EASTERNISATION OF INTERNATIONAL LAW:
FRAGMENTATION AND REGIME COMPLEX OF CYBERSPACE GOVERNANCE

PhD Dissertation

PhD Candidate:

Haekal Al Asyari

Supervisor:

Prof. Dr. habil Tamas Fézer, Ph.D.

UNIVERSITY OF DEBRECEN

MARTON GÉZA DOCTORAL SCHOOL OF LEGAL STUDIES

DEBRECEN, 2025

PLAGIARISM DECLARATION

I, the undersigned **Haekal Al Asyari** by signing the present statement declare that the thesis, entitled "Easternisation of International Law: Fragmentation and Regime Complex of Cyberspace Governance".

In the process of writing the thesis I have complied with the provisions of Act LXXVI of 1999 on Copyright and the regulations of the University of Debrecen regarding the principles of thesis writing, especially regarding references and citations.

I declare that I have not submitted a thesis with the same content as the submitted thesis for a doctoral degree at another university.

Furthermore, I declare that I did not mislead my supervisors in the course of the preparation of the thesis with regard to the condition of the individuality of my work.

I also declare that the thesis submitted in paper form and its electronic version are identical in all respects (see Rules and Regulations, Article 24, paragraph 8).

By signing this declaration, I acknowledge that the University of Debrecen has the right to refuse acceptance of the thesis and to take disciplinary measures against me if it can be proven that the thesis is not my intellectual creation and if there is a suspicion of copyright infringement. In this case, the refusal to accept the thesis and the disciplinary proceedings do not affect any other legal consequences caused by the copyright infringement.

Debrecen, January 19th 2026

.....

Signature

Haekal Al Asyari

RECOMMENDATION OF THE SUPERVISOR

Mr. Haekal Al-Asyari's doctoral work addresses one of the most actual and conceptually challenging developments in contemporary international law: the transformation of norm-production and governance structures in cyberspace against the background of shifting global power relations. In the 21st century, cyberspace has become a critical domain for economic activity, social interaction, and international security, yet it remains governed by a fragmented and non-hierarchical set of legal and quasi-legal regimes. At the same time, the growing normative and regulatory engagement of Southeast Asian countries raises fundamental questions about the continued Western dominance of international lawmaking and the possible emergence of alternative governance paradigms.

Mr. Haekal Al-Asyari's research is particularly timely in light of recent global developments, including intensified cyber threats, accelerating digitalization, and the gradual consolidation of international and regional cyber governance instruments. By focusing on ASEAN and its member states, the dissertation moves beyond the traditional Euro-Atlantic perspective and contributes to a more pluralistic understanding of international law. The central research question – whether and to what extent Southeast Asian cyberspace governance contributes to the easternization of international law – is both original and theoretically ambitious, while remaining firmly grounded in empirical analysis.

Methodologically, the dissertation demonstrates a high level of sophistication and innovation. The author adopts a mixed-method research design that combines doctrinal legal analysis with empirical, data-driven mapping techniques. A systematically constructed dataset of an abundant number of international, regional, and national governance instruments forms the empirical backbone of the research. These instruments are coded and analyzed through a detailed classification framework anchored in Lessig's Regulatability Theory, allowing the author to examine not only formal legal rules, but also the regulatory role of norms, architecture, and market mechanisms. The integration of computational tools for classification, coding, and visualization represents a notable methodological strength and responds convincingly to current calls for more empirically grounded approaches in international legal scholarship.

From a substantive perspective, the dissertation's main strengths lie in its analytical depth and conceptual clarity. The author provides a comprehensive mapping of international cyberspace governance, identifies patterns of fragmentation and regime complexity, and demonstrates how ASEAN-led approaches differ structurally and philosophically from Western-dominated models. Most importantly, the dissertation succeeds in operationalizing the concept of "easternization" through clearly defined indicators, thereby transforming an abstract theoretical notion into an empirically testable framework. This allows the author to advance a nuanced argument: rather than rejecting existing international legal norms, Southeast Asian actors selectively reinterpret and reconfigure them, contributing to a gradual redistribution of normative authority within international law.

Overall, this dissertation is a mature, original, and methodologically robust contribution to the field of international law and cyberspace governance. It reflects independent scholarly thinking, excellent command of the relevant literature, and a high level of analytical discipline. The work meets – and in several aspects exceeds – the standards expected of a doctoral dissertation and makes a valuable contribution to ongoing debates on fragmentation, regime complexity, and the evolving geography of international law.

Dr. Tamás Fézer
supervisor

LIST OF ABBREVIATIONS

AEC	ASEAN Economic Community
AMS	ASEAN Member States
APSC	ASEAN Political-Security Community
ASCC	ASEAN Socio-Cultural Community
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
CSTD	Commission on Science and Technology for Development (UN)
DEFA	Digital Economy Framework Agreement (ASEAN)
ECOSOC	United Nations Economic and Social Council
EU	European Union
GDPR	General Data Protection Regulation (EU)
GGE	Group of Governmental Experts (UN)
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICJ	International Court of Justice
ICT	Information and Communication Technology
IGF	Internet Governance Forum
ITU	International Telecommunication Union (UN)
IP	Internet Protocol
JAIF	Japan–ASEAN Integration Fund
LRT	Lessig's Regulatability Theory
MoU	Memorandum of Understanding
NIS2	Network and Information Security Directive 2 (EU)
OECD	Organisation for Economic Co-operation and Development
OEWG	Open-Ended Working Group (UN)
ODS	Official Document System of the United Nations

PDP	Personal Data Protection
PTA	Preferential Trade Agreement
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights (WTO)
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UNGA	United Nations General Assembly
UNIDIR	United Nations Institute for Disarmament Research
UNTS	United Nations Treaty Series
URL	Uniform Resource Locator
U.S.	United States
WGIG	Working Group on Internet Governance
WTO	World Trade Organization
WSIS	World Summit on the Information Society
WWW	World Wide Web

TABLE OF CONTENTS

LIST OF INTERNATIONAL TREATIES

ASEAN Agreement on Electronic Commerce, January 22, 2019, ASEAN Secretariat

Charter of the Association of Southeast Asian Nations November 20, 2007, ASEAN Secretariat

Convention on Cybercrime, November 23, 2001, CETS No. 185.

Directive 2013/40/EU on attacks against information systems, August 14, 2013

Directive (EU) 2016/680 (Law Enforcement Directive), OJ L 119, May 4, 2016.

Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment, OJ L 123, May 10, 2019.

Directive (EU) 2022/2555 (NIS2 Directive), OJ L 333, December 27, 2022.

e-ASEAN Framework Agreement, November 24, 2000, ASEAN Secretariat.

Regulation (EU, Euratom) 2023/2841 on measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union, OJ L 2023/2841, December 20, 2023.

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, May 4, 2016.

Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, OJ L 151, June 7, 2019.

United Nations Convention on the Law of the Sea, December 10, 1982, 1833 UNTS 397, 21 ILM 1261 (1982).

LIST OF DOMESTIC LAWS

Computer Misuse Act 1993 (2020 Revised Edition), Parliament of Singapore

Cybersecurity Code of Practice for Critical Information Infrastructure – Second Edition Revision One, Cyber Security Agency of Singapore (CSA)

Cybersecurity Act 2018, Parliament of Singapore

Cybersecurity (Critical Information Infrastructure) Regulations 2018, Parliament of Singapore

Cybersecurity (Amendment) Bill 2024, Parliament of Singapore

Electronic Commerce Act 2006 (Act 658), Parliament of Malaysia

Digital Signature Act 1997 (Act 562), Parliament of Malaysia

Computer Crimes Act 1997 (Act 563), Parliament of Malaysia

National Security Council Act 2016 (Act 776), Parliament of Malaysia

Communications and Multimedia Act 1998 (Act 588), Parliament of Malaysia

Penal Code (Act 574), Parliament of Malaysia

Electronic Information and Transactions Law (UU ITE), Parliament of Indonesia

Law No. 27/2022 on Personal Data Protection, Parliament of Indonesia

BSSN Regulation No. 3/2021 on Cybersecurity and Media Literacy, Badan Siber dan Sandi Negara (BSSN)

Presidential Regulation No. 47/2023 on National Cybersecurity Strategy and Cyber Crisis Management, Office of the President / BSSN

Government Regulation No. 71/2019 on Electronic Systems and Transactions, Parliament of Indonesia

Cybercrime Prevention Act of 2012 (RA 10175), Congress of the Philippines

Rules on Electronic Evidence (A.M. No. 01-7-01-SC), Supreme Court of the Philippines

Act on Computer Crime B.E. 2550 (2007), Royal Thai Government

Cybersecurity Act B.E. 2562 (2019), Ministry of Digital Economy and Society

Personal Data Protection Act B.E. 2562 (2019), Royal Thai Government

2001 Decree No. 55/2001/ND-CP on Internet Services, Government of Vietnam

2016 Law on Network Information Security, National Assembly

2018 Law on Cybersecurity, National Assembly

Criminal Code of Cambodia (Unofficial English Translation), Royal Government of Cambodia

Law on Telecommunications, Ministry of Posts and Telecommunications

Computer Misuse Act (Chapter 194), Government of Brunei

Electronic Transactions Act (Chapter 196), Government of Brunei

Commonwealth Model Law on Computer and Computer-Related Crimes, Commonwealth Secretariat

Electronic Transactions Law, Myanmar State Peace and Development Council

Telecommunications Law, Pyidaungsu Hluttaw (Myanmar)

Computer Science Development Law, Myanmar State Law and Order Restoration Council

LIST OF FIGURES

CHAPTER I
INTRODUCTION

A. Background of Study

Throughout history, global power has recurrently shifted toward the West, consolidating economic and political dominance and enabling Western states to shape international norms and governance frameworks.[1] For nearly five centuries, Western powers extended their influence over much of the Eastern world not only through military conquest and economic control, but also by embedding their authority in religion, regulation, and governance. These historical patterns positioned Western legal traditions and institutions as the primary architects of modern international law.[2]

Yet this long-standing configuration is increasingly contested. The rapid rise of nation-states in the Asia-Pacific has altered global economic and political dynamics, challenging the traditional dominance of Western powers. [3] The growing economic weight, demographic significance, and technological integration of this region now raise important questions about participation, influence, and autonomy within international legal and governance systems.

The increasing prominence of the Asia-Pacific highlights a persistent tension in international law. Despite accounting for a substantial share of the global population and economic activity, Asian and Pacific states historically played a limited role in shaping international legal norms and institutions. Their engagement with international law was often reactive rather than constitutive, occurring within frameworks largely designed elsewhere. Today, however, this trend is shifting. The region demonstrates growing engagement with international law,[4] driven simultaneously by challenges such as climate change, transnational crime, and digital insecurity, and by opportunities including economic integration and digital transformation.[5]

---

[1] Sushil Jain, "Easternization of the West: An Essay in Reverse Colonization," *SSRN Electronic Journal*, September 1, 1988, https://doi.org/10.2139/SSRN.1851868.
[2] Chimni, B. S. "Customary International Law: A Third World Perspective." American Journal of International Law 112, no. 1 (2018): 1–46. https://doi.org/10.1017/ajil.2018.12.
[3] Shirasihi Takashi, *Emerging States and Economies: Their Origins, Drivers, and Chalenges Ahead*, ed. Shiraishi Takashi and Sonobe Tetsushi, 2019, http://www.springer.com/series/16114.
[4] Simon Chesterman, "Asia's Ambivalence about International Law and Institutions: Past, Present and Futures," *European Journal of International Law* 27, no. 4 (November 29, 2016): 945–78, https://doi.org/10.1093/ejil/chw051.
[5] Chesterman Simon, Owada Hisashi, and Saul Be, *The Oxford Handbook of International Law in Asia and the Pacific* (Oxford , 2019), https://global.oup.com/academic/product/the-oxford-handbook-of-international-law-in-asia-and-the-pacific-9780198793854?cc=hu&lang=en&.

The concept of easternisation has predominantly been explored in economic and geopolitical scholarship,[6] where it commonly refers to a shift in global power from West to East. Its implications for international law, however, remain comparatively under-examined. International law has historically reflected Western legal traditions, institutional preferences, and normative priorities. [7] Rather than a wholesale transformation of international law, contemporary shifts more plausibly point toward the emergence of regionally distinctive approaches that coexist with, adapt, or selectively diverge from Western-dominated frameworks.

In the field of cyberspace governance, this dynamic becomes particularly visible. The international legal framework governing cyberspace has grown increasingly fragmented and regionalised, complicating the development of coherent and binding rules.[8] This fragmentation creates space for regional actors to articulate governance approaches that reflect local political values, institutional cultures, and developmental priorities. This dissertation therefore asks: to what extent do Southeast Asian states pursue governance approaches that are regionally distinctive and relatively independent from Western-dominated frameworks, illustrating a form of easternisation within international law?

Among contemporary issues, cyberspace stands out as the most rapidly evolving and disruptive phenomenon confronting the international community, making it a particularly revealing domain through which to examine whether and how easternisation manifests in international law.[9] Following the COVID-19 pandemic,[10] dependence on the internet has deepened,[11] positioning cyberspace as an indispensable domain of daily life.[12] Amplified by

---

[6] Gideon Rachman, *Easternization: Asia's Rise and America's Decline from Obama to Trump and Beyond* (Other Press, 2016).

[7] Eslava L. Trigueño, "International Law: On (Most of) the World Being (Always, Somehow) Out of Place," in *Out of Place: Fieldwork and Positionality in Law and Society*, ed. LJ Chua and MF Massoud (Cambridge Studies in Law and Society, Cambridge University Press, n.d.), 160–87.

[8] Joseph Nye, S., "The Regime Complex for Managing Global Cyber Activities." Global Commission on Internet Governance, no. Paper Series No.1 (May 2014).

[9] *See* Yee Fen Lim, *Law and Regulation in Cyberspace*, 2nd ed. (Oxford University Press, 2007), https://doi.org/10.1109/CYBER.2003.1253432., m Drake J, *The Working Group on Internet Governance*, ed. William Drake J, accessed August 28, 2025, https://www.apc.org/sites/default/files/IG_10_Final_0.pdf.

[10] World Health Organization (2020), Novel Coronavirus(2019- NCoV) Situation Report - 13, accessed on 27 May 2021 from https://www.who.int/docs/defaultsource/coronaviruse/situation-reports/20200202-sitrep-13- ncov-v3.pdf.

[11] Beltsazar A. Krisetya (2020), COVID-19 Exposes Vulnerabilities in Our Cyberspace, CSIS Commentaries DMRU-010, De', R., Pandey, N., & Pal, A. (2020), Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International journal of information management, 55, 102171. accessed on 27 May 2021 from https://doi.org/10.1016/j.ijinfomgt.2020.102171

[12] OECD (2020), Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement, OECD, Paris, accessed on 27 May 2021 from www.oecd.org/digital/digital-economy-outlook-covid.pdf.

accelerated technological innovation, cyberspace now disrupts not only economies and societies but also the very architecture of global governance.[13]

Unlike traditional domains regulated by international law, cyberspace is borderless, decentralised, and simultaneously public and private. No single entity can claim ownership or comprehensive control over it, yet a growing number of international institutions seek to govern its operation and use. [14] Governments, corporations, private entities, civil society actors, and international organisations all maintain enduring interests in this shared domain.[15] As observed by Wolfgang Kleinwächter, governing cyberspace entails shared decision-making over infrastructure, information, communication, and commerce, reflecting a complex blend of political, technological, and organisational dimensions. Despite these novel characteristics, governance cannot be meaningfully separated from the state, whose sovereignty and regulatory authority remain central to legal ordering in cyberspace.[16] An international law perspective therefore remains indispensable for understanding how authority, responsibility, and norm production operate in this domain.

