australia–Singapore Digital Economy Agreement*, *UK–*

臺灣大學學術期刊資料庫

Nevertheless, the FTAs provide no definition to these terms: such linguistic indeterminacy may trigger regulatory indeterminacy because "[a] name . . . is a primitive sign . . . that has a definition . . . [to] point the way."[83]

B. The Substance: Shallow Commitments and Exception-Normality Transition

1. Shallow Commitments — The commitments on cybersecurity cover two categories: one category of commitments is identified as "Transparency" because it requires "sharing information and experiences on laws, regulations, and programs in the sphere of electronic commerce, including those related to . . . security in electronic communications . . . ;"[84] and the other category is labeled as "Performance" because it requires capacity building at the domestic level and/or maintenance/establishment of cooperative mechanisms. For example, Paragraphs 2-3, Article 12.6 (Cooperation) of the Colombia–South Korea FTA provide that

> [t]he Parties . . . shall cooperate to help micro, small, and medium-sized enterprises overcome the obstacles they face in the use of electronic commerce . . . [and] the Parties agree to actively participate in regional and multilateral fora to promote the development of electronic commerce and to exchange views, as necessary, within the framework of such fora on issues related to electronic commerce.

The distribution of the two categories is as specified in Figure 4:[85]

Singapore Digital Economy Agreement (UKSDEA) and the *Digital Economy Partnership Agreement* (DEPA).

[83] LUDWIG WITTGENSTEIN, TRACTATUS LOGICO-PHILOSOPHICUS, ¶¶ 3.26-.261 (Ramsey Ogden & McGuinness Pears trans., 2022) (1922), http://people.umass.edu/klement/tlp/tlp.pdf.

[84] Free Trade Agreement Between Canada and The Republic of Colombia, Can.-Colom., art. 1507, ¶ 1(b), Nov. 21, 2008, https://wits.worldbank.org/GPTAD/PDF/archive/canada-columbia.pdfs.

[85] As is indicated in Figure 3, there are ten/eleven FTAs that include more than one provision/clause. Thus, there are sixty-five provisions/clauses that address "cybersecurity" in total.

臺灣大學學術期刊論文資料庫

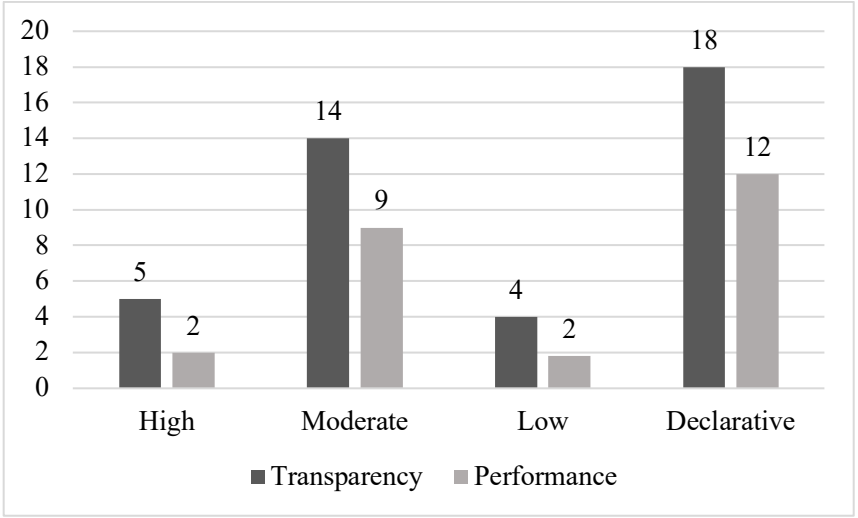


FIGURE 4: Distribution of "Transparency" and "Performance"[86]

There are three aspects. First, most states tend to avoid undertaking international obligations pertaining to cybersecurity in trade. This represents that the states largely intend to be flexible to cybersecurity issues in trade. Second, most of the commitments are shallow without addressing any procedural issues relating to information sharing and/or cooperation through pre-existing mechanisms. The only exception is the UK–EU Trade and Cooperation Agreement (TCA) which mandates the UK to participate in information sharing, capacity building and other activities launched by the EU's Computer Emergency Response Team (hereinafter "CERT"), the European Union Agency for Cybersecurity (ENISA) and other authorities on voluntary and reciprocal bases.[87] The situation indicates that the EU and UK

[86] The criteria for distinguishing different levels include (1) whether there is a modal verb and (2) whether the modal verb is imperative. In this regard, "shall" is assigned to the high level; "shall endeavour to" is assigned to the moderate level; and "should/may/will" is assigned to the low level. If there is no modal verb, this article identifies this as "no obligation". The commitments with a high level of obligation include the Agreement Between Australia and Japan for an Economic Partnership, the Free Trade Agreement Between the Government of the Socialist Republic of Viet Nam and the Government of the Republic of Korea, the SAFTA, the EU–Mexico Modernised Global Agreement, the Agreement Between the European Union and Japan for an Economic Partnership, and the UK–EU Trade and Cooperation Agreement (UK–EU TCA). The commitments with a low level of obligation are the US–Jordan FTA (should); the Canada–Costa Rica FTA and Chile–Brazil Bilateral Trade Agreement (will); and the ASEAN–Australia–New Zealand FTA (AANZFTA), EU–Colombia–Peru FTA, and Association Agreement between the European Union and the European Atomic Energy Community and their Member States and the Republic of Moldova (may).

[87] Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part arts. 705-07, Dec. 30, 2020, 2021 O.J. (L 149) 10.

臺灣大學學術期刊資料庫

have general consensus on how to cooperate on cybersecurity in trade,[88] while most of the states do not have such a consensus. Third, the enforceability of the commitments at the transnational level is questionable owing to their hortatory wording, even when they are legalized ones. For example, the Singapore–Australia FTA (SAFTA) provides that "[t]he Parties shall create and promote a safe online environment" and "shall endeavour to maintain an open, free and secure Internet in accordance with their respective laws and regulations."[89] In practice, it is difficult to assess whether a state has performed the commitment to their "best effort", although a few cases recognize that "best efforts" can be scrutinized and measured. For example, the Panel of the EU–Korea FTA has reasoned that "best effort" requires "continued and sustained efforts" whose "standard . . . is higher than undertaking merely minimal steps or none at all. . . . aiming for an effort, not result"; therefore, a state should "resor[t] to all the appropriate measures that could allow it to attain the objective."[90] Nevertheless, there is no evidence that the states under other FTAs also accept such reasoning and interpretation of "best effort". Additionally, there is no guarantee that conflicting practice would not arise because both categories of commitments cannot institutionalize cooperative activities.

2. Delegation as Law-Making Processes — A majority of the FTAs recognize that DSM is applicable to the cybersecurity provisions as specified in Figure 5:

[88] Tim Stevens & Kevin O'Brien, *Brexit and Cyber Security*, 164(3) RUSI J. 22, 23-25, 28-30 (2019).
[89] The Singapore–Australia Free Trade Agreement, Austl.-Sing., ch. 14, art. 18, Feb. 17, 2003, https://www.dfat.gov.au/sites/default/files/SAFTA-chapter-14.pdf.
[90] Rep. of the Panel of Experts, Panel of Experts Proceeding Constituted Under Article 13.15 of the EU–Korea Free Trade Agreement, ¶¶ 55, 264, 277, 280, 282 (Jan. 20, 2021), https://trade.ec.europa.eu/doclib/docs/2021/january/tradoc_159358.pdf.

臺灣大學學術期刊資料庫

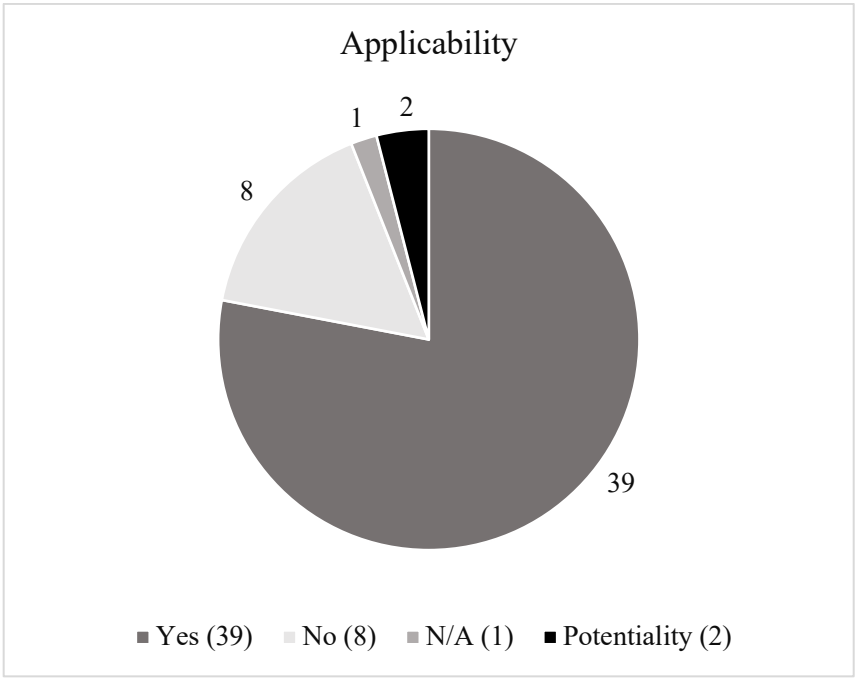


FIGURE 5: Distribution of DSM Applicability

The distribution suggests that a majority of states recognize the applicability of DSM to secure compliance with the "Transparency" and "Performance" commitments, although settlement of disputes arising from violating these commitments would only concern procedural issues pertaining to cooperation in the context of cybersecurity. Notwithstanding, substantive issues of cybersecurity may still be addressed, if they relate to alleged violations of other commitments. For example, the Appellate Body (AB) in *US — Gambling* indicated that internal practice of protecting cybersecurity would be tolerable if they have been designed to counter "a genuine and sufficiently serious threat . . . posed to one of the fundamental interests of society" and had no reasonable alternative.[91] In practice, one critical question arises: what if disputes arising from/related to cybersecurity are de facto "impossible cases" that frustrate "the willing participation of states, the substance of the rules and obligations, and the design and

[91] Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶¶ 297, 308-09, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005).