For the purpose of this study, cyberspace is defined as "a global, borderless domain within the information environment, consisting of layered and interdependent technological infrastructures; including the internet, telecommunications networks, computer systems, and embedded processors and controllers, capable of transmitting, receiving, storing, processing, and deleting information, enabled by institutional intermediation and characterised by decentralisation and constant interaction among diverse actors, constituencies, and interests.[17] Cyberspace is not merely a collection of hardware or technical systems, but also a space shaped by political, social, economic, cultural, and symbolic dimensions. [18]

---

[13] Henry H Perritt and Henry H Perriti, "The Internet Is Changing International Law, 73 Chi," *L. Rev*, vol. 73, 1998, https://scholarship.kentlaw.iit.edu/cklawreviewAvailableat:https://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/4.

[14] Yee Fen Lim, *Law and Regulation in Cyberspace*, 2nd ed. (Oxford University Press, 2007), https://doi.org/10.1109/CYBER.2003.1253432.

[15] William Drake J, *The Working Group on Internet Governance*, ed. William Drake J, accessed August 28, 2025, https://www.apc.org/sites/default/files/IG_10_Final_0.pdf.

[16] Haekal Al Asyari, "Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law," *AUC IURIDICA* 69, no. 4 (December 4, 2023): p. 212, https://doi.org/10.14712/23366478.2023.56.

[17] Jason Whittaker, *The Cyberspace Handbook* (Routledge, 2004), https://doi.org/10.4324/9780203486023., p.1

[18] *Ibid*

These characteristics present significant challenges to traditional legal, social, and political structures. The decentralised nature of cyberspace enables distributed creativity, communication, and commerce, while simultaneously hindering traceability and control. The increasing commercialisation of digital environments has heightened demand for secure and predictable regulatory frameworks for global transactions. Yet adapting existing national laws or creating new international rules is often impeded by slow political processes and divergent state interests. While multilateral cooperation is widely acknowledged as necessary, shared and binding international rules governing cyberspace remain limited.[19]

Fragmentation within international law further intensifies these challenges. International law is no longer characterised by a unified hierarchical structure but by overlapping and partially autonomous regimes across different issue-areas. This condition is particularly pronounced in cyberspace governance, where states, international organisations, regional bodies, and private actors all produce regulatory instruments.[20] As a result, cyberspace governance exhibits one of the most complex regime configurations in contemporary international law, raising fundamental questions about authority, effectiveness, and norm diffusion.

Recently, the United Nations recently adopted the Cybercrime Convention which was scheduled to open for signature on 25 October 2025 in Hanoi, Viet Nam[21]. It will enter into force ninety days after the deposit of the fortieth ratification instrument and will be implemented through a Conference of the States Parties tasked with promoting and reviewing its application.[22] Yet disparities remain in states' capacity to engage with global governance. Developed states advance sophisticated regimes in privacy, cybersecurity, and AI, while developing states face immediate threats such as data theft, malware, and ransomware.[23] This imbalance is sometimes described as "digital colonialism," with actors from the global North dominating digital

[19] Jürgen Feick and Raymund Werle, "Regulation of Cyberspace," in *The Oxford Handbook of Regulation* , ed. Robert, Baldwin, Martin Cave, and Martin Lodge, Online (Oxford University Press, 2010).
[20] Joseph Nye, S., "The Regime Complex for Managing Global Cyber Activities." Global Commission on Internet Governance, no. Paper Series No.1 (May 2014).
[21] At the time of writing, the Convention is awaiting its opening for signature in October 2025. For further details, see https://hanoiconvention.org.
[22] United Nations Office on Drugs and Crime (UNODC). United Nations Convention on Cybercrime. Accessed September 24, 2025. https://www.unodc.org/unodc/cybercrime/convention/home.html#:~:text=Signing%20Ceremony%20(25%2D26%20October,the%20United%20Nations%20Treaty%20Collection.
[23] Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN), Journal of Social and Political Sciences, Vol.3(4), pp.983-995

infrastructures and governance while developing states remain peripheral.[24] Western technology monopolies, particularly U.S.-based platforms, reinforce this dependency. [25] In Southeast Asia, the EU's GDPR often serves as a de facto benchmark for data protection, [26] yet cyber-attacks disproportionately target states with weaker infrastructure and legal safeguards. [27]

Nonetheless, ASEAN has begun to articulate its own distinct path. Member states have enacted domestic frameworks on cybersecurity, personal data protection, and digital economy regulation, while the bloc collectively has advanced regional strategies and cooperative mechanisms.[28] These efforts reveal governance aligned with regional political values, cultural norms, and economic priorities, rather than mere replication of Western frameworks.

To analyze these developments, this dissertation applies Lawrence Lessig's Regulability Theory (LRT) to map the governance modalities shaping international cyberspace law.[29] LRT four primary modalities of regulation: law, market, norms, and architecture, are re-interpreted to provides a lens to understand how different legal and regulatory models emerge.[30] Many Southeast Asian states, despite limited technological and institutional resources, have implemented governance structures aligned with regional political, cultural, and economic imperatives.[31] Linking LRT to regime complex theory and the easternisation framework situates Southeast Asian governance within broader debates about legal authority, fragmentation, and norm diffusion.

Building on this theoretical framing, the dissertation operationalises easternisation through four analytical indicators. The first is norm-setting share, which measures the relative contribution of ASEAN and its member states to normative instruments compared to the UN and EU. The second is the binding versus non-binding mix, assessing whether ASEAN relies primarily on soft law and political commitments versus the more legalistic traditions of Western institutions. The

---

[24] Dahiya, Bhavna. (2023). Digital Colonialism: Neo-Colonialism of the Global South.
[25] *Ibid*
[26] Valentina Ancillia Simbolon, Vishnu Juwono, Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation, *Public Jurnal Ilmu Administrasi,* Vol.11 No.2, 2022, pp.178-190
[27] Alex Kigerl, Routine Activity Theory and the Determinants of High Cybercrime Countries, Social Science and Computer Review, Vol.30 No.4, pp.470-486
[28] Monica Nila Sari, "ASEAN Regional Effort on Cybersecurity and Its Effectiveness," n.d., https://docs.broadcom.com/doc/istr-22-2017-en.
[29] *See* Lessig, *Code: And Other Laws of Cyberspace, Version 2.0*.
[30] *Ibid* 119
[31] Sari, ASEAN Regional Effort, 2

third is cross-referencing practices, evaluating whether ASEAN instruments import norms from external regimes or develop autonomous frameworks. Finally, institutional centrality captures ASEAN's relative position within the global regime complex, examining whether it functions as a peripheral actor or as an emerging reference point in cyberspace governance. Together, these indicators allow easternisation to be empirically distinguished from broader trends of regionalisation or pluralisation.

B. Research questions and hypothesis

In light of the aforementioned issues, this thesis will set out to answer the following main research question: **To what extent has the rise of Southeast Asia's cyberspace governance frameworks contributed to the easternization of international law?** In doing so by answering the follow sub-set of research questions:

1. How can LRT be applied to map the governance modalities of international cyberspace law?
2. How does the regime complex of international cyberspace governance reveal patterns of fragmentation across regions and modalities?
3. What are the distinct characteristics of ASEAN-led cyberspace governance frameworks compared to Western-led frameworks, and what evidence demonstrates a shift from Western-dominated norms to regionally driven regimes?

To complement the research questions, this study formulates a set of hypotheses that serve as analytical expectations. These are not predictions in a strict positivist sense, but working assumptions derived from the theoretical frameworks applied. They provide orientation for the mapping, classification, and interpretation of cyberspace governance regimes, and connect the empirical findings to the broader question of easternization in international law.

H1: LRT can be applied to international cyberspace governance to capture not only binding legal instruments but also the regulatory functions of norms, architecture, and markets.

H2: ASEAN-led cyberspace governance diverges from Western-led models by privileging non-binding norms, market integration, and technical cooperation over binding legal instruments, reflecting ASEAN's consensus-based and pragmatic orientation.

H3: International cyberspace governance exhibits fragmentation and regime complexity, with overlapping instruments and institutions producing both complementarities and conflicts.

ASEAN's initiatives form a parallel governance pole within this landscape, reinforcing decentralization.

H4: The easternisation of international law in cyberspace is observable through specific indicators, including (i) ASEAN's growing share of norm-setting, (ii) its reliance on non-binding over binding instruments compared to the UN and EU, (iii) reduced cross-referencing of Western frameworks alongside the creation of independent region-specific instruments, and (iv) increasing institutional centrality of ASEAN bodies within the regime complex. These shifts illustrate selective uptake and reinterpretation of Western norms, amounting to a redistribution of normative authority rather than outright rejection.

C. Literature Review: Conceptualisations of Cyberspace Governance

In order to situate this dissertation within the existing body of scholarship, it is essential to examine prior efforts that have sought to map cyberspace governance. While there is a growing body of literature addressing various aspects of digital governance, relatively few studies have attempted to provide a comprehensive or integrative mapping of cyberspace as a whole. Most existing works tend to focus on cybersecurity governance, reflecting both the historical evolution of the internet and the regulatory priorities that have shaped early governance interventions. This section critically reviews four prominent studies: GLOBE, Portnoy and Goodman, Joseph Nye, and Kuerbis and Badiei; each of which contributes to the conceptual and institutional understanding of global cyber governance from different methodological and disciplinary perspectives. Their approaches, while varied in scope and emphasis, collectively reveal the dominant institutional, economic, and security-oriented logics that have informed the development of governance frameworks in cyberspace. The section concludes by analysing why cybersecurity has remained the central focal point in most mapping initiatives, particularly in light of the internet's technical architecture, commercialization, and vulnerability to security threats.

One of the most substantial contributions to the literature on cyber governance mapping is the GLOBE (Global Governance and the European Union) report, titled Case Study of Cyber Governance.[32] Despite the generality of its title, the report primarily focuses on the mapping of cybersecurity governance through an institutional lens. Its analysis is anchored in the examination of 85 membership-based institutions involved in guiding collective global action in the realm of

[32] Kouliopoulos, Report: Case Study of Cyber Governance

cybersecurity.[33] The mapping emphasizes institutional membership structures and primary areas of activity, offering a typological overview rather than a conceptual or legal analysis of cyberspace governance as a whole. While its scope is thus narrower than the broader governance of cyberspace, the report makes a significant conceptual contribution by introducing the notion of regime complex; a framework that has become foundational to the structure of analysis in this dissertation. Moreover, the GLOBE report served as a key entry point for identifying two other scholarly studies on cyberspace governance, which will be addressed in subsequent sections.

The report's findings reveal that cybersecurity governance has largely evolved through existing institutional mechanisms, rather than the formation of entirely new cyber-specific bodies. Contrary to the frequently cited multistakeholder approach prevalent in broader internet governance debates, GLOBE finds that this model is only partially replicated in cybersecurity governance. Single-membership-type institutions, typically state-dominated, remain prevalent, with government actors retaining a central role in shaping global cybersecurity efforts.[34] The report also provides insightful observations on the geopolitical dimensions of cooperation. Transcontinental collaboration appears more frequent than regional coordination; however, regional institutions are notably active in the domain of cybercrime, with 84% having adopted specialized regional treaties to address related issues. This pattern underscores a pragmatic orientation toward security-oriented concerns at the regional level.[35]

Perhaps most relevant to this dissertation's thesis is the GLOBE report's analysis of institutional functions. It finds that cooperation among institutions is more feasible in areas involving less rigid or 'softer' governance functions; those that do not require binding legal commitments or strict compliance mechanisms.[36] These include information sharing, capacity building, agenda setting, norm-setting, technical standard-setting, and intelligence sharing. Among these, information sharing and capacity building are identified as the most easily implemented, highlighting a strategic preference for forms of governance that rely on flexibility, mutual assistance, and informal coordination; an insight that aligns closely with this dissertation's broader argument about the layered and non-hierarchical nature of cyberspace governance.

[33] *Ibid* 6
[34] *Ibid* 24
[35] *Ibid* 21
[36] *Ibid* 21

A second notable study is that of Portnoy and Goodman, which offers a historical and organizational account of cyber governance, with a particular emphasis on the roles of international intergovernmental organizations, regional bodies, and both public and private institutions in their efforts to secure cyberspace.[37] The authors adopt a descriptive and institutionally grounded framework, systematically mapping the mandates, operational structures, and policy instruments employed by various actors across multiple levels of governance. The analysis is conducted in a formalized and structured manner, encompassing areas such as public outreach, education, awareness-raising, regulatory harmonization, incident readiness, and response mechanisms. In this regard, the study mirrors the institutional emphasis of the GLOBE report, prioritizing a structural overview of organizational engagement in cyber governance without delving into more abstract conceptual or normative questions surrounding the nature of cyberspace itself.

Although the study was published in 2006 (nearly two decades ago) its analytical framework remains a foundational reference for understanding the institutional landscape of early cyber governance. One of the study's concluding observations is particularly relevant: despite increased activity in the cyber domain, few standardized metrics have been made publicly available by organizations to measure the progress and effectiveness of their initiatives. The absence of consistent data and evaluation frameworks continues to be a challenge, even as global cyber governance efforts have evolved. Nevertheless, the work of Portnoy and Goodman offers a valuable baseline mapping from which subsequent studies have drawn, particularly for understanding the institutional architecture and operational dimensions of early cyberspace governance efforts.

Although less extensive than the previous two studies, Joseph Nye's research makes a critical conceptual contribution by explicitly linking cyberspace governance with the theory of regime complexes.[38] In his formulation of the "Regime Complex for Managing Global Cyber Activities," Nye identifies a constellation of norms, institutions, and procedures involved in governing cyberspace. This framework provides a foundational basis for understanding cyberspace as a fragmented yet functionally interdependent system of governance, structured around distinct but overlapping issue areas. Importantly, Nye's work highlights the often-overlooked presence of

[37] Portnoy and Goodman, Global Initiatives to Secure Cyberspace,
[38] Nye, Regime Complex, 5

international law within cyberspace governance; albeit organized into separate regimes, such as human rights, telecommunications, trade, and intellectual property. While these regimes are typically discussed in isolation, Nye's regime complex approach underscores their collective relevance, and their shared grounding in international legal structures.

Nye's analysis distinguishes between various functional domains of cyberspace governance and the actors or mechanisms responsible for each. For example, technical standards are shaped through consensus among engineers in non-governmental bodies like the Internet Engineering Task Force (IETF) and W3C, reflecting the architectural modality of regulation. Network connections and domain name governance, meanwhile, are driven by private sector actors such as ISPs and ICANN, highlighting the role of market-based coordination. Issues such as copyright and intellectual property fall under the purview of national governments operating within international frameworks like WIPO, WTO, and the ITU. In the realm of security and espionage, Nye refers to the UN Charter and the Laws of Armed Conflict (LOAC), while cybercrime is associated with the Budapest Convention. Incident response, finally, is addressed through CSIRTs, often coordinated via regional, bilateral, or national frameworks.[39]

What is particularly noteworthy is how Nye's categorization anticipates the analytical structure of Lessig's Regulatability Theory. His delineation of cyberspace governance implicitly maps onto Lessig's four modalities: architecture (technical standards and network infrastructure), market (intellectual property and commercial governance), law (cybercrime and international security frameworks), and norms (procedural and institutional expectations). Nye's work thus serves as a pivotal bridge between governance theory and practical institutional mapping, providing essential groundwork for this dissertation's interdisciplinary analysis.

The final study worth highlighting is that of Kuerbis and Badiei,[40] which adopts a perspective distinct from the previously discussed works by drawing from institutional economics to analyse cybersecurity governance through the interplay of market, networked, and hierarchical governance structures. While maintaining an institutional focus similar to Portnoy and Goodman or the GLOBE report, their methodology is more theoretically grounded and analytically differentiated. Their central finding is that robust market and networked governance arrangements tend to limit the role of hierarchical (state-based) governance, particularly in proactive (ex-ante)

[39] *Ibid* 7
[40] Kuerbis and Badiei, Mapping the Cybersecurity Institutional Landscape,

cybersecurity initiatives. For instance, efforts to secure Internet identifiers through top-down regulatory means have struggled in the absence of sufficient market demand, while ex post responses, such as botnet mitigation, route monitoring, and information-sharing efforts, have proven more effective under hybrid combinations of governance modes.[41]

Kuerbis and Badiei disaggregate cybersecurity governance into three main structural modalities. Markets are characterized by transactions driven by price mechanisms and information flows, supported by legal instruments and contracts, exemplified by cybersecurity consulting services, security software, and hardware solutions. Networks represent semi-permanent, voluntary systems of cooperation, where interdependent actors negotiate collaboration without centralized authority. These are exemplified in domains such as internet routing coordination, anti-phishing efforts, and botnet mitigation. Hierarchies, by contrast, involve transactions compelled by sovereign authority, as reflected in laws and regulations within national jurisdictions. Notably, while Kuerbis and Badiei do not provide a detailed analysis of individual countries' cybersecurity laws, they aggregate existing literature to identify states with formalized national cybersecurity strategies, thus maintaining relevance to state-based governance without offering granular legal analysis.[42]

A key contribution of their study lies in its emphasis on the role of markets in cybersecurity governance, thereby reinforcing Lessig's "Market" modality as a critical regulatory force in cyberspace. One salient example is their identification of cyber insurance as a market-driven solution to cybersecurity challenges, illustrating how economic incentives can shape security behaviours and risk management strategies in ways that traditional hierarchical approaches may not.[43] This framing not only enriches the analytical landscape of cyberspace governance but also complements this dissertation's broader objective of exploring regulatory pluralism through Lessig's modalities.

It can be seen that a notable trend across existing literature on cyberspace governance is the tendency to narrow the analytical scope to cybersecurity, often treating it as the foundational layer of global cyber governance. This prioritization can be attributed to several structural and historical

[41] *Ibid* 26
[42] *Ibid*
[43] Alessandra Marotta, Luigi Sorrentino, Domenico Liberatore & Jason M. Ingham (2016): Vulnerability assessment of unreinforced masonry churches following the 2010-2011 Canterbury earthquake sequence, Journal of Earthquake Engineering, DOI: 10.1080/13632469.2016.1206761

factors. First, cybersecurity governance emerged as a subfield closely embedded within the technical development of computer networks, particularly the internet.[44] As a socio-technical system, the internet itself is a product of regulatory intervention, government-funded research initiatives, and the interplay of market dynamics and network externalities.[45] Crucially, the internet was not originally designed with security as a core feature. Its architecture was shaped by what scholars describe as the "procrastination principle"[46] the idea that problems should be solved as they arise, and the "trust your neighbor" model, which assumed a relatively competent and trustworthy user base. As internet use expanded to less technically proficient actors, these assumptions became increasingly problematic. The first known cyberattacks emerged as early as the 1980s, but it was in the late 1990s, following the commercialization of the internet, that such threats became more visible and financially consequential.[47] The economic stakes introduced by this commercialization phase elevated cybersecurity as both a policy priority and research focus, prompting international organizations, governments, and private actors to develop governance mechanisms that could respond to emerging digital threats. As such, many early and influential studies understandably framed cyberspace governance primarily through the lens of cybersecurity, treating it as both a practical entry point and a critical domain of global regulatory concern.

Study	Focus	Analytical Approach	Governance Structures Analysed	Key Findings	Relevance
GLOBE Report	Cybersecurity governance via institutional mapping	Typological mapping of 85 membership-based institutions; regime complex framework	State-led institutions, limited multistakeholderism	Transcontinental cooperation more common; institutions Favor 'softer' functions like info-sharing	Introduced regime complex and typological model foundational to analysis

[44] *Ibid* 10
[45] *Ibid* 7
[46] Zittrain, The Future of the Internet and How to Stop It, 31
[47] Yuchong Li and Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments," *Energy Reports* 7 (November 2021): 8176–86, https://doi.org/10.1016/j.egyr.2021.08.126.

Portnoy & Goodman	Organizational and historical account of cyber governance	Descriptive and structured institutional framework	Public and private institutions at multiple governance levels	Lack of standardized metrics despite institutional proliferation	Baseline mapping reference for institutional roles and practices
Joseph Nye	Conceptual framing via regime complex; functional domains	Theoretical framing using regime complex; functional differentiation	Norms, law, market, architecture; multiple issue areas	Cyberspace governance is fragmented but interdependent; aligns with Lessig's theory	Bridges Lessig's theory with practical mapping; highlights intermodal regulation
Kuerbis & Badiei	Cybersecurity governance through institutional economics	Theoretical-economic approach; disaggregated governance structures	Market, networks, hierarchies	Market demand crucial to success; hybrid structures more effective ex post	Highlights market modality; supports analysis of regulatory pluralism

Table 4. Previous Cyberspace Governance Mapping Efforts

While previous studies have made important contributions to the understanding of cyberspace governance, they tend to concentrate primarily on cybersecurity and adopt either an institutional, organizational, or economic perspective. In contrast, this dissertation expands the analytical scope by examining all identifiable cyber-related international legal instruments, not limited to the security domain. The approach is rooted explicitly in the framework of international law, with particular attention to its formal sources, including treaties, customary norms, and institutional practices. Accordingly, the analysis emphasizes international organizations and the legal regimes they generate or participate in, thereby shifting the focus from institutional typologies to legal authority and norm production. Moreover, the dissertation adopts Lessig's Regulatability Theory to map governance across all four modalities: Law, Norms, Market, and Architecture, in order to capture the full spectrum of regulatory mechanisms shaping behaviour in cyberspace. This

multidimensional and legally grounded perspective aims to produce a more comprehensive and systematic mapping of international cyberspace governance than currently exists in the literature.

D. Research Contribution

This dissertation contributes to international legal scholarship in three main ways. First, it advances the discourse on international cyberspace governance by providing one of the most systematic mappings of its regulatory landscape to date. By distinguishing between binding and non-binding instruments, formal law and soft law, and by situating these within Lessig's modalities, the research clarifies how governance actually operates across institutional levels and regions. This empirical foundation brings greater transparency to a field often described as fragmented but rarely mapped with this degree of precision.

Second, it offers a comparative regional perspective that has been largely absent in cyberspace law literature. By juxtaposing the UN, the EU, and ASEAN (alongside ASEAN member states), the study highlights not only the different institutional capacities of these actors but also their divergent governance philosophies. In doing so, it demonstrates how Southeast Asia is carving out a distinctive approach to cyberspace governance; consensus-based, norm-driven, and pragmatic that both complements and diverges from Western legalist traditions. This contributes to debates on regime complexity, fragmentation, and legitimacy in international law.

Third, and most distinctively, the thesis introduces the concept of easternisation into international legal scholarship and provides a framework to make it empirically testable. While existing debates on regime complexity emphasize pluralisation and decentralization,[48] this study develops operational indicators that reveal how Southeast Asian approaches diverge from Western-dominated models. These indicators include: (i) the share of norm-setting instruments produced by ASEAN compared to UN and EU institutions, (ii) the balance between binding and non-binding instruments, (iii) the extent to which ASEAN instruments cross-reference Western frameworks or generate autonomous rules, and (iv) the institutional centrality of ASEAN within the broader governance network. By applying these indicators, the dissertation demonstrates that

[48] See Anne Peters, The Refinement of International law: From Fragmentation to regime interaction, and politicization, I-CON, Vol. 15, No.3, pp.671-704, 2017, Gómez-Mera, Laura. "International Regime Complexity." Oxford Research Encyclopedia of International Studies. 31 Aug. 2021; Accessed 25 Sep. 2025. https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-648.,

ASEAN's approach reflects more than regionalisation; it signals a shift in the geography of international lawmaking authority, thus evidencing the easternisation of international law.

E. Innovative Content

The innovation of this study lies both in its methodological design and its theoretical framing. Methodologically, the dissertation pioneers the use of computational analysis of international law in the context of cyberspace. Drawing inspiration from Lie, Langford and Wolfgang,[49] it combines traditional document analysis with computational classification, coding, and visualization. The result is a large-N, empirically grounded ontology of 148 governance instruments, systematically coded across thirteen fields. This integration of "distant reading" (large-scale computational mapping) and "close reading" (qualitative interpretation) marks a methodological advance in international legal research, making fragmented and voluminous legal materials more comprehensible.

Analytically, the dissertation innovates by applying LRT (originally developed for domestic cyberspace regulation) to the domain of international law. This cross-application not only demonstrates the theory's explanatory value for mapping global governance modalities but also adapts it to highlight how law, norms, markets, and architecture interact differently across regions and institutional levels.

The most significant innovation lies in theorizing the easternisation of international law through the case of cyberspace governance. While much scholarship critiques the Western-centric foundations of international law, this study demonstrates empirically how Southeast Asia is shaping a parallel governance trajectory. To do so, it operationalizes easternisation through measurable indicators: (i) norm-setting share across regions, (ii) binding versus non-binding mix, (iii) cross-referencing practices, and (iv) institutional centrality within the regime complex. These indicators provide concrete empirical grounding to a concept that has previously remained abstract, allowing easternisation to be tested and distinguished from general processes of regionalisation or pluralisation.

[49] Runar Hilleren Lie and Malcolm Langford, "The Computational Turn in International Law," *Nordic Journal of International Law* 93, no. 1 (2024): 38–67, https://doi.org/10.1163/15718107-bja10081., Alschner Wolfgang, The Computational Analysis of International Law, in *Research Methods in International Law*, ed. Rossana Deplano and Nicholas Tsagourias (Edward Elgar Publishing, 2021), https://doi.org/10.4337/9781788972369.

Together, these innovations allow the dissertation to speak both to doctrinal debates about the sources and authority of international law and to theoretical debates about regime complexity, legitimacy, and the evolving balance between Western and non-Western governance paradigms.

CHAPTER II
RESEARCH METHODOLOGY

A. Applied methodology

This dissertation is situated within the tradition of empirical legal research, but it takes a distinctive form by incorporating both qualitative interpretation and quantitative mapping. At its core, the study builds on document analysis, yet it moves beyond conventional doctrinal methods by adopting computational tools of classification, coding, and visualization. The empirical foundation of the project is a curated corpus of 148 instruments of cyberspace governance issued by the United Nations, the European Union, ASEAN, and ASEAN member states.[50] Each instrument was examined not only in terms of its formal legal attributes but also through its functional and regulatory qualities, allowing the mapping of cyberspace governance across multiple layers of authority.

This design reflects what Wolfgang has described as the growing need for international lawyers to engage with "big data" approaches, as traditional methods premised on "small data" become increasingly inadequate in capturing the breadth and fragmentation of international law.[51] At the same time, the approach aligns with Lie and Langford's observation that computational analysis does not replace doctrinal reading but complements it through a "distant reading" of entire corpora alongside close legal interpretation.[52] In practice, this means that this dissertation draws on computational analysis to systematize and classify a large dataset of documents, while retaining the interpretive richness of legal reasoning to make sense of the results.

Methodologically, the research unfolded in four steps. First, relevant documents were systematically collected from institutional repositories such as the UN Official Document System, EUR-Lex, ASEAN databases, and the UNIDIR Cyber Policy Portal. Second, the documents were filtered and cleaned to ensure consistency, excluding informal or non-legal materials and removing duplicates. Third, each instrument was coded through a classification ontology of thirteen fields, covering aspects such as governance type, document form, source of international law, and Lessig's four regulatory modalities. Finally, the data was analyzed through a

[50]

[51] Wolfgang, Computational Analysis, 203

[52] Lie and Langford, The Computational Turn, 50

combination of manual interpretation and computational visualization, with Tableau dashboards used to generate comparative and temporal mappings across regions, levels, and modalities.

B. Research approach

The research approach can be best understood as epistemological within the computational turn in international law. While ontological approaches view computation as fundamentally transforming how law is conceived, this dissertation adopts the more modest and pragmatic position that computational methods serve to enrich existing doctrinal inquiry by extending its scale and evidentiary base.[53] Wolfgang has shown how computational tools enable doctrinal research to become more comprehensive, reproducible, and transparent, correcting its traditional tendency toward anecdotal evidence and selective sampling.[54] Similarly, Lie and Langford argue that the computational turn expands the epistemological repertoire of legal scholars, allowing them to discern patterns and networks that would remain invisible through manual analysis alone.[55]

The project therefore frames itself as an interpretive case study of cyberspace governance, with ASEAN as its focal lens. This comparative orientation (contrasting ASEAN with the UN and EU) allows both horizontal analysis across regions and vertical analysis between domestic, regional, and global levels. The logic is abductive: the mapping first surfaces empirical patterns that were not predetermined, such as modality asymmetries or ASEAN's unusual balance of law, norms, and architecture. These inductive findings are then reinterpreted through theoretical scaffolds, namely Lessig's Regulatability Theory, regime complex theory, and the easternization framework. The result is a cyclical process of discovery and theorization in which empirical material both grounds and challenges conceptual claims.

Methodologically, the study employs a combination of manual and computational techniques. Regular expression searches and dictionary-based coding were used to ensure consistency and exhaustiveness,[56] while the interpretive classification of instruments allowed nuanced judgments about scope, modality, and function. Visualization through **Tableau** facilitated the macroscopic reading of patterns across time and region, while doctrinal interpretation ensured that the data

[53] *Ibid*
[54] Wolfgang, Computational Analysis, 214
[55] Lie and Langford, The Computational Turn, 42
[56] Wolfgang, Computational Analysis, 211

remained situated in international law's normative and institutional context. This fusion of "distant" and "close" reading responds to Lie and Langford's call for a more balanced engagement with computational tools: they are not an end in themselves, but a method of expanding the epistemic reach of international law research.[57]

C. Analytical Threshold

The analytical threshold of the study lies in distinguishing descriptive mapping from normative claims. To maintain rigor, the unit of analysis was defined as the individual governance instrument, which had to meet two criteria: formal issuance by a state or international organization, and substantive relevance to at least one of the seven cyberspace governance clusters identified by the UN Commission on Science and Technology for Development (infrastructure, security, human rights, legal, economic, development, socio-cultural).[58]

Each document was coded against sources of international law as defined in Article 38(1) of the ICJ Statute, with an additional category of "national law" created to capture the substantial role of ASEAN states in norm production. Lessig's modalities were operationalized in precise terms: law was coded where obligations were binding and enforceable, norms where regulation was voluntary or declaratory, architecture where technical design choices constrained behavior, and market where economic structures or incentives acted as regulators.[59] Hybrid instruments were recognized as such when more than one modality was substantively operative.

Thresholds for analytical claims were then established. Overlap between regimes was only coded where two or more instruments addressed the same governance scope, and strong overlap was noted only when explicit cross-referencing occurred. Vertical fragmentation was assessed by comparing the balance of modalities and sources across domestic, regional, and global levels. Claims of easternization were grounded not in isolated examples but in recurring evidence across multiple instruments and issue areas. Validation procedures included cross-checks of coding consistency, triangulation across classification fields, and construct validation through anchoring the framework in established doctrinal categories.[60]

---

[57] Lie and Langford, The Computational Turn, 45
[58] Commission on Science and Technology for Development Eighteenth session, Mapping of international Internet public policy issues, E/CN.16/2015/CRP.2 17 April 2015,
[59] Wolfgang, Computational Analysis, 211
[60] Lie and Langford, The Computational Turn, 64

By making these thresholds explicit, the study ensures that its claims about fragmentation, regime complexity, and easternization are not speculative but grounded in reproducible coding and analysis. At the same time, it acknowledges the limitations identified by both Wolfgang and Lie: computational analysis cannot capture every nuance of legal meaning, and its results must always be reintegrated into interpretive, qualitative reasoning.[61] It is in this balance; between computation and interpretation, between scale and depth that the methodological novelty of this dissertation lies.