臺灣大學學術期刊資料庫

operation of the dispute settlement system itself"?[92] Recent development indicates that some states intend to ease the stresses on sovereignty and institutions when resorting to DSM, while maintaining predictability to a certain extent. For example, The Digital Economy Partnership Agreement mandates the parties to resort to a mediation mechanism where "[t]he mediator may offer advice and propose a solution for the consideration of the Parties to the mediation" without compelling the parties to accept or "comment[ing] on the consistency of the measure at issue with this Agreement."[93] This may help the parties achieve a compromised solution because "a mediator seeks to reduce the distance between the parties' positions and make the parties understand each other's point of view."[94] Besides, a few FTAs follow a middle-of-the-road approach which enables states to cultivate consensus in practice. For example, the Regional Comprehensive Economic Partnership (hereinafter ''the RCEP'') mandates the states to "refer the matter to the RCEP Joint Committee . . . to discuss differences that may arise regarding the interpretation or application of this Agreement and to issue interpretations of the provisions of this Agreement as it may deem appropriate and necessary," when they "fail to resolve the differences" after "consultations in good faith" to "make every effort to reach a mutually satisfactory solution." [95] In this regard, the RCEP Joint Committee may serve as a quasi-adjudicatory forum that help states clarify external uncertainties. In practice, the decision-making processes may signal "the process of geographic diffusion of a transnational mode . . . through the 'reception' of an emergent transnational mode, combining it with 'indigenous' elements, and the residuum of the previous mode . . . ."[96] Article 19.4 (General Provisions) and its footnote 2 of the RCEP provides that "[w]ith respect to any provision of the WTO Agreement that has been incorporated into this Agreement, the panel shall also consider relevant interpretations in reports of WTO panels and the WTO Appellate Body, adopted by the WTO Dispute Settlement Body;" and

---

[92] C. O'Neal Taylor, *Impossible Cases: Lessons from the First Decade of WTO Dispute Settlement*, 28(2) U. PA. J. INT'L ECON. L. 309, 328-29 (2007).

[93] Digital Economy Partnership Agreement art. 14B.4(4), June 11, 2020, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement (last visited Feb. 20, 2023). Apart from mediation, arbitration is also available to settle disputes pertaining to cybersecurity.

[94] Walter Mattli, *Private Justice in a Global Economy: From Litigation to Arbitration*, 55(4) INT'L ORG. 919, 927 (2001).

[95] Regional Comprehensive Economic Partnership Agreement arts. 12.17, 18.3, Nov. 15, 2020, https://rcepsec.org/legal-text/ (last visited Feb. 20, 2023) [hereinafter RCEP].

[96] Duncan Kennedy, *Three Globalizations of Law and Legal Thought: 1850–2000*, *in* THE NEW LAW AND ECONOMIC DEVELOPMENT: A CRITICAL APPRAISAL 19, 23 (David M. Trubek & Alvaro Santos eds., 2006).

臺灣大學學術期刊資料庫

> The Parties confirm that the first sentence of this paragraph does not prevent a panel from considering relevant interpretations in reports of WTO panels and the WTO Appellate Body adopted by the WTO Dispute Settlement Body, with respect to a provision of the WTO Agreement which is not incorporated into this Agreement.

Therefrom a new instrument may gradually emerge after future institutionalization:[97]

> As part of any general review of this Agreement undertaken in accordance with Article 20.8 (General Review), the Parties shall review the application of Chapter 19 (Dispute Settlement) to this Chapter [Electronic Commerce]. Following the completion of the review, Chapter 19 (Dispute Settlement) shall apply to this Chapter between those Parties that have agreed to its application.[98]

C. Appraisal

The aforementioned observations and analyses indicate that the cybersecurity provisions create no substantive standard for reconciling cybersecurity with trade; instead, they are similar to a "built-in agenda" open to future law-making processes. Essentially, they make no difference from other process commitments on cybersecurity outside the FTAs. For example, "Pillar I—Trade" of the Indo-Pacific Economic Framework for Prosperity (IPEF)[99] indicates that

> [w]e will seek to develop new and creative approaches to trade and technology policies that advance a broad set of objectives . . . [including] [a]dvancing inclusive digital trade by: building an environment of trust and confidence in the digital economy . . . and

---

[97] JAMES CRAWFORD, CHANCE, ORDER, CHANGE: THE COURSE OF INTERNATIONAL LAW, GENERAL COURSE ON PUBLIC INTERNATIONAL LAW 143 (2014).

[98] RCEP, *supra* note 95, art. 12.17 ¶ 3.

[99] Indo-Pacific Economic Framework for Prosperity (IPEF) was proposed by the US with the partnership of Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, and Vietnam. *See FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity*, THE WHITE HOUSE (May 23, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/; *FACT SHEET: Indo-Pacific Economic Framework for Prosperity Upskilling Initiative for Women and Girls*, U.S. DEP'T OF COM. (Sept. 8, 2022), https://www.commerce.gov/news/fact-sheets/2022/09/fact-sheet-indo-pacific-economic-framework-prosperity-upskilling.

臺灣大學學術期刊資料庫

> advancing resilient and secure digital infrastructure and platforms.[100]

Nevertheless, these open-ended cybersecurity provisions may bring about implicit and partial diversions from the pre-existing trade commitments, when the states exploit them to maintain flexibility in coordinating with the other party/parties in a trade to deal with cybersecurity issues: "treaties are time-bound promises or propositions that generally reflect a perspective at the time of being made. But . . . over time custom may actually be employed to 'mould and even modify' the content of otherwise static treaties." [101] For example, Viet Nam submitted a communication to New Zealand under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (hereinafter "CPTPP"), indicating that "[b]oth countries shall continue consultation on cooperation for the implementation of the Cyber Security Law of Viet Nam or related legislation concerning cyber security with a view to ensuring consistency with the Agreement."[102]

Consequently, some questions arise: will the trumping but marginal role of security vis-à-vis liberalization of trade[103] may have fewer constraints on domestic measures of cybersecurity? Will the requirement of "equal competitive conditions" by making "one group of services or products . . . not have any competitive advantage over another group" [104] has less significance in the context of cybersecurity? In other words, will the principles of non-discrimination, reciprocity and economic liberalism, which underpin the multilateral trading system,[105] become less relevant to check internal practice pertaining to cybersecurity in the trade as the cybersecurity provisions operate? Until now, these questions remain unanswered because the WTO e-commerce negotiations have not produced definitive outcomes yet.[106] Nevertheless, there is still a baseline in the multilateral trading system

---

[100] OFF. OF THE U.S. TRADE REPRESENTATIVE, MINISTERIAL TEXT FOR TRADE PILLAR OF THE INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY-INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY (IPEF): PILLAR I—TRADE 1 (May, 2022), https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text%20(Trade%20Pillar)_FOR%20PUBLIC%20RELEASE%20(1).pdf.

[101] CRAWFORD, *supra* note 97, at 143.

[102] N.Z. MINISTRY OF FOREIGN & TRADE, VIET NAM–NEW ZEALAND: CYBER SECURITY (Mar. 8, 2018), https://www.mfat.govt.nz/assets/Trade-agreements/CPTPP/Viet-Nam-New-Zealand-Cyber-Security.pdf.

[103] PETROS C. MAVROIDIS, THE REGULATION OF INTERNATIONAL TRADE (VOL. 1: GATT) 414-15 (2016).

[104] Appellate Body Report, *Argentina — Measures Relating to Trade in Goods and Services*, ¶ 6.144, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016).

[105] JOHN H. BARTON ET AL., THE EVOLUTION OF THE TRADE REGIME: POLITICS, LAW, AND ECONOMICS OF THE GATT AND THE WTO 39 (2008).

[106] WTO Joint Statement Initiative on Electronic Commerce, *WTO Electronic Commerce Negotiations—Consolidated Negotiating Text – December 2020*, WTO Doc. INF/ECOM/62/Rev.1

臺灣大學學術期刊資料庫

that there should not be "a broad defence for measures in FTAs that roll back on Members' rights and obligations under the WTO covered agreements".[107]

> Article XXIV conditions such departures on the fulfilment of the rule that the level of duties and other regulations of commerce, applicable in each of the FTA members to the trade of non-FTA members, shall not be higher or more restrictive than those applicable prior to the formation of the FTA.[108]

IV. THE NORM-MAKING PROCESSES ON CYBERSECURITY UNDER THE UN: AN EMERGING MINIMUM ORDER

A. An Overview

Built on "Role of science and technology in the context of security, disarmament and other related fields,"[109] the UN has started to engage in norm-making processes on cybersecurity since 1998 when Russia sponsored a resolution to include the item entitled *Developments in the field of information and telecommunications in the context of international security* in the First Committee's agenda.[110] Similar with the circumstance under the multilateral trading system, the decision-making processes are multi-forum under the auspice of the UN General Assembly (hereinafter ''UNGA'') as specified in Table 3:

(Dec. 14, 2020).

[107] Appellate Body Report, *Peru — Additional Duty on Imports of Certain Agricultural Products*, ¶ 5.116, WTO Doc. WT/DS457/AB/R (adopted July 31, 2015).

[108] *Id.* at ¶ 5.112.

[109] Motaz M. Zahran (Rapporteur of the First Committee), *Role of Science and Technology in the Context of Security, Disarmament and Other Related Fields Rep. of the First Committee*, ¶¶ 5-6, U.N. Doc. A/53/576 (Nov. 18, 1998).

[110] Permanent Representative of the Russian Federation to the U.N., Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations Addressed to the Secretary-General, at 2-4, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998).