D. Data collection

The empirical foundation of this dissertation is a systematically compiled corpus of 148 governance instruments relating to cyberspace. The unit of analysis is the formal governance document: laws, treaties, strategies, declarations, regulations, or cooperation frameworks, produced by international organizations, regional bodies, or states. These instruments were selected on the basis of their explicit relevance to cyberspace governance, whether through legal commitments, normative guidance, institutional design, or technical regulation.

1. Population and Scope

The scope of the dataset was restricted to formal state and intergovernmental outputs with identifiable legal, normative, or regulatory content. This decision reflects the study's orientation toward international legal authority, rather than informal or scholarly discourse. Consequently, several categories of material were excluded:

a. Institutional focus and selection of governance subjects

The selection of the United Nations (UN), the European Union (EU), and the Association of Southeast Asian Nations (ASEAN) as the primary governance subjects reflects the dissertation's grounding in international law rather than in state-centric cyber power or technological leadership. The analysis focuses on international and regional organizations that possess recognized legal personality and norm-generating capacity within the international legal system, and that function as institutional sites for the articulation, coordination, and diffusion of legal and quasi-legal norms. The UN, EU, and ASEAN thus provide a coherent comparative basis for examining

[61] *Ibid* 46

fragmentation, regime interaction, and modality variation in international cyberspace governance.

The exclusion of individual states, including the United States, is a deliberate methodological choice. While the United States has played a central historical role in the development of the internet and remains a dominant cyber power, its inclusion would introduce analytical asymmetry by juxtaposing a single sovereign state against international organizations with collective decision-making structures and distinct legal mandates. Such a comparison would complicate cross-regional analysis without advancing the study's core objective, which is to assess patterns of governance within international and regional legal frameworks rather than national cyber strategies.

This institutional focus also informs the exclusion of judicial decisions as a primary unit of analysis. Although jurisprudence constitutes a recognized source of international law, the absence of adjudicatory mechanisms within ASEAN would result in structural imbalance across the selected regimes. To maintain comparability, the study therefore concentrates on governance instruments that are common to all three contexts, including treaties, legislation, strategies, declarations, and cooperative frameworks.

b. Excluded materials

   i. Academic commentary and policy briefs, unless officially endorsed or adopted by a state or international organizations
   ii. Draft instruments or proposals, unless they had been formally adopted into an official process.
   iii. Documents not primarily cyber-related, such as general market or trade agreements (e.g., WTO, TRIPS, EU Digital Single Market), even if they carry digital implications. Their exclusion ensures that the dataset focuses on instruments directly situated within the governance of cyberspace.
   iv. Court decisions and jurisprudence, despite their legal significance, were excluded because of the uneven role of adjudication across regions (notably the EU) and to maintain comparability between UN, EU, and ASEAN sources.

2. Sources

To ensure coverage across institutional and national levels, documents were drawn from multiple repositories:

a. UN system: UNIDIR Cyber Policy Portal, UN Official Document System (ODS).
b. European Union: EUR-Lex database of EU law and policy.
c. ASEAN and Member States:[62] ASEAN Document Database, ASEAN Secretariat archives, and selected national legal repositories.

This multi-source strategy follows the practice of prior large-scale governance mappings, where reliance on a single repository risks under-representing particular regions or document types.

3. Filtering and Verification

Each candidate document underwent a verification protocol before inclusion:

a. Duplication checks: updated or amended instruments replaced earlier versions.
b. Finality: only formally adopted instruments were included; draft papers, consultations, or discussion notes were excluded.
c. Institutional attribution: documents were attributed to their issuing body at the highest level (e.g., ASEAN Summit declaration rather than working group communiqué) unless the subsidiary instrument had distinct legal or policy standing.
d. Cross-checking: ambiguous cases (e.g., whether a cooperation MoU had regulatory implications) were validated by triangulating multiple repositories or official press releases.

4. Coding Framework

All included documents were coded into a structured dataset using a thirteen-field classification system developed for this research. These fields capture legal, institutional, and functional attributes:

a. Document Title
b. Source/Link
c. Year
d. Country/Region (UN, EU, ASEAN, AMS)
e. Level (International, Regional, National)

[62] The ASEAN dataset is limited to instruments produced by the original ten ASEAN member states and excludes documents from newly admitted members to maintain analytical consistency across the study period.

f. Institution
g. Legal Subject (States, IOs)
h. Governance Type (Policy, Legislation, Structure, Cooperation)
i. Document Type (Law, Act, Convention, Strategy, Agreement, etc.)
j. Source of International Law (Treaties, Customs, General Principles, Judicial Decisions)
k. Lessig's Modality (Law, Norms, Architecture, Market)
l. Keywords/Indicators
m. Summary/Notes

This coding system operationalizes theoretical categories; Lessig's modalities, UNIDIR governance functions, and regime complex indicators, into an empirical ontology of cyberspace governance.

Document	Year	Country /Region	Level	Institution	Legal Subject	Governance function
A/72/327: Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security	2017	UN	International	UN General Assembly	IO	Cooperation
Roadmap for Digital Cooperation (Report of the Secretary-General)	2020	UN	International	UN Secretary General	IO	Cooperation
EU Cybersecurity Strategy 2020	2020	EU	Regional	European Commission	IO	Policy
EU Data Governance Act	2022	EU	Regional	European Parliament & Council	IO	Legislation
ASEAN ICT Masterplan 2020	2020	ASEAN	Regional	ASEAN	State	Cooperation

ASEAN Declaration to Prevent and Combat Cybercrime	2017	ASEAN	Regional	ASEAN Heads of State/Government	State	Cooperation
Computer Misuse Act 1993 (2020 Revised Edition)	2021	Singapore	National	Parliament of Singapore / Law Revision Commission	State	Legislation
Electronic Commerce Act 2006 (Act 658)	2006	Malaysia	National	Parliament of Malaysia	State	Legislation

Table 1 - Sample of Codebook - First Section

Document	Document type	Source of IL	Lessig's Modality	Main Scope	Supporting Scope	Governance Type
A/72/327: Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security	Report	General principles	Norms	Infrastructure and standardization	Security	Algorithmic
Roadmap for Digital Cooperation (Report of the Secretary-General)	Roadmap	General principles	Norms	Economy	Development	Institutional
EU Cybersecurity Strategy 2020	Strategy	General principles	Law, Market, Norms	Development	Legal	Institutional
EU Data Governance Act	Act	Treaties/ Convention	Architecture	Infrastructure and standardization	Infrastructure and standardization	Legal

ASEAN ICT Masterplan 2020	Workplan	General Principle	Architecture, Norms	Development	Security	Institutional
ASEAN Declaration to Prevent and Combat Cybercrime	Declaration	General Principles	Market, Norms	Human Rights	Economy	Institutional
Computer Misuse Act 1993 (2020 Revised Edition)	Act	National Law	Law	Security	Security	Legal
Electronic Commerce Act 2006 (Act 658)	Act	National Law	Law	Security	Economy	Legal

Table 2 Sample of Codebook - Second Section

For the full dataset refer to **ANNEX A**

Document title	Ambiguity	Decision
Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age (A/HRC/27/37) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/72/327)	Whether the legal subject should be coded as International Organization (IO) or State, since these institutions are comprised of member states and their representatives.	Coded as IO, on the basis that when drafting and adopting such reports, member states act collectively under the institutional mandate, representing the institution rather than their individual national interests.
EU-Malaysia Framework Agreement on Partnership and Cooperation (2022)	Whether the agreement should be classified as an EU document or a Malaysian document, since it was jointly negotiated and signed by both parties.	Coded under EU, as the agreement was initiated by the EU, requires ratification by EU Member States and conclusion at the EU level, and only enters into force once both the EU and Malaysia complete their respective ratification processes.

Table 3 Sample of Ambiguous Coding

5. Protocol for coding

a. Date of adoption was recorded as the official year of publication or entry into force.
b. Binding status was determined by formal designation (e.g., treaty, directive, law) versus soft instruments (strategy, declaration, framework).
c. Scope of governance was coded according to the CSTD's seven categories (security, infrastructure, human rights, legal, economic, development, socio-cultural), with both main and supporting scopes assigned.
d. Institutional attribution prioritized the highest legally responsible body but noted subsidiary or implementing agencies in the summary field.

Through this process, the dataset provides a replicable and transparent empirical base for the subsequent analysis of fragmentation, regime complexity, and easternisation in international cyberspace governance.

6. Reliability and Consistency

Although coding was conducted by a single researcher, steps were taken to enhance reliability and minimize subjective bias. A pilot round of coding was conducted on a subset of documents to test the clarity of the classification fields and refine the codebook where necessary. During the main coding process, consistency checks were performed by re-coding a random sample of documents at different stages of the research, with results compared to the original entries to identify discrepancies. This iterative process helped ensure that coding decisions were applied systematically across the entire dataset.

CHAPTER III
THEORETICAL FRAMEWORK

A. Conceptual foundations of cyberspace governance

1. Governance of Cyberspace

The discourse of cyberspace governance essentially concerns power in cyberspace.[63] With the current state of cyberspace and the extent of its development, the outcomes it has produced, whether positive or negative, are often perceived as unintentional by-products. When identifying certain debates such as privacy, surveillance, cyber-terrorism, and security, it is seldom that one views them holistically. To understand the distribution of power in cyberspace, it is necessary to take a bird's-eye view of who owns, controls, designs, and shapes it.

While efforts to map cyberspace governance vary, its definition remains contested. One conceptualization comes from Tsagourias, who describes it as an encompassing process of action coordination, understood from a sociological perspective to involve the interaction of states, markets, and corporate hierarchies.[64] However, while such definitions capture the multiplicity of actors involved, they do not fully account for the types of governance these actors perform. To address this gap, this study proposes a conceptual distinction between three interrelated forms of governance in cyberspace: algorithmic governance, institutional governance, and legal governance.[65] Rather than focusing solely on governance functions, such as norm-setting or capacity-building, this typology emphasizes the regulatory forms and mechanisms through which governance is exercised.

The algorithmic governance of cyberspace is derived from self-executing coded procedures that depart from the concept of formalism. [66] In coding, human expression is extracted through qualitative language theory and is reduced to sequences of zeros and ones. Only coders and their associated technical culture can understand and design this layer of

[63] Outi Korhonen and Ekaterina Markovich, "Mapping Power in Cyberspace," in *Resaerch Handbook on International Law in Cyberspace*, ed. Nicholas Tsagourias and Russel Buchan (United Kingdom: Edward Elgar Publishing, 2021).
[64] Nikolaos K.. Tsagourias and Russell. Buchan, "Research Handbook on International Law and Cyberspace," 2023, 672,https://www.e-elgar.com/shop/gbp/research-handbook-on-international-law-and-cyberspace-9781035316854.html.
[65] Korhonen and Markovich, Mapping Power, 47
[66] *Ibid*

cyberspace. Most users would not be able to name the organizations that manage internet domains or explain the infrastructure that maintains cyberspace and its ownership. Algorithmic governance, in this sense, refers to the regulation of cyberspace through code, protocols, and the design of technical infrastructures.[67] Regulatory choices are embedded directly into the architecture of cyberspace, shaping how systems operate and constraining the behaviour of users and intermediaries by technical means. Technical standards and digital protocols are not neutral; they embody specific regulatory logics and policy goals. Control over code and infrastructure is concentrated among technical communities and standard-setting bodies such as the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet Engineering Steering Group (IESG), and the Internet Corporation for Assigned Names and Numbers (ICANN). [68]

Institutional governance captures the political processes, agenda-setting activities, and multistakeholder collaborations that shape cyberspace through collective decision-making and norm diffusion. While public perception often points to Big Tech companies such as Google, Amazon, Facebook, and Apple as the operators of cyberspace, these firms are only the visible tip of the governance iceberg. The ecosystem also includes a range of public and private institutions; technical governance bodies, intergovernmental organizations, and regional entities; that influence cyberspace policy and practice. These processes often occur within international organizations, regional bodies, and industry coalitions, involving both state and non-state actors seeking to coordinate governance efforts and shape global discourse. States have become deeply engaged in cyberspace governance, as illustrated by initiatives such as Estonia's e-government projects, the EU's cyber policies, the United Nations cyber working groups, Georgia's crypto-mining infrastructure, and NATO's cybersecurity capabilities.

Legal governance refers to the application of formal legal instruments (including treaties, national legislation, and judicial decisions) to regulate cyberspace activities. This more traditional form of rule-based governance achieves compliance through binding obligations and enforcement mechanisms. Legal entities in cyberspace are often international in scope; ICANN, while organized as a California-based non-profit, operates transnationally with

[67] *Ibid*
[68] *Ibid* 48

public-interest commitments that interact with, and are influenced by, international norms.[69] Although the US government relinquished its oversight of ICANN in 2016, transitioning it into an international organization, Internet governance remains influenced by powerful corporate and state stakeholders, producing a hierarchical structure in which the strong dominate and the weak have limited influence. The tension between multi-stakeholder governance and cyberspace sovereignty is central here. While traditional telecommunications infrastructure falls within sovereign control, global Internet communications blur sovereignty's boundaries. Nevertheless, because the physical infrastructure of cyberspace; servers, cables, and data centers exist within national territories, sovereignty claims remain materially grounded. Recognition of cyberspace sovereignty is crucial for effective legislation, combating cybercrime, and regulating harmful content, as reflected in the integration of sovereignty principles into national legal and administrative systems. [70]

Drawing on Baldwin, Cave, and Lodge's distinction between technical and content regulation,[71] algorithmic governance primarily aligns with the regulation of technical infrastructure, encompassing the coordination and standardization of digital identifiers, communication protocols, and security architectures that sustain cyberspace. Institutional governance and legal governance, by contrast, align more closely with content regulation, encompassing the regulation of behaviour, speech, data flows, and informational content. Thus, cyberspace governance operates simultaneously at the level of infrastructure: through technical control, and at the level of content: through legal and institutional mechanisms. The complexity and evolution of cyberspace, shaped by rapidly shifting commercial practices and social uses of the Internet, prevent the establishment of a singular, coherent regulatory regime. Instead, governance consists of a patchwork of mechanisms: legal statutes, binding and non-binding technical standards, bilateral and multilateral agreements, informal codes of conduct, and voluntary best practices.[72] This multiplicity reflects the

[69] Binxing Fang, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* (Springer Singapore, 2018), https://doi.org/10.1007/978-981-13-0320-3.
[70] *Ibid* 85
[71] Robert Baldwin, Martin Cave, and Martin Lodge, *The Oxford Handbook of Regulation*, *The Oxford Handbook of Regulation* (Oxford University Press, 2010), https://doi.org/10.1093/oxfordhb/9780199560219.001.0001.
[72] Brenden Kuerbis and Farzaneh Badiei, "Mapping the Cybersecurity Institutional Landscape," *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 466–92, https://doi.org/10.1108/DPRG-05-2017-0024/FULL/XML.

polycentric nature of cyberspace governance, where overlapping actors and mechanisms interact without a central authority.[73] Regulation in this context ranges from coercive legal mandates to more diffuse forms of coordination and norm diffusion.[74] In its broadest sense, regulation refers to any deliberate collective action in the public interest, encompassing both public and private rulemaking, whether through mandatory laws or voluntary guidelines. [75]

This regulatory complexity is reflected in scholarly conceptualizations of the Internet's architecture. While some describe the Internet as comprising five layers, others use simplified models. Benkler identifies three layers: physical infrastructure, code, and content.[76] Zittrain similarly distinguishes physical, protocol, and application layers.[77] Habermas condenses these into two primary layers: the technical layer, comprising the infrastructure of cyberspace (e.g., TCP/IP protocols, browsers, cables, routers, and computers),[78] and the content layer, consisting of the applications and services enabling the production, transmission, filtering, and storage of content. Across these models, there is consensus that the lower layers are governed primarily through technical protocols and standards, while the upper layers involve social, cultural, and political dynamics. This layered structure parallels Baldwin, Cave, and Lodge's distinction: regulation of technical infrastructure; largely the domain of algorithmic governance, focuses on identification, compatibility, interconnectivity, and technological coordination, while content regulation (largely the domain of institutional and legal governance) addresses privacy, intellectual property, e-commerce, and the suppression of illegal content and conduct, employing approaches ranging from state legislation to platform content moderation policies.

By framing cyberspace governance through the three governance types; algorithmic, institutional, and legal, this study captures both the layered structure of the Internet and the diverse forms of regulation operating within it. Algorithmic governance maps onto the regulation of technical infrastructure, while institutional and legal governance address the

[73] Chang, Lennon YC, and Peter Grabosky, "The Governance of Cyberspace," in *Regulatory Theory: Foundations and Applications*, ed. Peter Drahos (ANU Press, 2017).
[74] Michael Barnett and Raymond Duvall, "Power in Global Governance," in *Power in Global Governance* (Cambridge University Press, 2004), 1–32, https://doi.org/10.1017/CBO9780511491207.001.
[75] Tsagourias and Buchan, Research Handbook, 37
[76] Yochai Benkler, *The Wealth of Networks How Social Production Transforms Markets and Freedom* (Yale University Press, 2006).
[77] Jonathan L Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press & Penguin UK, 2008).
[78] Jürgen Habermas, *Theorie Des Kommunikativen Handelns*, vol. 1 (Suhrkamp, 1995).

regulation of content. Together, these forms reflect the multilayered and fragmented nature of cyberspace governance, where technical design, political agendas, and legal norms intersect to shape the evolving global digital order.

2. Key governance regimes in cyberspace[79]

a. United Nations (UN)

The UN plays a pivotal (though often contested) role in the governance of cyberspace. Formal activity on cyber-security within the UN began in 1998, when the Russian Federation introduced a draft resolution to the UN General Assembly (UNGA) on "developments in the field of information and telecommunications in the context of international security".[80] This early engagement was modest in scope, with progress slow and discussions initially perceived as "dull" and lacking momentum.[81] However, a series of high-profile incidents, including the Distributed Denial of Service (DDoS) attacks on Estonia (2007)[82] and Georgia (2008),[83] the Stuxnet worm attack against Iran's nuclear programme (2010),[84] the Edward Snowden disclosures on state surveillance (2013),[85] and allegations of Russian interference in the 2016 U.S. elections,[86] brought renewed urgency to the issue. These events underscored the real-world security, political, and economic consequences of malicious activity in cyberspace, pushing cyber-security higher up the global governance agenda.[87]

---

[79] Tsagourias and Buchan, Research Handbook, 582

[80] Eneken Tikk-Ringas, "International Cyber Norms Dialogue as an Exercise of Normative Power," *Georgetown Journal of International Affairs* 17, no. 3 (2016): 47–59, https://doi.org/10.1353/gia.2016.0036.

[81] *Ibid*

[82] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" (Cooperative Cyber Defence Centre of Excellence, 2007)., Haataja, S. (2017). The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, 9(2), 159–189. https://doi.org/10.1080/17579961.2017.1377914

[83] Paulo Shakarian, "The 2008 Russian Cyber-Campaign Against Georgia," *Military Review*, 2011, 63–68., Maisaia, V., Guchua, A., & Zedelashvili, T. (2020). The cybersecurity of Georgia and threats from Russia. Eastern Review, 9, 105–119. https://doi.org/10.18778/1427-9657.09.07

[84] Marco De Falco, "Stuxnet Facts Report: A Technical and Strategic Analysis" (Tallin, 2012).

[85] Kiyoshi Murata, Andrew A. Adams, and Ana María Lara Palma, "Following Snowden: A Cross-Cultural Study on the Social Impact of Snowden's Revelations," *Journal of Information, Communication and Ethics in Society* 15, no. 3 (August 14, 2017): 183–96, https://doi.org/10.1108/JICES-12-2016-0047.

[86] Andrew R. N. Ross, Cristian Vaccari, and Andrew Chadwick, "Russian Meddling in U.S. Elections: How News of Disinformation's Impact Can Affect Trust in Electoral Outcomes and Satisfaction with Democracy," *Mass Communication and Society* 25, no. 6 (November 2, 2022): 786–811, https://doi.org/10.1080/15205436.2022.2119871.

[87] Tsagourias and Buchan, Research Handbook, 607

Despite this growing attention, progress within the UN has been hindered by deep geopolitical divisions. Core disagreements persist between Eastern and Western states over several foundational issues: whether the governance of cyberspace should prioritise the free flow of information or impose governmental controls; whether the main focus should be on economic espionage and cybercrime or on state-led cyber-attacks; and whether existing international law suffices or whether new, binding instruments are needed. These disagreements mirror broader geopolitical fault lines and have shaped the fragmented nature of UN-level discussions. Nevertheless, the UN has, for over a decade, sought to bridge these divides and develop mechanisms to ensure the stability and security of cyberspace.[88]

The UN's cyber governance efforts span multiple institutional bodies, each with distinct mandates and governance modalities. The UN Security Council (UNSC), as the only UN organ whose Chapter VII resolutions carry binding obligations on Member States, has addressed cyber issues mainly through counterterrorism and international peace and security frameworks.[89] The Office of the Secretary-General has sought to advance digital cooperation and promote inclusive, multi-stakeholder governance through initiatives such as the Roadmap for Digital Cooperation.[90] The Economic and Social Council (ECOSOC), particularly through the Commission on Crime Prevention and Criminal Justice (CCPCJ), has focused on cybercrime prevention, capacity-building, and the potential development of a global cybercrime treaty.[91] Technical and operational governance is shaped by the International Telecommunication Union (ITU), the UN's specialised agency for ICTs, which plays a central role in setting standards, building capacity, and fostering international cooperation. Research and policy development are supported by bodies such as the United Nations Institute for Disarmament Research (UNIDIR), which contributes analytical tools like the Cyber

[88] Christian Henderson, "The United Nations and the Regulation of Cyber-Security," in *Research Handbook on International Law in Cyberspace*, ed. Nicholas Tsagourias and Russel Buchan (Edward Elgar Publishing, 2021), 582–615.
[89] This authority, however, does not amount to a general international lawmaking power, but is confined to maintaining or restoring international peace and security as provided in Articles 24 and 39 of the UN Charter. *See* Maurizio Arcari, Limits to Security Council Powers under the UN Charter and Issues of Charter Interpretation, pp.239-259 in *Polish Yearbook of International Law XXXII*, Wydawnictwo Naukowe Scholar, 2013
[90] Henderson, The United Nations, 582
[91] *Ibid*

Policy Portal and convenes expert dialogues. The United Nations Office on Drugs and Crime (UNODC) operationalises many of these norms through technical assistance, particularly in law enforcement and criminal justice responses to cybercrime.[92]

Hence, these institutions form a complex web of overlapping mandates within the broader international cyber regime complex. While the UN has not established a single, comprehensive cyber-security treaty or governance framework, its diverse initiatives reflect a gradual institutionalisation of cyber norms, capacity-building programmes, and cooperative mechanisms. These activities also demonstrate how the UN's role in cyberspace governance is both shaped and constrained by geopolitical contestation, institutional fragmentation, and the competing regulatory philosophies of its member states.

i. UN General Assembly

The origins of the UN discourse on cyber norms can be traced to a proposal by the Russian Federation to the United Nations General Assembly (UNGA) First Committee; the Disarmament and International Security Committee, which, in 1999, adopted the first resolution in a series entitled *"Developments in the field of information and telecommunications in the context of international security"* (UNGA 1999).[93] In its 1998 proposal, Russia argued that the rapid development and application of new information technologies and telecommunications represented a qualitatively new stage of the scientific and technological revolution.[94] While acknowledging the many positive effects of this revolution, Russia warned of potential threats arising from growing dependence on ICTs. Such technologies, it argued, could be used for purposes incompatible with the objectives of maintaining international peace and security[95] and could violate core principles of international law, including the non-use of force, non-intervention, and respect for human rights and fundamental freedoms.[96] Russian Foreign Minister Igor Ivanov stressed that

[92] *Ibid*
[93] *Ibid*
[94] Dennis Broeders, Bibi van den Berg, Governing Cyberspace: Behaviour, Power, and Diplomacy
[95] UNGA Res 53/70 4 December 1998 UN Doc A/RES/53/70
[96] François Delerue, Arun Sukumar, and Dennis Broeders, "RESPONSIBLE BEHAVIOUR IN CYBERSPACE Global Narratives and Practice Edited By," n.d., https://doi.org/10.2815/643871.

these risks required preventive action to avoid the emergence of a "fundamentally new area of international confrontation," potentially leading to an arms race based on the latest technological developments.[97] The proposal called for a ban on "information weapons," which Russia claimed could be as destructive as weapons of mass destruction (UNGA 1998).[98]

At the time, however, the international community (particularly technologically advanced Western states); was not eager to pursue multilateral negotiations on ICT regulation.[99] The proposal was widely perceived as an attempt to negotiate a treaty prohibiting information weapons and preventing "information wars".[100] In the early 2000s, during the Bush administration, differing policy priorities and scepticism toward the Russian initiative stalled progress on discussions of responsible state behaviour in cyberspace.[101] It was not until 2004, six years after the original proposal, that the resolution provided the basis for convening the first session of the UN Group of Governmental Experts (GGE) under Russian chairmanship.[102] The GGE's mandate was to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as to study international concepts aimed at strengthening the security of global ICT systems.[103] However, this first GGE did not produce a consensus report, due to the reluctance of permanent members of the UN Security Council to approve it and the lack of broader international interest in cyber stability issues at the time.[104]

The United Nations Group of Governmental Experts (UN GGE), formed in the 1990s, initially received little attention from Western states.[105] However, its 2013 report, recognizing the application of international law to cyberspace,

[97] *Ibid* 187
[98] *Ibid* 64
[99] *Ibid* 11
[100] Alexandra Kulikova, "Working out the Rules of Global Cyberspace Governance," in *Securing Cyberspace: International and Asian Perspectives*, ed. Cherian Samuel and Munish Sharma (Pentagon Press, 2016).
[101] *Ibid* 81
[102] *Ibid*
[103] *Ibid* 87
[104] Henderson, The United Nations, 588
[105] Tikk-Ringas, International Cyber Norms, 2

marked a significant milestone.[106] Additionally, in 2011, Russia and its partners in the Shanghai Cooperation Organization submitted the first draft of the International Code of Conduct for information security, outlining principles for responsible state behaviour in securing information and cybersecurity.[107] Despite limited support, this initiative demonstrated early efforts towards norms building. The UN GGE report of 2015 further emphasized the desire of states to find common ground on cybersecurity standards, despite their differences.[108]

Regionally, the Organization for Security and Cooperation in Europe (OSCE) countries signed Confidence Building Measures (CBMs) in 2013 to reduce ICT-related conflict risks, followed by an extension of practical cooperation measures in 2016.[109] The BRICS Summit Declaration in 2015 also emphasized the importance of developing norms for cyberspace conflict prevention.[110] Additionally, bilateral agreements, particularly within the US-China-Russia triangle, have contributed to norms building efforts by establishing mutual CBMs and conduct principles in the cyber domain[111].

Although there is no binding instrument to regulate cyberspace, the UN GGE can be considered a normative tool and platform for countries to further advance their national interests regarding the development and use of cyberspace.[112] The UN GGE establishes a series of principles that apply in the UN Charter and international law such as: sovereignty; sovereign equality; peaceful resolution of international disputes; prohibition of the threat or use of force against the territorial integrity or political independence of a State, or in any manner inconsistent with the purposes of the United Nations; respect for

[106] UNGA Doc. A/70/174 (22 Jul. 2015)
[107] Tikk-Ringas, International Cyber Norms, 2
[108] Fang, Cyberspace Sovereignty, 164
[109] Tikk-Ringas, International Cyber Norms, 5
[110] *Ibid*
[111] *Ibid*
[112] Heli Tiirmaa-Klaar, "The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body Cyberstability Paper Series New Conditions and Constellations in Cyber," 2021.

human rights and fundamental freedoms; and non-intervention in the internal affairs of other countries.[113]

The initiation of the GGE, first proposed by Russia, aims to consider existing and potential threats in the field of information security and possible cooperative actions to overcome them.[114] It also conducts studies on international concepts aimed at strengthening the security of global information and telecommunications systems.[115] The second UN GGE invited further dialogue between states to discuss norms relating to state use of ICT, reducing collective risks, and protecting critical national and international infrastructure, as well as recommending confidence-building strategies.[116] This was followed by the third UN GGE, which discussed the application of international legal norms regarding responsible state behaviour.[117] These are considered voluntary, non-binding norms that do not seek to limit or prohibit actions consistent with international law.[118]

The standards set by the UN GGE include the application of international humanitarian law; the application of the law of armed conflict (LOAC) in cyberspace; and the principle that cyberspace is to be used peacefully[119]. The UN GGE report highlights the principles of sovereign equality, the peaceful resolution of international disputes, the obligation to refrain from the threat or use of force, and non-intervention.[120] The GGE also provides views on how international law applies to a country's use of ICT, affirming that states have jurisdiction over ICT structures located in their respective territories and the inherent right to act consistent with international law, as recognized in the UN Charter.[121] Applicable principles of international law, including humanity, necessity, proportionality, and distinction, must be considered.[122] States should

[113] Tikk-Ringas, International Cyber Norms **7**
[114] Tsagourias and Buchan, Research Handbook,
[115] *Ibid* 601
[116] *Ibid* 609
[117] UNGA Doc. A/70/174 (22 Jul. 2015)
[118] *Ibid* 556
[119] *Ibid* 562
[120] Fang, Cyberspace Sovereignty, 420
[121] UNGA Doc. A/70/174 (22 Jul. 2015)
[122] *Ibid* para 28 (d)

not use proxies to commit internationally wrongful acts using ICTs and should endeavour to ensure that their respective territories are not used by non-state actors to commit such acts.

ii. UN Security Council (UNSC)

The UNSC remains the only UN body with the authority to create binding international law.[123] While its resolutions have generally not been directed at the broader spectrum of cybersecurity issues, the UNSC has been active in addressing cybersecurity concerns related to terrorism. Following the 11 September 2001 terrorist attacks, the UNSC adopted Resolution 1373 (2001), establishing the Counter-Terrorism Committee (CTC).[124] The CTC has since engaged in efforts to address the abuse of information and communications technologies (ICTs) by terrorists and terrorist organizations. This has included assessing Member States' implementation of counter-terrorism obligations under Resolutions 1373 (2001),[125] 1624 (2005),[126] and 2178 (2014)[127] in relation to ICT, as well as convening meetings on cyber-related terrorism concerns. Notably, in 2015 the CTC organized a meeting on preventing terrorists from exploiting the internet for recruitment and incitement to violence,[128] and in 2016 it addressed broader challenges in preventing the exploitation of ICTs for terrorist purposes.[129]