臺灣大學學術期刊資料庫

TABLE 3: The Multi-Forum Decision-Making Processes[111]

Forum	Scope
The First Committee	(de-)militarization of cyberspace
The Second Committee	Regulatory norms of protecting cybersecurity
The Third Committee	(de-)criminalization of cyberspace

These deliberative streams have certain interplay as they refer to each other. For example, the UNGA resolution on the report of the Third Committee (A/74/401) was "[r]ecalling also the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which is of the view that States should consider how best to cooperate to prosecute the criminal use of information and communications technologies." [112] Nevertheless, they produced different outcomes: the decision-making processes on cybersecurity under the Second Committee discontinued after 2010, although it produced three resolutions that crystallize some regulatory norms of protecting cybersecurity. Simultaneously, the processes left countries such as China and Russia side.[113] The Third Committee has established the Ad Hoc Committee (AHC) with the purpose of forming a treaty that binds states to counter cybercrimes,[114] but the negotiations on "a comprehensive international convention on countering the use of information and communications technologies for criminal purposes"[115] are far from being concluded. Conversely, the First Committee has convened six Governmental Groups of Experts (hereinafter "GGEs") and an Open-ended Working Group (hereinafter "OEWG") to develop non-binding norms voluntarily adopted by states to apply in protecting cybersecurity. Until now, the GGEs have developed eleven norms that states have reached general consensus. In this regard, the following subsections will mainly focus on the norm-making processes under the auspice of the First Committee for the sake of relevance.

[111] Christian Henderson, *The United Nations and the Regulation of Cyber-Security*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 582, 584-89 (Nicholas Tsagourias & Russell Buchan eds., 2d ed. 2021).
[112] G.A. Res. 74/247, at 1-3 (Jan. 20, 2020).
[113] Henderson, *supra* note 111, at 586-88.
[114] *Id.* at 589-601.
[115] *See generally* Chair's Rep. of the Second Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, U.N. Doc. A/A C.291/CRP.12 (July 6, 2022).

臺灣大學學術期刊論文

B. Non-Legalized Obligation as Emerging Custom

The eleven non-binding norms of responsible state behavior are as specified in Table 4:

TABLE 4: The Norms[116]

<table>
<tr><th>Do's</th><th>Don'ts</th></tr>
<tr><td>Consistent with the purposes of the UN to collectively maintain peace and security in cyberspace (a)</td><td rowspan="2">Connivance of internationally wrongful acts using ICTs (c)</td></tr>
<tr><td>Due diligence before attribution (b)</td></tr>
<tr><td>Best efforts in cooperation (d)</td><td rowspan="6">To intentionally harm computer emergency response teams (CERTs)/cybersecurity incident response teams (CSIRTs) or use them in malicious international activity (k)</td></tr>
<tr><td>To respect human rights (e)</td></tr>
<tr><td>To protect critical infrastructure from ICT threats (g)</td></tr>
<tr><td>To provide necessary assistance (h)</td></tr>
<tr><td>To ensure the integrity of supply chain (i)</td></tr>
<tr><td>To report ICT vulnerabilities and share information on available remedies to such vulnerabilities (j)</td></tr>
</table>

[116] U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 13, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter U.N. Doc. A/70/174]; U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, at 8-17, U.N. Doc. A/76/135 (July 14, 2021) [hereinafter U.N. Doc. A/76/135].

臺灣大學學術期刊資料庫

Evidently, the norms are a set of framework standards that guide states to behave properly in risk management, reporting vulnerabilities and resolving information and communications technology (hereinafter "ICT") incidents to prevent critical infrastructure (CI) and supply chains (SCs) from cybersecurity threats.[117] In particular, the tentative classification of prohibitive conducts against cybersecurity seems to be an effort to identify misconducts against cybersecurity because a wide range of active measures in cyberspace need no justification under international law in practice.[118] Nevertheless, its effectiveness is questionable because the norms prescribe no consequence for disobedience,[119] especially when the norms "do not seek to limit or prohibit action that is otherwise consistent with international law."[120] In this regard, international law instead of the norms should decide the legality of state behavior in cyberspace: specifically, it includes that the principles of the UN Charter, other international law including international humanitarian law and state responsibility,[121] and "international norms and principles that flow from sovereignty."[122] This all-encompassing enumeration represents that all present and future rules based on state consent, including the trade rules, belong to "applicable international law to cyberspace." Uncertainty may emerge because most of the pre-existing international rules have not originally been designed to resolve cybersecurity issues; therefore, direct application is unlikely without reconstruction. Just as the International Court of Justice (hereinafter "ICJ") indicated in the *Fisheries* case,

> [A]lthough the ten-mile rule has been adopted by certain States both in their national law and in their treaties and conventions, and although certain arbitral decisions have applied it as between these States, other States have adopted a different limit. Consequently, the ten-mile rule has not acquired the authority of a general rule of international law.[123]

Then, another question arises: what is the legal status of the norms and the commitment to recognize the applicability of international law? In the advisory opinion *Certain Expenses of the United Nations*, the ICJ indicated that

---

[117] U.N. Doc. A/76/135, *supra* note 116, at ¶¶ 56-68.
[118] HENNING LAHMANN, UNILATERAL REMEDIES TO CYBER OPERATIONS: SELF-DEFENCE, COUNTERMEASURES, NECESSITY, AND THE QUESTION OF ATTRIBUTION 125 (2020).
[119] H. L. A. HART, THE CONCEPT OF LAW 82-91 (Penelope A. Bulloch & Joseph Raz eds., 2d ed. 1994).
[120] U.N. Doc. A/76/135, *supra* note 116, at ¶15.
[121] *Id.* at ¶ 71(f)-(g).
[122] *Id.* at ¶¶70, 71(b).
[123] Fisheries (U.K. v. Nor.), Judgment, 1951 I.C.J. 116, at 131 (Dec. 18).

臺灣大學學術期刊資料庫

> [T]he functions and powers conferred by the Charter on the General Assembly are not confined to discussion, consideration, the initiation of studies and the making of recommendations; they are not merely hortatory. Article 18 deals with 'decisions' of the General Assembly 'on important questions'. These 'decisions' do indeed include certain recommendations, but others have dispositive force and effect. . . . [A]nd it is the General Assembly which decides and whose decision determines status.[124]

Analogically, the norm-making processes on cybersecurity should be recognized as falling into the scope of "[d]ecisions of the General Assembly on important questions:" the UNGA in the resolution 76/19 "[w]elcomes"[125] it to "reflect the expectations of the international community and set standards for responsible State behaviour" as well as to recognize international law as "the basis for States' shared commitment to preventing conflict and maintaining international peace and security."[126] In this regard, the norms and the commitment to recognize the applicability of international law can be regarded as evidence of "a proto-legal step in order to establish . . . subsequent legal rule[s],"[127] but they are not *lex lata* yet.

C. Embedded Mechanisms of Delegation

The norm-making processes develop no administrative and/or enforcement mechanism; instead, states use the strategy of networking to realize enforcement and implementation of the norm-law institution. Firstly, states may voluntarily use "bilateral, sub-regional, regional and multilateral fora and informal consultations"[128] with the purpose of cultivating common understanding of cybersecurity and mitigating the digital divide disabling "states to secure ICTs and ensure their peaceful use" in the international community and others.[129] Therefore, decision-making processes on cybersecurity under other forums could have impacts on the norm-making processes. Nevertheless, the interactions are not balanced because states have little concordant collaboration at the universal level. For example, inter-organizational collaboration between the UN and the WTO under the UN Economic and Social Council (ECOSOC) are limited to the members of the Economic Commission for Europe (hereinafter ''ECE''): they address cybersecurity issues concerning trade facilitation through regular staff

[124] Certain Expenses of the United Nations (Article 17, paragraph 2, of the Charter), Advisory Opinion, 1962 I.C.J. 151, at 163 (July 20).
[125] G.A. Res. 76/19, ¶ 2 (Dec. 8, 2021).
[126] U.N. Doc. A/76/135, *supra* note 116, at ¶¶ 15, 69.
[127] CRAWFORD, *supra* note 97, at 80.
[128] U.N. Doc. A/76/135, *supra* note 116, at ¶¶ 76-86.
[129] U.N. Doc. A/70/174, *supra* note 116, at ¶¶ 19-21.

臺灣大學學術期刊資料庫

meeting outside the interagency group[130] in reference to the ECE's common regulatory framework on cybersecurity.[131] Furthermore, private actors may also influence the norm-making processes: states are recommended to "involv[e] other stakeholders such as the private sector, academia, civil society and the technical community [which] can help States apply the framework for the responsible behaviour of States in their use of ICTs" as well as to voluntarily support each other in "[i]mproving the security, resilience and protection of critical infrastructure."[132] Nevertheless, "more informed and less biased rules and decisions than either these institutions' officials or those they directly or indirectly govern would achieve on their own" do not necessarily emerge from these cooperative activities unless there is "effective engagement with external epistemic agents."[133]

Secondly, pre-existing secondary rules of *lex generalis* and *lex specialis,* including the trade rules should have served as the mechanisms for settling disputes involving cybersecurity as "[t]he Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law."[134] Nevertheless, those networked dispute settlement mechanisms are actually dysfunctional in practice because reconstruction of pre-existing international rules is yet to be finished. Simultaneously, many misconducts fall outside the scope of CIL on state responsibility because they do not satisfy the established standards of attribution such as "overall control" or "effective control." For example, states are increasingly involved in activities of cyber mercenaries against cybersecurity, including the extension of "passive support to the proxies but does not establish clear oversight mechanisms over their operations."[135] Nevertheless, both the standards of "overall control" and "effective control" require active involvement, although they require different degrees of control: "overall control" requires

> The Assembly and its leaders played a role in the overall conduct of the war both in the Republic of Bosnia and Herzegovina and beyond, in addition to the supply of paramilitary forces to

[130] *See* U.N. Econ. & Soc. Council, Econ. Comm'n for Eur., Rep. of the Activities Under the Grp. of Experts on Managing Risks in Regulatory Systems, ¶¶ 2-16, U.N. Doc. ECE/CTCS/WP.6/2020/5 (Aug. 21, 2020).
[131] *See, e.g.*, U.N. Econ. & Soc. Council, Econ. Comm'n for Eur., Draft Proposal for a Common Regulatory Framework on Cybersecurity, U.N. Doc. ECE/CTCS/WP.6/2018/9 (Sept. 10, 2018).
[132] U.N. Doc. A/76/135, *supra* note 116, at ¶¶ 87, 89(c).
[133] David Lefkowitz, *The Legitimacy of International Law*, *in* GLOBAL POLITICAL THEORY 98, 106 (David Held & Pietro Maffettone eds., 2016).
[134] U.N. Doc. A/76/135, *supra* note 116, at ¶ 71(g).
[135] U.N. Secretary-General, *Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, ¶ 31, U.N. Doc. A/76/151 (July 15, 2021).

臺灣大學學術期刊資料庫

> supplement the fighting strength of the new VRS units, which forces took part in the military operations . . . .[136]

while "effective control" needs more than "the selection of its military or paramilitary targets, and the planning of the whole of its operation."[137] Therefore, states are increasingly tilting to use means of self-help to relieve losses instead of submitting to third-party adjudication.[138]

D. Appraisal

The aforementioned analyses indicate that the norm-making processes on cybersecurity under the UN may create a minimum public order featured as "the global state of affairs with limited recourse to unauthorized violence to solve disputes."[139] However, they are far from legally authoritative to mediate conflicting interests between the states in the context of cybersecurity. Simultaneously, it appears that international law is tacitly sidelined because it always leaves a question open in terms of how to apply.[140] For example, in a resolution adopting

> Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society," the UNGA indicated that "[w]e recognize the important role of international law . . . in building confidence and security in the use of information and communications technologies by States . . . however, about certain growing uses of information and communications technologies that threaten security and development benefits . . . .We reiterate our belief that a global culture of cybersecurity needs to be promoted and developed and that cybersecurity measures should be implemented in cooperation with all stakeholders and international expert bodies in order to foster trust and security in the information society.[141]

---

[136] Prosecutor v. Tadić, Case No. IT-94-1-I, Opinion and Judgment, ¶ 599 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997).

[137] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27) [hereinafter Military and Paramilitary Activities in and Against Nicaragua].

[138] *See, e.g.*, OFF. OF FIN. SANCTIONS IMPLEMENTATION, CONSOLIDATED LIST OF FINANCIAL SANCTIONS TARGETS IN THE UK (May 7, 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088191/Cyber.pdf.

[139] Steven R. Ratner, *Between Minimum and Optimum World Public Order: An Ethical Path for the Future*, *in* LOOKING TO THE FUTURE: ESSAYS ON INTERNATIONAL LAW IN HONOR OF W. MICHAEL REISMAN 195, 195 (Mahnoush H. Arsanjani et al. eds., 2011).

[140] Nico Krisch, *The Decay of Consent: International Law in an Age of Global Public Goods*, 108(1) AM. J. INT'L L. 1, 34 (2014).

[141] G.A. Res. 70/125, ¶¶ 51-52 (Feb. 1, 2016).

臺灣大學學術期刊資料庫

This wording, in fact, calls in question the functionality of international law in the context of cybersecurity as it is not inclusive enough for all stakeholders.

Consequently, two potentialities may arise: one is that the proxies to decide the legality of state behavior in cyberspace will be low: states may only need to observe "the very minimum of the obligation to respect and to preserve the territorial integrity and political independence of other members" as well as those rules that "perfor[m] in wars between sovereign States, namely, to humanize and regularize the conduct of hostilities as between the parties."[142] For example, some states attempt to expand the inherent right of self-defense. Australia proposes that anticipatory self-defense is feasible in protecting cybersecurity because "[t]he rapidity of cyber activities, as well as their potentially concealed and/or indiscriminate character" will make "the victim . . . lose its last opportunity to effectively defend itself unless it acts."[143] Correspondingly, some states such as Germany and Israel propose that states may exercise the right to self-defense against non-state actors in an actual or imminent armed attack in cyber domain in considering the prevailing misconducts of non-state actors in cyberspace.[144] Nevertheless, the ICJ indicated that a state may invoke self-defense when a conduct against it constitutes "acts of armed force against another State of such gravity as to amount to' (inter alia) an actual armed attack conducted by regular forces . . . ."[145] Therefore, an expansive interpretation of the right to self-defense would "render the efforts and restrictions placed into Article 51 almost meaningless . . . ."[146]

The other is a stake that "a State may be held to be bound by a norm to the creation of which it objected."[147] The reason is that participation of states in the norm-making processes is still limited, although the OEWG enables "all Member States . . . [to] engage in interactive discussions and share their

---

[142] SIR HERSCH LAUGHTERPACHT, RECOGNITION IN INTERNATIONAL LAW 245, 417 (Cambridge University Press 2013) (1947).

[143] *Annex B: Australia's Position on How International Law Applies to State Conduct in Cyberspace*, AUSTRALIAN GOV'T, https://www.internationalcybertech.gov.au/our-work/annexes/annex-b (last visited Mar. 19, 2023).

[144] Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INT'L L. STUD. 395, 399 (2021); Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, U.N. Doc. A/76/136, at 20 (July 13, 2021) [hereinafter U.N. Doc. A/76/136].

[145] Military and Paramilitary Activities in and Against Nicaragua, *supra* note 137, at ¶ 195.

[146] NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 58 (2010).

[147] Joseph H. H. Weiler, *Introduction* to *Are We Heading For a New Normativity in the International Community?*, *in* CHANGE AND STABILITY IN INTERNATIONAL LAW-MAKING 63, 64 (Antonio Cassese & Joseph H. H. Weiler eds., 1988).

臺灣大學學術期刊資料庫

views, which the Chair shall convey to the group of governmental experts for consideration."[148] In this regard, a situation that "the general practice of States is predicated on the conduct of a relatively small number of States"[149] may arise owing to the asymmetric participation of states. For example, Japan stated in the voluntary submission that

> [i]t should be noted that international law applicable to cyber operations is not limited to those mentioned in this document. . . . Treaty provisions related to the Data Free Flow with Trust principle, for which Japan is promoting rule-making under the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the Japan-U.S. Digital Trade Agreement, and the Japan-UK Economic Partnership Agreement, also constitute international law applicable to some aspects of cyber operations."[150]

Conversely, a majority of the African countries are silent on the norm-making processes, while some of them, such as Djibouti, Côte d'Ivoire and others, are still expressing needs for expanding Internet access and other capacity building without addressing substantive issues of the norms and applicable international law.[151] Nevertheless, the silence of states on certain conduct should "not [be] that they recognized themselves as being obliged to do so; for only if such abstention were based on their being conscious of having a duty to abstain would it be possible to speak of an international custom."[152]

---

[148] G.A. Res. 73/266, ¶ 5 (Jan. 2, 2019).

[149] YORAM DINSTEIN, THE INTERACTION BETWEEN CUSTOMARY INTERNATIONAL LAW AND TREATIES 283 (2007).

[150] U.N. Doc. A/76/136, *supra* note 144, at 45-46.

[151] *See, e.g.*, Declaration de Djibouti: A La Premiere Session de Fond du Groupe de Travail A Composition Non Limitée sur la Securité de l'Utilisation des Technologie de l'Information 2021-2025, Delivre par Mme Zeinab Ismael Assoweh, Conseillère à la Mission Permanente Auprès des Nations Unies [Djibouti Declaration: At the First Substantive Session of the Open-Ended Working Group on the Security of the Use of Information Technology 2021-2025, Delivered by Ms. Zeinab Ismael Assoweh, Counselor at the Permanent Mission to the United Nations] (Dec. 14, 2021), https://documents.unoda.org/wp-content/uploads/2022/01/DECLARATION-CYBERSECURITE.pdf; Renforcement des Capacités, Intervention de S.E.M. Désiré Wulfran G. Ipo Ambassadeur, Représentant Permanent Adjoint de La République de Côte D'Ivoire auprès des Nations Unies [Capacity Building, Intervention of H.E. Désiré Wulfran G. Ipo Ambassador, Deputy Permanent Representative of the Republic of Côte d'Ivoire to the United Nations] (Mar. 31, 2022), https://documents.unoda.org/wp-content/uploads/2022/04/Declaration-de-la-CI-2e-SESSION-DE-FOND-OEWG-30.3.2022.pdf.

[152] S.S. Lotus (Fr. v. Turk.), Judgement, 1927 P.C.I.J. (ser. A) No. 10, ¶ 76 (Sept. 7).

臺灣大學學術期刊資料庫

V. SOFT LEGALIZATION AS RECALIBRATION?

This section discusses what soft legalization of the cybersecurity provisions in the FTAs and the norm-making processes on cybersecurity under the UN means to the multilateral trading system. Then, this article will discuss if institutional linkages could be a mitigator to disruptions arising from the soft legalization of cyberspace.

A. An Appraisal

The aforementioned observations indicate that cybersecurity is situated in the flux of numerous communicative flows[153] which reflect a shared understanding of states: *lex generalis* and *lex specialis* at the international level need to give greater attention to cybersecurity, but they fall short in regulation. As the shared understanding triggers interactions between different decision-making processes,[154] the norm-making processes on cybersecurity under the UN may integrate with the multilateral trading system through the cybersecurity provisions in the FTAs. For example, "Our Common Agenda" released by the UN the Secretary-General indicated that "[t]he World Trade Organization (WTO) is being reinvigorated and updated to take account of twenty-first century realities, such as electronic commerce and the digital economy," when proposing a preparation for

> a Global Digital Compact . . . [that] would outline shared principles for an open, free and secure digital future for all . . . include[ing]: reaffirming the fundamental commitment to connecting the unconnected; avoiding fragmentation of the Internet; providing people with options as to how their data is used; application of human rights online; and promoting a trustworthy Internet by introducing accountability criteria for discrimination and misleading content.[155]

In this regard, the pre-established standards under the multilateral trading system may not be the main criteria to assess state behavior in the context of cybersecurity. In other words, the trade rules have less capacity to mediate between the sovereign right to regulate and the pursuit of trade interests in the context of cybersecurity, but such a capacity is the cornerstone

---

[153] W. Michael Reisman, *International Lawmaking: A Process of Communication: The Harold D. Lasswell Memorial Lecture*, *in* 75 PROCEEDINGS OF THE ASIL ANNUAL MEETING 101, 105 (1981).
[154] JUTTA BRUNNÉE & STEPHEN J. TOOPE, LEGITIMACY AND LEGALITY IN INTERNATIONAL LAW: AN INTERACTIONAL ACCOUNT 71-72 (James Crawford et al. eds., 2010).
[155] U.N. SECRETARY-GENERAL, OUR COMMON AGENDA – REPORT OF THE SECRETARY-GENERAL, ¶¶ 74, 93, U.N. Sales No. E.21.I.8 (2021).