The Counter-Terrorism Committee Executive Directorate (CTED) has played an important advisory and operational role for the CTC. It has coordinated

[123] Devon Whittle, "The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action," *European Journal of International Law* 26, no. 3 (August 1, 2015): 671–98, https://doi.org/10.1093/ejil/chv042.
[124] UNSC Res. 1373, UN Doc. S/RES/1373 (28 Sep. 2001) para. 6
[125] *Ibid* para. 3 (a-g)
[126] UNSC Res. 1624, UN Doc. S/RES/1624 (14 Sept 2005) para 1-5
[127] UNSC Res. 2178, UN Doc. S/RES/2178 (24 Sept 2014) para 5
[128] Counter-Terrorism Committee Executive Directorate, "Technical Meeting of the Counter-Terrorism Committee Executive Directorate on 'Preventing Terrorists from Exploiting the Internet and Social Media to Recruit Terrorists and Incite Terrorist Acts, While Respecting Human Rights and Fundamental Freedoms' Final Agenda Opening Session," 2015, https://doi.org/10.00-10.15.
[129] Counter Terrorism Committee, "Concept Note Special Meeting of the Counter-Terrorism Committee with Member States and Relevant International and Regional Organisations, Civil Society and the Private Sector on 'Preventing the Exploitation of Information and Communications Technologies for Terrorist Purposes, While Respecting Human Rights and Fundamental Freedoms,'" 2016.

events, launched initiatives in cooperation with the private sector and civil society, such as its project with the Swiss Foundation ICT4Peace, and sought to identify good practices in industry responses to the use of new technologies for terrorist purposes. Coordination has also been facilitated by the Counter-Terrorism Implementation Task Force, created in 2005 to implement Resolution 1373 (2001).[130] Among its working groups, the one on "Countering the Use of the Internet for Terrorist Purposes" has become increasingly relevant to the broader cybersecurity debate. Its objectives have included identifying relevant stakeholders, mapping terrorist use of the internet, quantifying associated threats, and evaluating the UN's potential role in mitigation.[131]

The group's first report in 2009 found no immediate terrorist threat that warranted UN counter-terrorism action, but suggested ways for the UN to contribute, such as facilitating best practice sharing, compiling research databases, promoting counter-extremism narratives, and considering international legal measures to restrict terrorist content online.[132] Subsequent phases shifted toward addressing legal and technical challenges in countering terrorist use of the internet. The 2011 report advocated harmonization of national laws through regional and international instruments such as the Budapest Convention on Cybercrime and the Convention against Transnational Organized Crime.[133] Later work focused on counter-narratives and the role of credible messengers, recognizing the UN's unique role in facilitating global discussions on such measures.[134]

---

[130] Counter Terrorism Implementation Task Force, "COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF," n.d., www.ewi.info. https://www.ipinst.org/wp-content/uploads/2012/06/pdfs_terrorism-directory_3-CTITF-AlQaida.pdf

[131] *Ibid*

[132] UN Counter-terrorism Implementation Task Force, 'Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes' (February 2009) https://www.statewatch.org/media/documents/news/2013/jul/ctitf-internet-wg-2009-report.pdf

[133] UN Counter-terrorism Implementation Task Force, 'Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects' (May 2011) https://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

[134] For the conference summary and follow-up/recommendations see UN Counter-terrorism Implementation Task Force, 'CTITF Working Group on Use of the Internet for Terrorist Purposes Riyadh Conference on Use of the Internet to Counter the Appeal of Extremist Violence' (January 2011)

The UNSC has also addressed cybersecurity in its wider peace and security mandate through Arria-formula meetings. In November 2016, Spain and Senegal co-convened a meeting on "Cybersecurity and International Peace and Security," which explored challenges such as the speed and anonymity of cyberattacks, difficulties of attribution, and the importance of national strategies, information sharing, and cross-sectoral cooperation.[135] In March 2017, Ukraine organized a meeting on "Hybrid Wars as a Threat to International Peace and Security," which examined the intersection of cyber threats, political interference, and propaganda, defining hybrid warfare as operations designed to remain below thresholds that would trigger a military response.[136]

More recently, UNSC attention to cybersecurity has been shaped by its rotating membership. Estonia's successful campaign for a 2020–21 term, built in part on its strong interest in cyber issues has brought increased focus on cybersecurity to the Council's deliberations, suggesting that state-level priorities can influence the Council's engagement with emerging security domains.

iii. UN Secretary General

The United Nations Secretary-General (UNSG) has played a pivotal role in elevating cyberspace governance within the broader UN agenda.[137] In July 2018, António Guterres recognized the growing urgency of coordinated, cross-sectoral cooperation to address the economic, social, ethical, and legal dimensions of digital technologies.[138] To this end, he established a High-Level Panel on Digital Cooperation tasked with assessing the multi-faceted impacts of digital transformation, with the dual aim of leveraging its benefits while mitigating associated risks. The Panel's report underscored the need for

[135] Security Council Report, 'In Hindsight: The Security Council and Cyber Threats' (23 December 2019) https://www.securitycouncilreport.org/monthly-forecast/2020 -01/the-security-council-and-cyber-threats.php
[136] Henderson, The United Nations, 537
[137] Sarah Collins Fattedad et al., "Towards A Global Digital Governance Architecture: Mapping Pathways for Cooperation and Inclusion 2," n.d.
[138] *Ibid* 10

international collaboration and a renewed global commitment to a safe, inclusive, and equitable digital future, framing its recommendations as "building blocks of an inclusive and interdependent digital world, with a fit-for-purpose new governance architecture".[139]

This vision was operationalized through the Secretary-General's Roadmap for Digital Cooperation, which outlines a multi-year, multi-stakeholder, action-oriented strategy to address global interconnectivity, digital equity, and cyber resilience.[140] Among its priorities are achieving universal digital connectivity by 2030, promoting digital public goods to reduce global inequalities, and developing a framework for digital trust and security aligned with the Sustainable Development Goals (SDGs). The roadmap also emphasizes the importance of embedding digital rights within the broader human rights framework, reflecting the recognition that cyberspace governance is inseparable from international human rights law.

To implement the Roadmap, the Office of the Secretary-General's Envoy on Technology was created as a dedicated institutional mechanism to coordinate initiatives, engage with diverse stakeholders; including Member States, the technology sector, private companies, and civil society, and advance negotiations towards a Global Digital Compact as proposed in the Common Agenda.[141] This institutionalization reflects an acknowledgment that governance of digital space requires not only normative frameworks but also practical coordination platforms capable of bridging fragmented regulatory domains.

The UNSG's approach positions the UN as a convener and facilitator of global digital governance, balancing the imperatives of security and access while promoting a rights-based, multi-stakeholder model. In theoretical terms, this aligns with the broader regime complex literature by illustrating how leadership at the

[139] *Ibid*
[140] United Nations. (2020). Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation: Report of the Secretary-General (A/74/821). United Nations. https://daccess-ods.un.org/tmp/9803106.18877411.html
[141] Office of the Secretary-General's Envoy on Technology. https://www.un.org/techenvoy/

intergovernmental level can generate linkages between existing regimes, such as human rights, development, trade, and security, through agenda-setting and institutional innovation. This approach also reinforces the concept of regime orchestration, where a central actor does not directly legislate but coordinates a diverse network of institutions and stakeholders towards shared objectives.

iv. UN Economic and Social Council

The United Nations Economic and Social Council (ECOSOC) functions as the UN's principal body for coordination, policy review, dialogue, and recommendations on economic, social, and environmental issues, and has also engaged with matters relating to cyber-security. While its interest in the topic has been broad (hosting, for example, a 2010 briefing on "Cyber Security: Emerging Threats and Challenges" and a 2011 special event on "Cybersecurity and Development")[142] its most substantial cyber-related work has taken place within its functional commissions, particularly the Commission on Crime Prevention and Criminal Justice (CCPCJ) and, to a lesser extent, the Commission on Narcotic Drugs.

The CCPCJ, established in 1992 as the UN's principal policymaking body in the field of crime prevention and criminal justice,[143] began addressing computer-related crime in the late 1990s. In 1998, it requested that the UN General Assembly (UNGA) include a workshop on "crimes related to the computer network" in the Tenth Crime Congress.[144] This process culminated in the 2000 Vienna Declaration on Crime and Justice, in which Member States committed to developing policy recommendations to prevent and control computer-related crime, and invited the CCPCJ to take forward work in this area.[145] By 2001, the Commission had adopted a plan of action that included

[142] 2010 ECOSOC General segment briefing on "Cyber security: emerging threats and challenges", 'Special Event on Cybersecurity and Development – Informal summary' (9 December 2011) http://www.un.org/en/ecosoc/cybersecurity/summary.pdf.
[143] ECOSOC Res 1992/1 (6 February 1992)
[144] ECOSOC E/1998/30-E/CN.15/1998/11
[145] Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, UNGA Res 55/59 (4 December 2000) para 18

measures against high-technology and computer-related crime,[146] although at that stage the focus remained on "computer crime" rather than the broader concept of "cybercrime".[147] The term "cyber" first appeared in the CCPCJ's 2002 report,[148] with calls for a global cybercrime convention emerging by 2004.[149]

From 2010 onwards, cybercrime became a recurring and prominent theme in CCPCJ reports, with discussions covering child exploitation, economic fraud, identity-related crime, and capacity-building for law enforcement. Notably, cyber-related issues became embedded within a wider spectrum of criminal justice concerns, such as trafficking of cultural property and organized crime.[150] In line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges, ECOSOC and the UNGA mandated the CCPCJ to establish an open-ended intergovernmental expert group on cybercrime.[151] This expert group was tasked with conducting a comprehensive study of the problem, including national legislation, best practices, technical assistance, and options for strengthening national and international responses.

Since its first session in January 2011,[152] the expert group has evolved into an important forum for states, the private sector, and international organizations to exchange information and deliberate on policy. Its successive sessions have addressed legislation and frameworks, criminalization, law enforcement, electronic evidence, international cooperation, and prevention.[153] Debates have revealed divergences over whether a new global cybercrime instrument is necessary, reflecting broader tensions in international cyber governance

[146] ECOSOC E/2001/30/Rev.1-E/CN.15/2001/13/Rev.1
[147] Henderson, The United Nations, 608
[148] ECOSOC E/2002/30-E/CN.15/2002/14.
[149] ECOSOC E/2004/30–E/CN.15/2004/16.
[150] ECOSOC E/2014/30 E/CN.15/2014/20.
[151] ECOSOC Res 2010/18 (22 July 2010); UNGA Res 65/230 (21 December 2010) UN Doc A/ RES/65/230.
[152] The report on that meeting is contained in document UNODC, 'Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime held in Vienna from 17 to 21 January 2011' (31 March 2011) UN Doc UNODC/CCPCJ/ EG.4/2011/3
[153] Henderson, The United Nations, 609

between those advocating for treaty-based harmonization and those preferring non-binding, capacity-focused cooperation.

From a regime complex perspective, ECOSOC (through the CCPCJ) plays a distinct role in linking cyber governance to the broader crime prevention and criminal justice regime. It exemplifies how thematic specialization can integrate cyber governance concerns into existing institutional mandates, while also highlighting fragmentation risks when divergent policy preferences emerge over the scope and form of international instruments. The open-ended expert group's deliberations also demonstrate the "incremental layering" characteristic of regime complexes, where issue-specific governance evolves within existing institutional structures rather than through entirely new treaty frameworks.

v. Subsidiary Organs and Specialized Agencies of the UN

1. International Telecommunications Union (ITU)

The ITU; UN's specialized agency for information and communication technologies (ICTs), is the principal UN body tasked with the practical and technical dimensions of cyber-security. Although it predates the UN, the ITU became a specialized agency under Article 57 of the UN Charter in 1945,[154] giving it a formal place within the UN system. Its mandate extends beyond serving as a discussion forum for cyber-security issues, encompassing the development of specific initiatives and the establishment of international technical standards that shape the global ICT environment.

A pivotal moment in the ITU's engagement with cyber-security came in May 2007, when the ITU Secretary-General launched the Global Cyber-Security Agenda (GCA) as an "international framework for cyber-security".[155] Central to this initiative was the creation of a high-level group of experts on cyber-security, which met three times between

[154] United Nations, Charter of the United Nations, 26 June 1945, 1 UNTS XVI, art. 57.
[155] Henderson, The United Nations, 609

2007 and 2008 before publishing the Global Strategic Report in 2008.[156] The report identified five priority areas for action: (1) legal measures, (2) technical and procedural measures, (3) organizational measures, (4) capacity-building, and (5) international cooperation.

The expert group's recommendations to the ITU illustrate its dual role in norm promotion and capacity-building. Key proposals included the development of model legislation for Member States, accompanied by a cybercrime legislation toolkit containing sample provisions and explanatory commentary to facilitate harmonization of national laws; the creation of a Cyber-security Readiness Index; a framework for protecting national critical infrastructure; and a conceptual framework for fostering a global "culture of cyber-security."

The ITU Secretary-General has maintained a high-profile role in advancing this agenda. At the 2010 World Telecom Development Conference in Hyderabad, he proposed a "no first attack vow" for cyberspace and urged states to commit to not harbouring cyberterrorists or attackers without punishment.[157] He also drafted five principles of "cyber-peace",[158] signalling an attempt to expand the ITU's role from technical standardization into the normative and ethical dimensions of cyber governance.

The ITU has also spearheaded initiatives in specific sub-areas such as child online safety. In 2014, in partnership with UNICEF and the Child Online Protection Initiative, the ITU released updated guidelines aimed at strengthening online protections for children.[159] These efforts have been noted as a rare point of consensus among states, where shared

[156] Global Cybersecurity Agenda (GCA)' (ITU) https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf

[157] Henning Weggener, "Cyber Peace," in *The Quest for Cyber Peace* (International Telecommunications Union, 2011), 77–86.

[158] *Ibid* 78

[159] COP Guidelines' (ITU) http://www.itu.int/en/cop/Pages/guidelines.aspx.

values and trust-building can generate positive spillover effects for broader cyber-security cooperation.[160]

The ITU's current cybersecurity programme is framed within Objective 2 of the Buenos Aires Action Plan adopted at the 2017 World Telecommunication Development Conference.[161] This programme offers Member States access to tools and knowledge for strengthening national cybersecurity capacities, with the stated goal of enhancing security, building confidence, and fostering trust in the use of ICTs, thereby "making the digital realm more safe and secure for everyone".[162]

2. United Nations Institute for Disarmament Research (UNIDIR)

UNIDIR is a voluntarily funded autonomous institute within the UN system that focuses on generating ideas and promoting action on disarmament and security. It was among the first UN entities to engage with the issue of cyber-security, positioning itself early as a knowledge and capacity-building hub within the emerging cyber governance landscape.[163]

UNIDIR's cyber-related work centers on policy-focused capacity-building at the national, regional, and multilateral levels, complemented by research and analytical outputs that aim to inform both UN processes and broader policy debates. Its early involvement in the field is marked by the hosting of two notable conferences linked to the discussions of the UN General Assembly's First Committee. In 1999, with funding from the United Nations Department for Disarmament Affairs, UNIDIR convened a two-day meeting on "Developments in the field of information and telecommunications in the context of international security"[164]echoing the title of a resolution introduced by Russia the

[160] Henderson, The United Nations, 611
[161] Final Report, World Telecommunication Development Conference, Buenos Aires (9-20 October 2017) https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.
[162] Henderson, The United Nations, 613
[163] See 'Cyber' (United Nations Institute for Disarmament Research) http://www.unidir.org/est-cyber.
[164] Henderson, The United Nations, 609

year before. This early forum revealed stark divergences in states' primary concerns regarding ICTs, highlighting from the outset the difficulty of forging consensus on cyber norms.