臺灣大學學術期刊資料庫

of the multilateral trading system.[156] Consequently, the cybersecurity conundrum in trade emerges, which signals "decoupling"[157] of trade and cybersecurity because the trade rules "designed to cushion the domestic economy from external disruptions . . . [can no longer] be commensurate with the degree of external disturbance and compatible with the long-term expansion of international transactions."[158]

Nevertheless, what triggers the "decoupling" of cybersecurity from trade, or, precisely, the embedded liberalism underpinning the post-war economic order?[159] What does the "decoupling" mean to the multilateral trading system? A workable explanation is that a compromise that enables "multilateralism [to] be predicated upon domestic interventionism"[160] did not take place in digitalized trade; instead, its emergence was mercantilist: "the centralized state was a new creation called forth by the Commercial Revolution which had shifted the center of gravity of the Western world from the Mediterranean to the Atlantic seaboard and thus compelled the backward peoples of larger agrarian countries to organize for commerce and trade."[161] For example, on July 1, 1997, the then-President of the US, Bill Clinton advocated in *The Framework for Global Electronic Commerce* (hereinafter "FGEC") that "private sector . . . to lead," while "governments should encourage industry self-regulation wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet." Simultaneously, the FGEC called for states to yield their sovereign jurisdiction and the right to regulate to "consistent principles . . . that lead to predictable results" because they "support[] commercial transactions on the Internet."[162] In other words, it meant that governments should adopt a minimalist approach to design their domestic regulation to enter into the global Internet market.

Inequality thereupon arises because the minimalist approach has been underpinned by robust private sectors at the domestic level and sovereign power to diffuse domestic policy to the international plane.[163] Nevertheless, almost all developing countries lacked these two elements. Therefore, they

---

[156] John Gerard Ruggie, *International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order*, 36(2) INT'L ORG. 379, 393, 405 (1982).

[157] "Decouple" in this article means "to separate from someone or something else; to separate something from something else that it was joined to or part of." *See Decouple*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/decouple (last visited Jan. 2, 2022).

[158] Ruggie, *supra* note 156, at 405.

[159] *Id.* at 379-415.

[160] *Id.* at 393.

[161] KARL POLANYI, THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME 69 (2001).

[162] *Read the Framework*, NATIONAL ARCHIVES, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html (last visited Feb. 17, 2023).

[163] ROXANA RADU, NEGOTIATING INTERNET GOVERNANCE 43-112 (2019); Shin-yi Peng, *The Uneasy Interplay Between Digital Inequality and International Economic Law*, 33(1) EUR. J. INT'L L. 205, 207-15 (2022).

臺灣大學學術期刊資料庫

have to "subordinate the substance of society itself to the laws of the market"[164] by accepting such a practice. Simultaneously, redefinition and adaption of the external norms oftentimes accompany their reception, leveraging the pre-existing order when they are uploaded by sovereign and social actors transnationally.[165] These interactive processes further challenge the legitimacy and stability of the pre-existing order, prompting states to renegotiate "the boundary between the constraints that apply to actors in cyberspace and their autonomy"[166] by maintaining "a high degree of fluidity in the making and remaking of coalitions."[167] Otherwise, states will continuously be trapped in a predicament: either they have a fat chance to successfully invoke a defense[168] or there is a stake of encroaching sovereign autonomy. In *United States — Restrictions on Imports of Tuna*, the Panel

> considered that if . . . each contracting party could unilaterally determine the life or health protection policies from which other contracting parties could not deviate without jeopardizing their rights under the General Agreement[,] [t]he General Agreement would then no longer constitute a multilateral framework for trade among all contracting parties but would provide legal security only in respect of trade between a limited number of contracting parties with identical internal regulations.[169]

Notwithstanding, provided that "every country [has the right] to adopt the economic and social system that it deems the most appropriate for its own development and not to be subjected to discrimination of any kind as a result,"[170] does the multilateral trading system really have the legitimacy to require states to design their internal practice to be not predicated on "unilateral character?"[171]

---

[164] POLANYI, *supra* note 161, at 75; H. Jeffrey Leonard, *Review: Multinational Corporations and Politics in Developing Countries*, 32(3) WORLD POL. 454, 456 (1980).
[165] Amitav Acharya, *How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism*, 58(2) INT'L ORG. 239, 251 (2004); Matthew S. Erie, *Chinese Law and Development*, 62(1) HARV. INT'L L.J. 51, 65 (2021).
[166] Kubo Mačák, *From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers*, 30(4) LEIDEN J. INT'L L. 877, 879 (2017).
[167] HAROLD D. LASSWELL & MYRES S. MCDOUGAL, JURISPRUDENCE FOR A FREE SOCIETY: STUDIES IN LAW, SCIENCE AND POLICY 442 (1992).
[168] Daniel Rangel, *WTO General Exceptions: Trade Law's Faulty Ivory Tower*, PUBLIC CITIZEN (Feb. 4, 2022), https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.
[169] Report of the Panel, *United States — Restrictions on Imports of Tuna*, ¶ 5.27, GATT Doc. DS21/R – 39S/155 (circulated Sept. 3, 1991).
[170] G.A. Res. S-6/3201, ¶ 4(d) (May 1, 1974).
[171] MAVROIDIS, *supra* note 103, at 419.

臺灣大學學術期刊資料庫

B. Will Institutional Linkages Be a Way to Recoupling?

This article considers that the "decoupling" of cybersecurity from trade is transitory and ostensible without leading to a thorough transformation of the multilateral trading system: "as long as the purpose is held constant, there is no reason to suppose that the normative framework of regimes must change as well."[172] It is undeniable that one purpose of the multilateral trading system still lies on "promoting the interests of all participants on a mutually advantageous basis and at securing an overall balance of rights and obligations, while giving due respect to national policy objectives."[173] Nevertheless, the "decoupling" may help recalibrate the operation of the multilateral trading system originally rooted in "international fair dealing."[174] This article proposes that enlargement of institutional linkages between the UN decision-making processes and WTO[175] could be a way to recouple cybersecurity and trade. The reason is that linkages between the decision-making processes under the UN and multilateral trading system may enable conceptual interactions that "produce and disseminate authoritative ways of understanding and organizing the world."[176] This may further ensure coherent "multilevel governance" of interdependent public goods that are often neglected by regimes arising from reciprocity.[177] The ultimate goal is to establish interfunctional linkages between trade and cybersecurity,[178] but it depends on whether states could network and institutionalize the decision-making processes under both forums "without taking control of society as a whole, but respecting the *eigen*-rationalities of the subsystems."[179] Ideally, there would be "a set of legal principles of paramount importance for every one of the subjects belonging to the social community ruled by it"[180] because state behavior of protecting cybersecurity "should, to the extent possible, be interpreted so as to give rise to a single set

---

[172] Ruggie, *supra* note 156, at 384.

[173] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167, at 285.

[174] William S. Culbertson, *Introduction* to HUGH O. DAVIS, AMERICA'S TRADE EQUALITY POLICY vii, vii.

[175] General Council, *Arrangements for Effective Cooperation with Other Intergovernmental Organizations-Relations Between the WTO and the United Nations*, WTO Doc. WT/GC/W/10 (Nov. 3, 1995).

[176] Jeffrey L. Dunoff, *A New Approach to Regime Interaction*, *in* REGIME INTERACTION IN INTERNATIONAL LAW: FACING FRAGMENTATION 136, 167 (Margaret A. Young ed., 2012).

[177] Ernst-Ulrich Petersmann, *The Future of the WTO: From Authoritarian Mercantilism to Multilevel Governance for the Benefit of Citizens*, 6(1) ASIAN J. WTO & INT'L HEALTH L. & POL'Y 45, 49-50 (2011).

[178] JOEL P. TRACHTMAN, THE ECONOMIC STRUCTURE OF INTERNATIONAL LAW 200-01 (2009).

[179] Ino Augsberg, *Carl Schmitt's Fear: Nomos – Norm – Network*, 23(4) LEIDEN J. INT'L L. 741, 757 (2010).

[180] PIERRE-MARIE DUPUY, THE CONSTITUTIONAL DIMENSION OF THE CHARTER OF THE UNITED NATIONS REVISITED 3 (1997).

臺灣大學學術期刊資料庫

of compatible obligations."[181] Therefrom the cybersecurity conundrum could be resolved because the rules under one institution will turn into interpretative instruments and/or gap-fillers to what have been left by the others.[182] Just as Professor Jessup indicated that "while diversity of law among interacting groups has been tolerated, uniformity has often been sought as an end in itself . . . on the international level;" therefore, "international law is not a random collection of such norms"[183] that "[w]e may find that many of the processes . . . can make their contribution to that international harmony which it is the function of international law to promote and which may best be attained by gradual stages."[184]

VI. CONCLUSION

The assessments of the cybersecurity provisions in the FTAs and the norm-making processes on cybersecurity under the UN indicated that cybersecurity has been softly legalized: claims on a minimum public order in cyberspace derogate the post-war embedded liberalism which seeks economic liberalization with limited government interventions. Thus, recalibration of the multilateral trading system in the form of "decoupling" cybersecurity from trade emerges. Specifically, it attributes to the interactive processes between emerging states and the pre-existing norm-makers: on the one hand, there are adaption and reconstruction of the rules "being inequitable and . . . perpetuating the interests of the economically advantaged countries" in order to not accede "to every international law obligation (including treaties) incumbent upon the parent state."[185] On the other hand, the adaption *de facto* leverages the pre-existing order. Potentially, institutional linkages would be a way to recouple trade and cybersecurity, but international law "lacks regular and comprehensive mechanisms of centralized enforcement and thus has to live with auto-determination and self-help, reciprocity will remain a major *leitmotiv*."[186] Therefore, the outcome of the recalibration depends on whether states can uphold "the

[181] Int'l Law Comm'n, Rep. on the Work of Its Fifty-Eighth Session, at 408, ¶ 251(4), U.N. Doc. A/61/10 (1 May-9 June and 3 July-11 Aug., 2006) [hereinafter U.N. Doc. A/61/10].
[182] Joost Pauwelyn, *The Role of Public International Law in the WTO: How Far Can We Go?*, 95(3) AM. J. INT'L L. 535, 553-578 (2001); Anastasios Gourgourinis, *General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System*, 22(4) EUR. J. INT'L L. 993, 1004-16 (2011).
[183] U.N. Doc. A/61/10, *supra* note 181, at 407, ¶ 251(1).
[184] Philip C. Jessup, *Diversity and Uniformity in the Law of Nations*, 58(2) AM. J. INT'L L. 341, 342, 344 (1964).
[185] ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 11-13 (1994).
[186] Application of the Interim Accord of 13 September 1995 (the former Yugoslav Republic of Macedonia v. Greece), Judgment, 2011 I.C.J. 644, ¶ 10 (Dec. 5, 2011) (separate opinion by Simma, J.).

臺灣大學學術期刊資料庫

principle of public right . . . over the individual interests of particular nations . . . that they should agree to coöperate in a common cause, and that they should so act that the guiding principle of that common cause shall be even-handed and impartial justice."[187] Otherwise, frictions will endure if states consider "necessary to maintain ascendancy at home" and/or misappraises owing to information asymmetry.[188] In particular, it appears that soft legalization seemingly confer to states the reminiscent right of recourse to "just war" that "le coeur de cette doctrine réside dans le fait que le fait que la guerre ne se justifie que comme sanction d'un tort subi. La guerre n'est en droit et en morale licite que comme «guerre-sanction»."[189]

[187] Woodrow Wilson, President of the U.S., Address delivered at the First Annual Assemblage of the League to Enforce Peace: "American Principles", THE AMERICAN PRESIDENCY PROJECT (May 27, 1916), https://www.presidency.ucsb.edu/node/206570.

[188] LASSWELL & MCDOUGAL, *supra* note 167, at 443.

[189] ROBERT KOLB, LE DROIT RELATIF AU MAINTIEN DE LA PAIX INTERNATIONALE: EVOLUTION HISTORIQUE VALEURS FONDATRICES ET TENDANCES AUTUELLES [THE LAW RELATING TO THE MAINTENANCE OF INTERNATIONAL PEACE: HISTORICAL EVOLUTION FOUNDING VALUES AND ACTUAL TRENDS] 16 (A. Pedone ed., 2005).

臺灣大學學術期刊資料庫

REFERENCES

Books

1 MAVROIDIS, PETROS C. (2016), THE REGULATION OF INTERNATIONAL TRADE (VOLUME 1: GATT).

2 MAVROIDIS, PETROS C. (2016), THE REGULATION OF INTERNATIONAL TRADE (VOLUME 2: THE WTO AGREEMENTS ON TRADE IN GOODS) .

7 LASSWELL, HAROLD D. & MYRES S. MCDOUGAL (1992), JURISPRUDENCE FOR A FREE SOCIETY: STUDIES IN LAW, SCIENCE AND POLICY.

BARTON, JOHN H. ET AL. (2008), THE EVOLUTION OF THE TRADE REGIME: POLITICS, LAW, AND ECONOMICS OF THE GATT AND THE WTO.

BIEHLER, GERNOT (2008), PROCEDURES IN INTERNATIONAL LAW.

BRUNNÉE, JUTTA & STEPHEN J. TOOPE (2010), LEGITIMACY AND LEGALITY IN INTERNATIONAL LAW: AN INTERACTIONAL ACCOUNT, James Crawford et al. eds.

CHOUCRI, NAZLI & DAVID D. CLARK (2019), INTERNATIONAL RELATIONS IN THE CYBER AGE: THE CO-EVOLUTION DILEMMA.

CRAWFORD, JAMES (2014), CHANCE, ORDER, CHANGE: THE COURSE OF INTERNATIONAL LAW.

DINSTEIN, YORAM (2007), THE INTERACTION BETWEEN CUSTOMARY INTERNATIONAL LAW AND TREATIES.

DUPUY, PIERRE-MARIE (1997), THE CONSTITUTIONAL DIMENSION OF THE CHARTER OF THE UNITED NATIONS REVISITED.

GUZMAN, ANDREW T. (2008), HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY.

HART, H. L. A. (1998), THE CONCEPT OF LAW, Penelope A. Bulloch & Joseph Raz eds., 2d ed.

HIGGINS, ROSALYN (1995), PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT.

IKENBERRY, G. JOHN (2011), LIBERAL LEVIATHAN: THE ORIGINS, CRISIS, AND TRANSFORMATION OF THE AMERICAN WORLD ORDER.

KOLB, ROBERT (2005), LE DROIT RELATIF AU MAINTIEN DE LA PAIX INTERNATIONALE: EVOLUTION HISTORIQUE VALEURS FONDATRICES ET TENDANCES AUTUELLES [THE LAW RELATING TO THE MAINTENANCE OF INTERNATIONAL PEACE: HISTORICAL EVOLUTION FOUNDING VALUES AND ACTUAL TRENDS].

KOREMENOS, BARBARA (2016), THE CONTINENT OF INTERNATIONAL LAW: EXPLAINING AGREEMENT DESIGN.

LAHMANN, HENNING (2020), UNILATERAL REMEDIES TO CYBER OPERATIONS: SELF-DEFENCE, COUNTERMEASURES, NECESSITY, AND THE QUESTION OF ATTRIBUTION.

LEPARD, BRIAN D. (2010), CUSTOMARY INTERNATIONAL LAW: A NEW THEORY WITH PRACTICAL APPLICATIONS.

臺灣大學學術期刊資料庫

LUBELL, NOAM (2010), EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS.
MAVROIDIS, PETROS C. (2022), THE WTO DISPUTE SETTLEMENT SYSTEM: HOW, WHY AND WHERE?.
PELC, KRZYSZTOF J. (2016), MAKING AND BENDING INTERNATIONAL RULES: THE DESIGN OF EXCEPTIONS AND ESCAPE CLAUSES IN TRADE LAW.
POLANYI, KARL (2001), THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME.
RADU, ROXANA (2019), NEGOTIATING INTERNET GOVERNANCE.
REISMAN, W. MICHAEL (2012), THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY.
SIR LAUTERPACHT, SIR HERSCH (2011), THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY.
SIR LAUTERPACHT, SIR HERSCH (2013), RECOGNITION IN INTERNATIONAL LAW.
TRACHTMAN, JOEL P. (2009), THE ECONOMIC STRUCTURE OF INTERNATIONAL LAW.
TREVES, TULLIO (2015), THE EXPANSION OF INTERNATIONAL LAW.
WHYTE, CHRISTOPHER & BRIAN MAZANEC (2019), UNDERSTANDING CYBER WARFARE: POLITICS, POLICY AND STRATEGY.

Articles

Aaronson, Susan (2015), *Why Trade Agreements Are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security*, 14(4) WORLD TRADE REVIEW 671.
Abbott, Kenneth W. & Duncan Snidal (2000), *Hard and Soft Law in International Governance*, 54(3) INTERNATIONAL ORGANIZATION 421.
Abbott, Kenneth W. et al. (2000), *The Concept of Legalization*, 54(3) INTERNATIONAL ORGANIZATION 401.
Acharya, Amitav (2004), *How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism*, 58(2) INTERNATIONAL ORGANIZATION 239.
Addis, Adeno (2010), *Authority and Community*, 18(1) ASIA PACIFIC LAW REVIEW 63.
Alford, Roger P. (2011), *The Self-Judging WTO Security Exception*, 2011(3) UTAH LAW REVIEW 697.
Augsberg, Ino (2010), *Carl Schmitt's Fear: Nomos – Norm – Network*, 23(4) LEIDEN JOURNAL OF INTERNATIONAL LAW 741.
Azaria, Danae (2022), *Trade Countermeasures for Breaches of International Law Outside the WTO*, 71 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 389.
Baldwin, Richard et al. (2009), *Beyond Tariffs: Multilateralizing Non-Tariff*

臺灣大學學術期刊資料庫

RTA Commitments, *in* MULTILATERALIZING REGIONALISM: CHALLENGES FOR THE GLOBAL TRADING SYSTEM 79 (Richard Baldwin & Patrick Low eds.).

Bhala, Raj (1998), *National Security and International Trade Law: What the GATT Says, and What the United States Does*, 19(2) UNIVERSITY OF PENNSYLVANIA JOURNAL OF INTERNATIONAL ECONOMIC LAW 263.

Boklan, Daria & Amrita Bahri (2020), *The First WTO's Ruling on National Security Exception: Balancing Interests or Opening Pandora's Box?*, 19(1) WORLD TRADE REVIEW 123.

Branch, Jordan (2020), *What's in a Name? Metaphors and Cybersecurity*, 75(1) INTERNATIONAL ORGANIZATION 39.

Cavelty, Myriam Dunn (2020), *Cybersecurity Between Hypersecuritization and Technological Routine*, *in* ROUTLEDGE HANDBOOK OF INTERNATIONAL CYBERSECURITY 11 (Eneken Tikk & Mika Kerttunen eds.).

Chen, Tsai-fang (2017), *To Judge the "Self-Judging" Security Exception Under the GATT 1994 – A Systematic Approach*, 12(2) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 311.

Conrad, Victoria (2018), *Digital Gold: Cybersecurity Regulations and Establishing the Free Trade of Big Data*, 10 WILLIAM & MARY BUSINESS LAW REVIEW 295.

Coulibaly, Souleymane et al. (2022), *Overview: Market Access Strategy in a New Trade Environment*, *in* AFRICA IN THE NEW TRADE ENVIRONMENT: MARKET ACCESS IN TROUBLED TIMES 1 (Souleymane Coulibaly, Woubet Kassa & Albert G. Zeufack eds.).

Culbertson, William S. (1942), *Introduction* to HUGH O. DAVIS, AMERICA'S TRADE EQUALITY POLICY vii.

Dunoff, Jeffrey L. (1999), *The Death of the Trade Regime*, 10(4) THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 733.

Dunoff, Jeffrey L. (2012), *A New Approach to Regime Interaction*, *in* REGIME INTERACTION IN INTERNATIONAL LAW: FACING FRAGMENTATION 136 (Margaret A. Young ed.).

Erie, Matthew S. (2021), *Chinese Law and Development*, 62(1) HARVARD INTERNATIONAL LAW JOURNAL 51.