Nearly a decade later, in 2008, Russia funded a second major UNIDIR conference on "Information and Communication Technologies and International Security" with the explicit objective of examining both existing and potential threats from the hostile use of ICTs, as well as the unique challenges such technologies pose to international security, and possible responses.[165]

Today, UNIDIR continues to operate at the intersection of policy development and technical awareness-raising. It serves as a consultant to the UN Groups of Governmental Experts (GGEs) and maintains the Cyber Policy Portal, an interactive online reference tool mapping national, regional, and multilateral cyber policies worldwide. This tool enhances transparency and enables cross-comparison of governance approaches, a function that directly addresses fragmentation within the cyber regime complex. In addition, UNIDIR hosts annual Cyber Stability Conferences, which act as a platform for cross-sectoral and cross-regional dialogue. For example, the June 2019 conference brought together experts from the UN, regional organizations, the private sector, the technical community, and academia to assess the state of global cybersecurity policy. Discussions focused on the outputs of the UN GGE and Open-Ended Working Group (OEWG), the development and reinforcement of cyber norms, and strategies to counter threats from the malicious use of ICTs.

3. UNODC

The United Nations Office on Drugs and Crime (UNODC), while not originally mandated to address cyber-security, became formally engaged in the field in 2008 when the Third Committee of the UN

[165] *Ibid* 612

General Assembly requested that it provide technical assistance on "cybercrime".[166] UNODC leverages its core expertise in criminal justice systems to deliver capacity-building, prevention and awareness programmes, promote international cooperation, and conduct data collection, research, and analysis on cybercrime.

The agency's involvement in cyber issues expanded in 2011, when Member States (through the 20th session of the Commission on Crime Prevention and Criminal Justice (CCPCJ)) formally tasked UNODC with addressing the use of the Internet for terrorist purposes, a matter first raised at the CCPCJ's 19th session.[167] In response, UNODC's Terrorism Prevention Unit contributed to the 2012 *Counter-Terrorism Implementation Task Force (CTITF)* publication for law enforcement investigators and criminal justice officers, offering practical guidance for cases involving online terrorist activities.

A central component of UNODC's cyber-related work is its leadership role in the Global Programme on Cybercrime, initiated by the CCPCJ.[168] Hosted within the Organized Crime Branch of UNODC's Division for Treaty Affairs, the programme supports Member States in strengthening national and international legal responses to cybercrime. Activities span legislative assistance, law enforcement training, and facilitation of cross-border cooperation, reflecting UNODC's operational focus on implementation rather than norm creation.

An important tool under this programme is the Cybercrime Repository, a database of cybercrime laws and lessons learned designed to aid in the continuous assessment of states' needs and capabilities in criminal justice responses. The repository also serves as a coordination mechanism for technical assistance, allowing for the identification of legislative gaps, good practices, and opportunities for harmonization.

---

[166] *Ibid*

[167] UNODC, 'The use of the internet for terrorist purposes' (UN, 2012) https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[168] Henderson, The United Nations, 612

From a regime complex perspective, UNODC operates as both an implementer and capacity-builder within the international cyber governance system. While it does not set binding global norms, its work shapes the operational and legal capabilities of states, bridging the gap between policy frameworks developed in other UN fora (e.g., UNGA, UNODIR, ITU) and their practical enforcement at the national level. This positioning allows UNODC to exert indirect normative influence by embedding its technical assistance and training within the broader UN discourse on cybercrime and cyber-security.

b. European Union (EU)[169]

The EU occupies a distinctive position in the global cyber-regime complex: it wields binding legislative authority while also coordinating national action in areas where explicit Union competences are thin. Although "cybersecurity" is not expressly listed in the EU Treaties, successive policy moves; culminating in the 2013 Cybersecurity Strategy (updated in 2017) and the 2015 Council conclusions on cyber-diplomacy, have pushed the issue high on the EU agenda.[170] The Union's first binding measure was the 2016 NIS Directive, followed by the 2019 Cybersecurity Act, which strengthened the mandate of ENISA (relabelled the European Union Agency for Cybersecurity) and introduced EU-wide cybersecurity certification.[171] The Act's unusually long preamble reflects the EU's sensitivity about its legal basis in this field, while the 2020 Security Union Strategy further extends the policy architecture (including the planned Joint Cyber Unit).[172]

[169] Ramses A Wessel, "European Law and Cyberspace," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar Publishing, 2021), 491–408, https://doi.org/10.4337/9781789904253.
[170] European Commission, 'State of the Union 2017 – Cyber-security: Commission scales up EU's response to cyber-attacks', Press Release (Brussels, 19 September 2017).
[171] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1)., Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ EU L 151/15, 7.6.2019.
[172] EU Security Union Strategy, COM(2020) 605 final, Brussels, 24.7.2020; https://ec.europa.eu/info/ sites/info/files/ communication-eu-security-union-strategy .pdf.

Substantively, the EU frames cybersecurity around resilience, critical infrastructure protection, cybercrime control, cyberdefence development, industrial/technical capacity, and cyber-diplomacy; an approach justified by rising attacks on states and critical infrastructure and the inherently cross-border character of cyber risks.[173] "Resilience" itself is a leitmotif of the 2016 Global Strategy, but the Union's role often remains to coordinate, support, or assist Member States given the lack of explicit competences; the 2019 Cybersecurity Act confirms that public security, defence, national security, and criminal law remain national domains.[174] Where no express power exists, the EU has either repurposed other legal bases or relied on soft-law and coordination, a piecemeal path that complicates task allocation and blurs the scope of "cybersecurity" as a legal concept.[175] As Fuster and Jasmontaite note, EU actors use divergent definitions of cybersecurity, raising questions about the coherence and consistency of existing and proposed legislation.[176]

A pivotal vector for EU action is the Digital Single Market (DSM), adopted in 2015 with 16 initiatives delivered by early 2017.[177] Here, cybersecurity is cast as an economic enabler; a precondition for trust in connected technologies and e-commerce.[178] The Commission anchored the NIS Directive in Article 114 TFEU (internal market harmonisation), requiring transposition by 9 May 2018, and argued that security of network and information systems is essential to the functioning of the internal market.[179] In theoretical terms, this is a Law–Market strategy: internal-market

[173] Wessel, European Law and Cyberspace, 492
[174] Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy, 2016; https://europa.eu/globalstrategy/en.
[175] Krzysztof Feliks Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent," *Contemporary Security Policy* 35, no. 3 (September 2, 2014): 468–86, https://doi.org/10.1080/13523260.2014.959261.
[176] Wessel, European Law and Cyberspace, 494
[177] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 final.
[178] Wessel, European Law and Cyberspace, 501
[179] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concern- ing measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, 1 ('NIS Directive'). See also Johan David Michels and Ian Walden, 'Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?' (2020), European Law Review,; Dimitra Markopoulou, Vagelis Papakonstantinou, Paul de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) Computer Law & Security Review 105336.

competences harmonise security baselines across the Union, while Lessig's Architecture enters through certification, interoperability, and technical standards.

In cybercrime, the EU's authority is clearer. The 2005 Framework Decision on attacks against information systems; one of the Union's earliest cybersecurity-related instruments was replaced by the 2013 Cybercrime Directive grounded in Article 83(1) TFEU (Area of Freedom, Security and Justice).[180] The Directive sets minimum rules on offences and sanctions and standardises core definitions, while adjacent measures—on child sexual exploitation online, ePrivacy, and fraud/counterfeiting—reinforce the enforcement toolkit.[181] More recently, e-evidence proposals (2018–2019) and an updated Directive on non-cash means of payment seek to ease cross-border investigations and modernise cooperation.[182] This cluster blends Law (harmonised offences, sanctions) with Norms (common procedures, cooperation practices) and operationalises them via Architecture (data access and preservation mechanisms).

Through cyber-diplomacy, the EU leverages CFSP competences: Article 24(1) TEU covering all areas of foreign policy and questions of the Union's security, to respond collectively to malicious cyber activities.[183] The cyber-diplomacy toolbox articulates non-military instruments for mitigation, prevention, and stability (85, 86). In 2019, the Council adopted a Decision and connected Regulation establishing a cyber sanctions regime applicable to significant cyber-attacks against the Union or its Member States, including attempted attacks.[184] Member States must bar listed persons

[180] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[181] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, 8. This Directive replaced the 2005 EU Framework Decision on Attacks against Information Systems., Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 OJ L 337, 18.12.2009, 11., Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, OJ L 149, 2.6.2001, 1

[182] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM/2018/225 final - 2018/0108 (COD); Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final - 2018/0107 (COD)., Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA PE/89/2018/REV/3.

[183] Rames A Wessel and Joris Larik, 'The EU as a Global Actor' in Ramses A Wessel and Joris Larik (eds), EU External Relations Law: Text, Cases and Materials (Hart 2020) 1–28.

[184] Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I, 17.5.2019; and Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 129I,

from entry/transit and freeze funds of responsible actors and those supporting or associated with them; the Regulation makes these rules binding Union-wide.[185] The first listings (30 July 2020) targeted Russian, Chinese, and North Korean actors linked to major incidents, signalling the EU's willingness to translate cyber norms into coercive foreign-policy tools.[186]

By contrast, cyberdefence remains less developed. As noted by Odermatt, there is no comprehensive EU approach to cyberdefence, despite claims that "the next war will begin in cyberspace".[187] The EU Cyber Defence Policy Framework (2014, updated 2018) integrates cyberspace as the fifth operational domain and connects cyberdefence to the CSDP, often in cooperation with the European Defence Agency.[188] Under PESCO, projects such as the Cyber Threats and Incident Response Information Sharing Platform and Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity indicate gradual capability-building.[189] On collective reaction, the solidarity clause (Article 222 TFEU) can encompass aspects of cyber-incidents, and the European Parliament has explicitly included cybersecurity within its scope.[190] The mutual defence clause (Article 42(7) TEU) could, in principle, be invoked where cyber operations amount to "armed aggression," though international-law thresholds complicate automatic applicability.[191] In practice, activation is likely to turn more on political choice than on doctrinal certainty.

Taken together, the EU exhibits a Law–Architecture core (binding rules plus technical implementation), supplemented by Norms (strategic guidance, cooperation practices) and Market leverage (DSM framing). In regime-complex terms, the Union generates rule overlaps (e.g., internal-market law intersecting with security and

17.5.2019; updated in 2020 by Council Decision (CFSP) 2020/651 of 14 May 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 153, 15.5.2020.

[185] Wessel, European Law and Cyberspace, 504

[186] Council Decision (CFSP) 2020/1127 of 30 July 2020, OJ 246/12, 30.7.2020.

[187] General Keith B Alexander, upon accepting the post to lead the first United States Cyber-Command (USCYBERCOM). Quoted by Rex Hughes, 'A Treaty for Cyberspace' (2010) 86 International Affairs 523.

[188] Cyber Defence Policy Framework; https://www.consilium.europa.eu/media/37024/st14413-en18.pdf.

[189] https://pesco.europa.eu/. See also Lorenzo Pupillo, Melissa K. Griffith, Steven Blockmans, Andrea Renda, 'Strengthening the EU's Cyber Defence Capabilities' (November 2018) CEPS Report.

[190] European Parliament resolution of 22 November 2012 on the EU's mutual defence and solidarity clauses: political and operational dimensions (2012/2223(INI)) para 20.

[191] Wessel, European Law and Cyberspace, 506

foreign-policy instruments), jurisdictional overlaps (EU vs national competences), and institutional overlaps (engagement with UN processes, coordination with NATO/FAO/Council of Europe). This mix enables the EU to project standards beyond its borders but can also produce fragmentation where EU rules diverge from global norms. Through Lessig's lens, the EU's distinctive contribution is to codify cyber norms into hard law and to embed compliance in technical architecture, thereby shifting the overall constraint profile within the international cyber-regime complex.

c. Association of Southeast Asian Nation (ASEAN)

Cyber infrastructure is global to economy. Information and technology industry is now largely Pacific-based with Asian countries, US, and India creating most digital products. Development of global institutions, challenged by new economic power have shifted powers from Europe due the international security environment; particularly creating conflict and competition in cyberspace.[192] The Cyber powers of Asia-Pacific are US, China, Russia, Taiwan, North and South Korea, and Australia.

In Southeast Asia, the ten ASEAN Member States[193] have a combined population of around 600 million, approximately 162 millions of whom were Internet users in 2013, an increase from 81 million in 2009,28 and this figure is set to increase as ICT infrastructure becomes more widespread and the ICTs become more accessible. Within the ASEAN region, more attention and resources are being devoted to combating prevailing types of cybercrimes such as telecommunications fraud, hacking, identity theft, and e-mail or credit card fraud. ASEAN Member States do have different levels of technological advancements and knowledge as well as national law enforcement capabilities in tackling these crimes. Although many ASEAN Member States have established Computer Emergency Response Teams (CERTs) and national authorities on cyber security, there is still much to be done.[194]

[192] James Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia," n.d., https://www.interpol.int/Public/ICPO/PressReleases/PR2010/PR052.asp.
[193] Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam.
[194] ITU, ITU World Telecommunication/ICT Indicators database 2014, Percentage of Individuals Using the Internet, cited in The Internet Society, Unleashing the Potential of the Internet for ASEAN Economies (Washington, DC: Internet Society, 2015), 10.

In the wider context of the ASEAN Regional Forum (ARF),[195] on 12 July 2012 the 27 Members of the ARF issued the Statement on Cooperation in Ensuring Cyber Security expressing their aspiration to further intensify regional cooperation on security in the use of the ICTs including through strategies to address emerging cyber threats "consistent with international law and its basic principles" and "dialogue on confidence-building, stability, and risk reduction measures to address the implications of ARF participants' use of the ICTs, including exchange of views on the potential use of ICTs in conflict". The ARF also launched a Work Plan on Cyber Security, to be drafted by Australia, Malaysia, and Russia, focusing on practical cooperation on confidence-building measures (CBMs) and transparency.[196]

Regional cooperation is needed to support market interdependence, as well as regional economic and social growth. This supports Asian countries' digital strategies and digital economy.[197] Political willingness is the major factor for Asian countries. Other difficulties to find common ground of state behaviour in cyberspace; state competition and self-interest, intensifying major power rivalry, rising nationalism, challenges to the rule of law, and human rights obligations. Another challenge to note is different conception of world order and conceptual understandings of cybersecurity and information security, including disruptive state behaviour in multilateral cyber efforts. States are more willing to engage in cyber-enabled influence operations and low-level activity below the threshold of armed conflict to bring about change in the national security architecture.

Countries across Asia have been actively engaged in shaping the global agenda for cyber stability, demonstrating a collective commitment to addressing the evolving challenges of cyberspace governance. Brunei and Singapore have provided their national perspectives to the United Nations Office for Disarmament Affairs

[195] The ARF has 27 Members; namely, the 10 ASEAN Member States plus Australia, Bangladesh, Canada, China, European Union, India, Japan, Democratic People's Republic of Korea, Republic of Korea, Mongolia, New Zealand, Pakistan, Papua New Guinea, Russian Federation, Sri Lanka, Timor Leste, and United States.

[196] Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, vol. 32 (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-54657-5.

[197] Caitríona Heinl, "Asia Pacific Contributions to International Cyber Stability," n.d., https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace,.