Franck, Thomas M. (1988), *Legitimacy in the International System*, 82(4) AMERICAN JOURNAL OF INTERNATIONAL LAW 705.

Gourgourinis, Anastasios (2011), *General/Particular International Law and Primary/Secondary Rules: Unitary Terminology of a Fragmented System*, 22(4) THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 993.

Guzman, Andrew T. & Timothy L. Meyer (2010), *International Soft Law*, 2(1) JOURNAL OF LEGAL ANALYSIS 171, 174.

Haggard, Stephan & Beth A. Simmons (1987), *Theories of International Regimes*, 41(3) INTERNATIONAL ORGANIZATION 491.

臺灣大學學術期刊資料庫

Heath, J. Benton (2020), *Trade and Security Among the Ruins*, 30(2) DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 223.

Helfer, Laurence R. (2002), *Overlegalizing Human Rights: International Relations Theory and the Commonwealth Caribbean Backlash Against Human Rights Regimes*, 102(7) COLUMBIA LAW REVIEW 1832.

Helfer, Laurence R. (2013), *Flexibility in International Agreements*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART 175 (Jeffrey L. Dunoff & Mark A. Pollack eds.).

Henckels, Caroline (2020), *Permission to Act: The Legal Character of General and Security Exceptions in International Trade and Investment Law*, 69(3) INTERNATIONAL & COMPARATIVE LAW QUARTERLY 557.

Henderson, Christian (2021), *The United Nations and the Regulation of Cyber-Security*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 582 (Nicholas Tsagourias & Russell Buchan eds., 2d ed.).

Jervis, Robert (1982), *Security Regimes*, 36(2) INTERNATIONAL ORGANIZATION 357.

Jessup, Philip C. (1964), *Diversity and Uniformity in the Law of Nations*, 58(2) AMERICAN JOURNAL OF INTERNATIONAL LAW 341.

Kennedy, Duncan (2006), *Three Globalizations of Law and Legal Thought: 1850–2000*, *in* THE NEW LAW AND ECONOMIC DEVELOPMENT: A CRITICAL APPRAISAL 19 (David M. Trubek & Alvaro Santos eds.).

Keohane, Robert O. et al. (2000), *Legalized Dispute Resolution: Interstate and Transnational*, 54(3) INTERNATIONAL ORGANIZATION 457.

Kinne, Brandon J. (2018), *Defense Cooperation Agreements and the Emergence of a Global Security Network*, 72(4) INTERNATIONAL ORGANIZATION 799.

Koremenos, Barbara (2013), *Institutionalism and International Law*, *in* INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS: THE STATE OF THE ART 59 (Jeffrey L. Dunoff & Mark A. Pollack eds.).

Koremenos, Barbara et al. (2001), *The Rational Design of International Institutions*, 55(4) INTERNATIONAL ORGANIZATION 761.

Koskenniemi, Martti (2011), *The Mystery of Legal Obligation*, 3(2) INTERNATIONAL THEORY 319.

Krasner, Stephen D. (1982), *Structural Causes and Regime Consequences: Regimes as Intervening Variables*, 36(2) INTERNATIONAL ORGANIZATION 185.

Krisch, Nico (2014), *The Decay of Consent: International Law in an Age of Global Public Goods*, 108(1) AMERICAN JOURNAL OF INTERNATIONAL LAW 1.

Lam, Joanna & Güneş Ünüvar (2019), *Transparency and Participatory Aspects of Investor-State Dispute Settlement in the EU "New Wave"*

臺灣大學學術期刊資料庫

Trade Agreements, 32(4) LEIDEN JOURNAL OF INTERNATIONAL LAW 781.
Lee, Jaemin (2018), *Commercializing National Security: National Security Exceptions' Outer Parameter Under GATT Article XXI*, 13(2) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 277.
Lefkowitz, David (2016), *The Legitimacy of International Law*, *in* GLOBAL POLITICAL THEORY 98 (David Held & Pietro Maffettone eds.).
Leonard, H. Jeffrey (1980), *Review: Multinational Corporations and Politics in Developing Countries*, 32 WORLD POLITICS 454.
Lindsay, Peter (2003), *The Ambiguity of GATT Article XXI: Subtle Success or Rampant Failure?*, 52(6) DUKE LAW JOURNAL 1277.
Lipson, Charles (1991), *Why are Some International Agreements Informal?*, 45(4) INTERNATIONAL ORGANIZATION 495.
Mačák, Kubo (2017), *From Cyber Norms to Cyber Rules: Re-Eengaging States as Law-Makers*, 30(4) LEIDEN JOURNAL OF INTERNATIONAL LAW 877.
Marwell, Jeremy C. (2006), *Trade and Morality: The WTO Public Morals Exception After Gambling*, 8(2) NEW YORK UNIVERSITY LAW REVIEW 802.
Mattli, Walter (2001), *Private Justice in a Global Economy: From Litigation to Arbitration*, 55(4) INTERNATIONAL ORGANIZATION 919.
Mishra, Neha (2020), *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19(3) WORLD TRADE REVIEW 341.
Mishra, Neha (2020), *The Trade: (Cyber)Security Dilemma and its Impact on Global Cybersecurity Governance*, 54(4) JOURNAL OF WORLD TRADE 567.
Mitchell, Andrew D. & Neha Mishra (2019), *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22(3) JOURNAL OF INTERNATIONAL ECONOMIC LAW 389.
Pauwelyn, Joost (2001), *The Role of Public International Law in the WTO: How Far Can We Go?*, 95(3) AMERICAN JOURNAL OF INTERNATIONAL LAW 535.
Peng, Shin-yi (2015), *Cybersecurity Threats and the WTO National Security Exceptions*, 18(2) JOURNAL OF INTERNATIONAL ECONOMIC LAW 449.
Peng, Shin-yi (2020), *A New Trade Regime for the Servitization of Manufacturing: Rethinking the Goods-Services Dichotomy*, 54(5) JOURNAL OF WORLD TRADE 669.
Peng, Shin-yi (2022), *The Uneasy Interplay Between Digital Inequality and International Economic Law*, 33(1) THE EUROPEAN JOURNAL OF INTERNATIONAL LAW 205.
Petersmann, Ernst-Ulrich (2011), *The Future of the WTO: From Authoritarian Mercantilism to Multilevel Governance for the Benefit of Citizens*, 6(1) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW

臺灣大學學術期刊資料庫

AND POLICY 45.
Prazeres, Tatiana Lacerda (2020), *Trade and National Security: Rising Risks for the WTO*, 19(1) WORLD TRADE REVIEW 137.
Ratner, Steven R. (2011), *Between Minimum and Optimum World Public Order: An Ethical Path for the Future*, *in* LOOKING TO THE FUTURE: ESSAYS ON INTERNATIONAL LAW IN HONOR OF W. MICHAEL REISMAN 195 (Mahnoush H. Arsanjani et al. eds.).
Raustiala, Kal (2005), *Form and Substance in International Agreements*, 99(3) AMERICAN JOURNAL OF INTERNATIONAL LAW 581.
Reisman, W. Michael (1981), *International Lawmaking: A Process of Communication: The Harold D. Lasswell Memorial Lecture*, *in* 75 PROCEEDINGS OF THE ASIL ANNUAL MEETING 101.
Rosendorff, B. Peter & Helen V. Milner (2001), *The Optimal Design of International Trade Institutions: Uncertainty and Escape*, 55(4) INTERNATIONAL ORGANIZATION 829.
Ruggie, John Gerard (1982), *International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order*, 36(2) INTERNATIONAL ORGANIZATION 379.
Schachter, Oscar (1977), *The Twilight Existence of Nonbinding International Agreements*, 71(2) AMERICAN JOURNAL OF INTERNATIONAL LAW 296.
Schöndorf, Roy (2021), *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395.
Siniver, Asaf & Scott Lucas (2019), *Understanding Tacit Security Regimes*, 4(4) JOURNAL OF GLOBAL SECURITY STUDIES 510.
Stevens, Tim & Kevin O'Brien (2019), *Brexit and Cyber Security*, 164(3) RUSI JOURNAL 22.
Sykes, Alan O. (2003), *The Least Restrictive Means*, 70(1) THE UNIVERSITY OF CHICAGO LAW REVIEW 403.
Taylor, C. O'Neal (2007), *Impossible Cases: Lessons from the First Decade of WTO Dispute Settlement*, 28(2) UNIVERSITY OF PENNSYLVANIA JOURNAL OF ECONOMIC INTERNATIONAL LAW 309.
Thirlway, Hugh (2001), *Reflections on* lex ferenda, 32 NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 3.
van Aaken, Anne & Betül Simsek (2021), *Rewarding in International Law*, 115(2) AMERICAN JOURNAL OF INTERNATIONAL LAW 195.
Weber, Rolf H. & Rainer Baisch (2018), *Revisiting the Public Moral/Order and the Security Exceptions under the GATS*, 13(2) ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW AND POLICY 375.
Weil, Prosper (1983), *Towards Relative Normativity in International Law?*, 77(3) AMERICAN JOURNAL OF INTERNATIONAL LAW 413.
Weiler, Joseph H.H. (1988), *Introduction* to *Are We Heading for a New Normativity in the International Community?*, *in* CHANGE AND

臺灣大學學術期刊資料庫

STABILITY IN INTERNATIONAL LAW-MAKING 63 (Antonio Cassese & Joseph H. H. Weiler eds.).

Weiler, Joseph H.H. (2001), *The Rule of Lawyers and the Ethos of Diplomats Reflections on the Internal and External Legitimacy of WTO Dispute Settlement*, 35(2) JOURNAL OF WORLD TRADE 191.

Cases

Appellate Body Report, *Argentina — Measures Relating to Trade in Goods and Services*, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016).

Appellate Body Report, *Peru — Additional Duty on Imports of Certain Agricultural Products*, WTO Doc. WT/DS457/AB/R (adopted July 31, 2015).

Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services* WTO Doc. WT/DS285/AB/R (adopted April 20, 2005).

Application of the Interim Accord of 13 September 1995 (the former Yugoslav Republic of Macedonia v. Greece), Judgment, 2011 I.C.J. 644 (December 5, 2011) (separate opinion by Simma, J.).

Case C-284/16, Slowakische Republik (Slovak Republic) v. Achmea BV., https://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX:62016CJ0284#t-ECR _62016CJ0284_EN_01-E0001 (March 6, 2018).

Certain Expenses of the United Nations (Article 17, paragraph 2, of the Charter), Advisory Opinion, 1962 I.C.J. 151 (July 20).

Fisheries (United Kingdom v. Norway), Judgment, 1951 I.C.J. 116, (December 18).

Island of Palmas case (Netherlands v. United States of America), 2 R.I.A.A. 831 (Permanent Court of Arbitration 1928).

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United State of America), Judgment, 1986 I.C.J. 14 (June 27).

Panel Report, *Russia — Measures Concerning Traffic in Transit*, WTO Doc. WT/DS512/R (adopted April 26, 2019).

Prosecutor v. Tadić, Case No. IT-94-1-I, Opinion and Judgment, (International Criminal Tribunal for the Former Yugoslavia May 7, 1997).

Report of the Panel, *United States – Restrictions on Imports of Tuna*, GATT Doc. DS21/R — 39S/155 (circulated September 3, 1991).

S.S. Lotus (France v. Turkey), Judgement, 1927 P.C.I.J. (ser. A) No. 10 (September 7).

Treaties

Digital Economy Partnership Agreement, June 11, 2020, https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement.

Free Trade Agreement Between Canada and The Republic of Colombia,

臺灣大學學術期刊資料庫

Canada-Colombia, November 21, 2008, https://wits.worldbank.org/GPTAD/PDF/archive/canada-columbia.pdfs.

General Agreement on Trade in Services, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167.

Regional Comprehensive Economic Partnership Agreement, November 15, 2020, https://rcepsec.org/legal-text/.

The Singapore – Australia Free Trade Agreement, Australia–Singapore, February 17, 2003, https://www.dfat.gov.au/sites/default/files/SAFTA-chapter-14.pdf.

Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, December 30, 2020, 2021 O.J. (L 149) 10.

U.N.-related Documents

Chair's Report of the Second Intersessional Consultation of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, U.N. Doc. A/A C.291/CRP.12 (July 6, 2022).

General Assembly Resolution S-6/3201 (May 1, 1974).

General Assembly Resolution 70/125 (February 1, 2016).

General Assembly Resolution 73/266 (January 2, 2019).

General Assembly Resolution 74/247 (January 20, 2020).

General Assembly Resolution 76/19 (December 8, 2021).

International Law Commission, Report on the Work of Its Fifty-Eighth Session, U.N. Doc. A/61/10 (1 May-9 June and 3 July-11 August 2006).

Martti Koskenniemi, *Report of the Study Group of the International Law Commission*, U.N. Doc. A/CN.4/L.682 and Add.1 (April 13, 2006).

Motaz M. Zahran (Rapporteur), *Role of Science and Technology in the Context of Security, Disarmament and Other Related Fields Rep. of the First Committee*, U.N. Doc. A/53/576 (November 18, 1998).

Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, U.N. Doc. A/76/136 (July 13, 2021).

Permanent Representative of the Russian Federation to the U.N., Report of the First Committee, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. Doc. A/C.1/53/3 (September 30, 1998).

臺灣大學學術期刊資料庫

U.N. Economic and Social Council, Economic Commission for Europe, Draft Proposal for a Common Regulatory Framework on Cybersecurity, U.N. Doc. ECE/CTCS/WP.6/2018/9 (September 10, 2018).
U.N. Economic and Social Council, Economic Commission for Europe, Report of the Activities Under the Group of Experts on Managing Risks in Regulatory Systems, U.N. Doc. ECE/CTCS/WP.6/2020/5 (August 21, 2020).
U.N. SECRETARY-GENERAL, OUR COMMON AGENDA – REPORT OF THE SECRETARY-GENERAL, U.N. Sales No. E.21.I.8 (2021).
U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/76/135 (July 14, 2021).
U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174 (July 22, 2015).
U.N. Secretary-General, *Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, U.N. Doc. A/76/151 (July 15, 2021).

WTO-related Documents

GATT Secretariat, *Analytical Summary of Information Exchanged Among Contracting Parties*, GATT Doc. MDF/7/Rev.2 (November 25, 1985).
General Council, *Arrangements for Effective Cooperation with Other Intergovernmental Organizations-Relations Between the WTO and the United Nations*, WTO Doc. WT/GC/W/10 (November 3, 1995).
WTO Joint Statement Initiative on Electronic Commerce, *WTO Electronic Commerce Negotiations—Consolidated Negotiating Text – December 2020*, WTO Doc. INF/ECOM/62/Rev.1 (December 14, 2020).

Internet Sources

Annex B: Australia's Position on How International Law Applies to State Conduct in Cyberspace, AUSTRALIAN GOVERNMENT, https://www.internationalcybertech.gov.au/our-work/annexes/annex-b.
Decouple, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/dictionary/english/decouple.
FACT SHEET: In Asia, President Biden and a Dozen Indo-Pacific Partners Launch the Indo-Pacific Economic Framework for Prosperity, THE WHITE HOUSE (May 23, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/23/fact-sheet-in-asia-president-biden-and-a-dozen-indo-pacific-partners-launch-the-indo-pacific-economic-framework-for-prosperity/.
FACT SHEET: Indo-Pacific Economic Framework for Prosperity Upskilling Initiative for Women and Girls, U.S. DEPARTMENT OF COMMERCE

臺灣大學學術期刊資料庫

(September 8, 2022), https://www.commerce.gov/news/fact-sheets/2022/09/fact-sheet-indo-pacific-economic-framework-prosperity-upskilling.

Individuals Using the Internet (% of population), THE WORLD BANK, https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&start=1960&view=chart.

Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 18 final (December 16, 2020).

Joint Statement by President von der Leyen and President Yoon on the EU–Republic of Korea Digital Partnership, European Commission (November 28, 2022), https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7232.

Joint Statement by President von der Leyen and Prime Minister Lee on the EU–Singapore Digital Partnership, European Commission (December 14, 2022), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_7743.

Rangel, Daniel, *WTO General Exceptions: Trade Law's Faulty Ivory Tower*, PUBLIC CITIZEN (February 4, 2022), https://www.citizen.org/article/wto-general-exceptions-trade-laws-faulty-ivory-tower/.

Read the Framework, NATIONAL ARCHIVES, https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html.

Significant Cyber Incidents Since 2006, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/230207_Significant_Cyber_Incidents.pdf?VersionId=f3TcDDNQ0 YCzPY72D_AdhyuYY21ifK_h.

TAPED: A New Dataset on Data-Related Trade Provisions, UNIVERSITY OF LUCERNE, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

Tidy, Joe, *President Rodrigo Chaves Says Costa Rica Is at War with Conti Hackers*, BBC News (May 18, 2022), https://www.bbc.com/news/technology-61323402.

U.S.–EU Joint Statement of the Trade and Technology Council (Annex IX: Conclusions on Working Group 9 – Promoting SME Access to and Use of Digital Tools), THE WHITE HOUSE (May 16, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/05/TTC-US-text-Final-May-14.pdf.

Wittgenstein, Ludwig, Tractatus Logico-Philosophicus, (Ramsey Ogden & McGuinness Pears translated, 2022) (1922), http://people.umass.edu/klement/tlp/tlp.pdf.

Other Sources

Declaration de Djibouti: A La Premiere Session de Fond du Groupe de Travail A Composition Non Limitée sur la Securité de l'Utilisation des

臺灣大學學術期刊資料庫

Technologie de l'Information 2021-2025, Delivre par Mme Zeinab Ismael Assoweh, Conseillère à la Mission Permanente Auprès des Nations Unies [Djibouti Declaration: At the First Substantive Session of the Open-Ended Working Group on the Security of the Use of Information Technology 2021-2025, Delivered by Ms. Zeinab Ismael Assoweh, Counselor at the Permanent Mission to the United Nations] (December 14, 2021), https://documents.unoda.org/wp-content/uploads/2022/01/DECLARATION-CYBERSECURITE.pdf.

NEW ZEALAND MINISTRY OF FOREIGN & TRADE, VIET NAM–NEW ZEALAND: CYBER SECURITY (March 8, 2018), https://www.mfat.govt.nz/assets/Trade-agreements/CPTPP/Viet-Nam-New-Zealand-Cyber-Security.pdf.

OFFICE OF FINANCIAL SANCTIONS IMPLEMENTATION, CONSOLIDATED LIST OF FINANCIAL SANCTIONS TARGETS IN THE UK, (May 7, 2022), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088191/Cyber.pdf.

OFFICE OF THE U.S. TRADE REPRESENTATIVE, MINISTERIAL TEXT FOR TRADE PILLAR OF THE INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY-INDO-PACIFIC ECONOMIC FRAMEWORK FOR PROSPERITY (IPEF): PILLAR I—TRADE (May 2022), https://ustr.gov/sites/default/files/2022-09/IPEF%20Pillar%201%20Ministerial%20Text% 20(Trade%20Pillar)FOR%20PUBLIC%20RE LEASE%20(1).pdf.

Renforcement des Capacités, Intervention de S.E.M. Désiré Wulfran G. Ipo Ambassadeur, Représentant Permanent Adjoint de La République de Côte D'Ivoire auprès des Nations Unies [Capacity Building, Intervention of H.E. Désiré Wulfran G. Ipo Ambassador, Deputy Permanent Representative of the Republic of Côte d'Ivoire to the United Nations] (March 31, 2022), https://documents.unoda.org/wp-content/uploads/2022/04/Declaration-de-la-CI-2e-SESSION-DE-FOND-OEWG-30.3.2022.pdf.

Report of the Panel of Experts, Panel of Experts Proceeding Constituted Under Article 13.15 of the EU–Korea Free Trade Agreement (January 20, 2021), https://trade.ec.europa.eu/doclib/docs/2021/january/tradoc_159358.pdf.

Woodrow Wilson, President of the U.S., Address delivered at the First Annual Assemblage of the League to Enforce Peace: "American Principles" (May 27, 1916), The American Presidency Project, https://www.presidency.ucsb.edu/node/206570.

臺灣大學學術期刊資料庫