(UNODA),[198] offering valuable insights into the implementation of norms in cyberspace. Meanwhile, Malaysia has played a proactive role as a member of two Groups of Governmental Experts (GGEs),[199] contributing to international discussions and policymaking on cybersecurity issues. Japan, the United States, Australia, and China have emerged as key players in the international arena, demonstrating their commitment to cybersecurity through active engagement in various forums and initiatives. Indonesia and Korea have also been active participants in former GGEs, highlighting their dedication to shaping norms and confidence-building measures in cyberspace.[200] Singapore has taken a regional approach by launching a cyber capacity-building programme aimed at enhancing cybersecurity in the Asia-Pacific region and supporting the implementation of norms and confidence-building measures. Additionally, India has been actively involved in GGEs and has served as a co-chair of the Global Forum on Cyber Expertise (GFCE), showcasing its leadership and commitment to international cooperation on cybersecurity issues.[201] Overall, these collective efforts underscore the importance of collaboration and multilateral engagement in addressing cyber threats and promoting stability in cyberspace. By participating in international forums, initiatives, and capacity-building programmes, Asian countries are contributing to the development of norms, confidence-building measures, and cooperative frameworks essential for enhancing cybersecurity on a regional and global scale.

Nevertheless, regional development and digital divide determine the cyber maturity that each Asian state has. The uneven levels of capacity could also affect the consensus

---

[198] *See* BRUNEI DARUSSALAM'S VIEWS ON THE UNITED NATIONS GENERAL ASSEMBLY RESOLUTION A/RES/78/23 – 'Relationship between disarmament and development' https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_(2024)/78-23-Brunei-Darussalam-EN.pdf, and Statement by Ms Berenice Low, First Secretary (Political), Permanent Mission of Singapore to the United Nations at the 2024 Session Of The Disarmament Commission, 1 April 2024, https://docs-library.unoda.org/United_Nations_Disarmament_Commission_-_(2024)/singapore_en.pdf

[199] Ms. Shariffah Rashidah binti Syed Othman, "Statement by Ms. Shariffah Rashidah binti Syed Othman, Delegate, Permanent Mission of Malaysia, on 'Existing and Potential Threats in the Sphere of Information Security, inter alia, Data Security, and Possible Cooperative Measures to Prevent and Counter such Threats,' at the Second Substantive Session of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025, New York, 29 March 2022," UN e-statements, March 29, 2022, accessed [date], https://estatements.unmeetings.org/estatements/12.1255/20220330/zQAu2Wo0dGU9/mUJjhUItMh1p_en.pdf.

[200] Monica Nila Sari, "ASEAN Regional Effort on Cybersecurity and Its Effectiveness," *Keio SFC Journal* 23, no. 1 (2023): 26–42, https://docs.broadcom.com/doc/istr-22-2017-en.

[201] *Ibid*

required for future progress within regional institutional mechanisms such as ASEAN, thus affecting its collective ability to inform the global cyber norms discussion. Varying understanding of cybersecurity and what they perceive to constitute a cyber threat will continue to shape their domestic priorities (security interests also vary widely between countries in the region). How can capacity building be conducted where there are such different views and approaches to internet sovereignty and information control.[202]

One of the ways are through bilateral and like-minded efforts. For example, and MOU between Singapore and Thailand. But this cold challenge the efforts towards achieving a 'global norm'? In terms of capacity building, many states in the region are still challenged by the speed of technological changes, they often lack technical capacity and gaps in the law persist, which is hindering international cooperation and exchange of good practice. The problem with Asian States is that while they may not agree on the global standard set by majority of western institutions, at the same time they cannot provide a solution or propose way out that is suitable for themselves.

3. Regulation of Cyberspace

The conceptual approach to regulating cyberspace involves two key perspectives: governance and regulation. Governance, viewed from a sociological standpoint, encompasses various forms of collective action aimed at addressing public concerns. On the other hand, regulation extends beyond traditional command-and-control methods, instead emphasizing the creation and enforcement of rules (whether public or private) to manage specific aspects of cyberspace.[203]

Regulation both influences and is influenced by technology. Technological advancements reshape the methods and tools used for regulation, including determining who has the authority to regulate. Given the dynamic nature of internet usage and the global reach of the World Wide Web (WWW), there is no singular regulatory framework for governing cyberspace. Instead, there exists a varied landscape of regulations, comprising legal statutes, technical standards, international agreements, informal codes of conduct, and other mechanisms. This results in a diverse array of regulatory elements that may complement or

[202] *Ibid*
[203] Feick and Werle, Regulation of Cyberspace, 1

conflict with one another, including formal laws, voluntary standards, and informal norms of behaviour.[204]

To streamline internet regulation, it involves dissecting the internet's multitude of services and applications into manageable components and assigning them to different layers of the network's protocol. This approach ensures precision in regulation by matching specific regulatory measures to specific layers. The internet is typically delineated into layers, with variations in classification. Benkler[205] identifies three layers: the physical layer, code layer, and content layer, while Zittrain[206] identifies the physical layer, protocol layer, and application layer. Generally, these layers are categorized as technical (lower) and social (upper). Feick expands on this by distinguishing between the technical layer, which encompasses infrastructure and fundamental protocols like TCP/IP and browsers, and the content layer, which involves the application and utilization of software for accessing, transmitting, and managing various types of content.[207]

a. Regulation of technical infrastructure

The internet can function as a decentralized global network because of components of compatibility, identification, and interconnectivity. Compatibility facilitates the smooth interoperation of networks in technical terms and is usually achieved through conformance to technical standards. Identification is accomplished by the assignment of unique addresses to all users or objects which inhabit the networks. Interconnectivity entails the commitment or obligation of providers, or operators of networks to link their networks to another in compliance with compatibility.[208]

i. Identification

The primary area of regulation at the infrastructure level primarily concerns identification and the domain name system (DNS). Assigning a unique address to each connected host is crucial for routing and transmitting data packets. The domain name system, visible in email and website addresses, is based on this addressing system. Unlike strings of numbers, names serve as human-friendly

[204] *Ibid* 1
[205] Benkler, The Wealth of Networks, 383
[206] Zittrain, The Future of the Internet and How to Stop It, 63
[207] Feick and Werle, Regulation of Cyberspace, 3
[208] *Ibid*

identifiers, enhancing the network's usability. Initially intended for coordination, the DNS, particularly names in the '.com' top-level domain, became valuable business assets used for branding. This shift transformed domain name allocation from coordination to resource allocation, potentially disadvantaging those seeking specific domain names, such as trademark owners, who find them already assigned to others, like competitors. The US government shifted control of number and name assignment, along with managerial duties, from IANA to ICANN due to escalating DNS issues. ICANN, a non-profit based in California since 1998, was established to be a globally inclusive body following principles of internationalization and privatization. Despite this, it has remained under US government oversight through contracts with the Department of Commerce, restricting influence from other governments. While the original aim was to reduce US dominance and empower various stakeholders, a hierarchical political element has persisted, with ICANN operating under the shadow of state influence. This dynamic raises questions about the necessity of such an arrangement. ICANN holds sole authority to develop and enforce rules within its jurisdiction, including authorizing new top-level domains like '.biz' and '.info', and managing root servers that maintain up-to-date information about domain names. Root servers are consulted when data packets cannot find their destination. ICANN also supervises organizations managing top-level domains (registries), such as '.uk' or '.jp', ensuring compliance with its terms. It has instituted a dispute resolution mechanism through approved providers, including the Uniform Domain Name Dispute Resolution Policy (UDRP), known for efficiently resolving domain name disputes at a low cost.[209]

ii. Compatibility

Private self-regulation on the technical layer of the Internet has a long history, primarily driven by the need to ensure compatibility in the decentralized structure of the Internet. The Internet Engineering Task Force (IETF), formed in 1986, has been a key player in developing technical standards for the

[209] *Ibid*

Internet, emphasizing a non-hierarchical, consensus-based approach. Similarly, the World Wide Web Consortium (W3C), founded in 1994, focuses on standards for Web components and applications. While these standards are voluntary, they carry an implicit expectation of compliance. However, due to network effects, they can attain quasi-mandatory status in industries like telecommunications and information technology. For example, the adoption of the IPv6 protocol suite, introduced by the IETF in 1998, faced challenges and delays due to diverging political and business interests. While governments like the US, Japan, and the EU supported IPv6 for various reasons, its worldwide adoption was hindered by differing strategies and concerns, highlighting the limitations of private self-regulation. Despite its consensus-based approach, the IETF lacked the formal legitimacy and resources to enforce global implementation. Furthermore, regulation by intergovernmental organizations like the International Telecommunications Union (ITU) faced similar challenges due to conflicting government stances.[210]

iii. Interconnectivity

The Internet operates with minimal regulatory oversight, particularly concerning network operators and service providers' interconnection. This decentralized structure facilitates voluntary agreements and commercial negotiations among providers. However, concerns persist regarding access disparities, termed the "digital divide," which is not only about user numbers but also about usage patterns and technological inequalities. Commercial interests have driven the development of specialized Internet services, leading to potential discrimination in access and pricing. The concept of "network neutrality" has emerged as a response to fears of Internet fragmentation and loss of openness. Proponents advocate for regulatory intervention to ensure equal access and prevent market abuses, while opponents argue that market competition can address these concerns without stifling innovation or content

[210] *Ibid*

diversity. This debate mirrors similar discussions in the telecommunications industry and raises questions about the future governance of the Internet.[211]

b. Regulation of content

Cyberspace, characterized by its intangible and borderless nature, poses a challenge to established national norms and legal frameworks. Unlike traditional telecommunications networks, its decentralized structure fosters widespread creativity and collaboration, making regulation difficult. As the internet continues to evolve into a global commercial platform, ensuring a secure and reliable online environment becomes paramount.[212]

Content regulation on the internet encompasses a wide range of issues, including but not limited to, combating child pornography, hate speech, and discrimination against minorities, while also promoting or restricting the free exchange of information. Additionally, it addresses concerns related to online conduct, such as electronic fraud, privacy violations, unsolicited content, and cyberattacks. This regulatory domain is diverse and involves various stakeholders, making it a complex policy area with far-reaching implications.

Regulating content usually starts on the national law level. This is due to the prior existence of national law at addressing commercial, civil or criminal action on the internet. If, however, the adjustment of existing rules to cyber environment is necessary or new legal regulations are required, slow political rule-making procedure often reduce their effectiveness.[213] However, national law would only extend within a country's borders. Once a user's action crosses the border and it becomes transnational, often a jurisdictional compromise takes place through a multilateral agreement.

Regulation of content within cyberspace doesn't exhibit anarchic openness and uncontrollability. Instead, it's governed by diverse national and international institutional setups along with a wide array of intervention mechanisms tailored to

[211] *Ibid*
[212] *Ibid*
[213] Shane Greenstein, "Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked so Well," *Innovation Policy and the Economy* 1 (January 2000): 151–86, https://doi.org/10.1086/ipe.1.25056144.

specific internet applications, influencing what's known as the content and social layer of the internet. Often, a blend of public authority and private actor responsibility is seen in hybrid arrangements. Regulatory tools vary from traditional governmental directives and control measures to hands-off approaches relying on self-protection. Between these extremes lie other methods such as 'soft' informational strategies, persuasion tactics, comparative assessments, procedural regulations, and overseeing self-regulatory practices.[214]

While Internet activities aren't entirely detached from territorial considerations, allowing territorial governments some influence over control, regulating activities that cross borders on the Internet proves challenging and at times impossible. This difficulty largely arises from differences in international legal systems and enforcement mechanisms. Additionally, technical capabilities to conceal or alter the identities of internet users further complicate efforts to track illegal or hostile actions.[215] International agreements aimed at aligning legal regulations are rare, typically limited in scope, and lack global reach. Only the European Union possesses supranational potential, offering a realistic opportunity for legal alignment, albeit EU efforts remain somewhat constrained.[216] However, achieving legal alignment always entails trade-offs, with some scholars contending that international regulatory conflicts are often preferable to attempts at harmonization, which may obscure irreconcilable national differences, creating merely the illusion of effective regulation.[217] These potential shortcomings in de facto regulation may fuel calls for self-regulatory solutions at the international level. Yet, securing international agreements among firms and associations proves no less challenging than intergovernmental treaties. Some affected firms may view such agreements as even more restrictive than intergovernmental regulation, as dominant global players might exploit their strong positions to shape the rules.

i. Privacy and data protection

[214] Feick and Werle, Regulation of Cyberspace, 12
[215] *Ibid*
[216] Fernando Mendez, "The European Union and Cybercrime: Insights from Comparative Federalism," *Journal of European Public Policy* 12, no. 3 (June 20, 2005): 509–27, https://doi.org/10.1080/13501760500091737.
[217] J Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence," *European Journal of International Law* 11, no. 1 (January 1, 2000): 135–48, https://doi.org/10.1093/ejil/11.1.135.

Data protection encompasses safeguarding against theft, misuse, and intentional or unintentional distortion by both public and private entities. The right to manage the dissemination of personal information and to understand who has access to it and under what legal basis is recognized as a fundamental human right in many liberal democracies. However, there is no universal consensus on privacy, as different countries balance the tension between privacy and other rights, such as freedom of speech, freedom of information, and collective security, in varying ways.[218] In the United States, for example, freedom of speech often takes precedence over privacy concerns, whereas in many European countries, privacy and data protection laws are more extensive. In authoritarian regimes like China, government priorities prioritize system security and social stability over individual privacy and freedom of speech. These differences stem from cultural, political, and legal legacies that shape policy decisions. Even within the European Union (EU), where harmonizing national legislation is a key goal, it took over two decades of political negotiations and lobbying to enact EU Directives and Regulations governing cyberspace governance in the mid-1990s. The complex relationship between the right to privacy and personal data protection raises the question of whether each is a distinct right or whether they are complementary. This is clear from the scholarly discussion surrounding the position of the Right to Private Life and the Right to Personal Data in the EU's Charter of Fundamental Rights.[219] Others argued that the right to data protection is an additional right to the right to privacy.[220] The EU's perception of the right to privacy and the right to personal data protection as distinct rights has changed. The GDPR and CJEU case law both emphasise this. National laws on data protection are frequently referred to as "privacy laws" in traditional data protection instruments of the OECD, for instance.[221] While "data protection by design" and "data protection

[218] Feick and Werle, Regulation of Cyberspace, 10
[219] Menno Mostert et al., "From Privacy to Data Protection in the EU: Implications for Big Data Health Research," *European Journal of Health Law* (Brill Nijhoff, 2017), https://doi.org/10.1163/15718093-12460346.
[220] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol. 16 (Cham: Springer International Publishing, 2014), https://doi.org/10.1007/978-3-319-05023-2.
[221] ECtHR, Khelili v. Switzerland, App no. 16188/07 (18 October 2011),

impact assessment" have replaced earlier "privacy-based" ideas. Mostert et al., have addressed the differential aspects between the right to privacy and data protection for the context of big data health research.[222] In order to understand the complexities of the two, it is perceived that individual rights were to be decoupled from privacy. While both rights guarantee individual rights, their scope and substance differ.[223] The right to data protection encompasses almost all types of personal data protection, regardless of whether the right to privacy is interfered.[224] The interference with the right to privacy is contingent on the nature and context of the particular processing. The right to privacy does not extend to the simple collection of personal information. Rather, it lies within the scope of the right to data protection because it constitutes protection of personal data.[225] Individual rights pertaining to the right to privacy are more context-dependent in nature. The link between the right to data protection and the right to privacy is when the collected data permit very precise conclusions to be drawn about the private lives of the person whose data has been retained, such as their habits of everyday life, permanent or temporary places of residence, daily or other movements, activities performed, social relationships, and the social environments.[226] The right to privacy does not assure a general right of access to personal data by the data subject.[227] While the right to data protection explicitly guarantees such a right of access, regardless of any interference with the right to privacy, the right to access is not affected by the right to privacy. However, there is a trend towards the ECtHR recognising a general right to data based on the right to privacy, which creates a difficulty in differentiating the substantive protection provided by both rights.[228] The right to data protection is a positive obligation, meaning that states are obligated to

[222] Mostert et al., From Privacy to Data Protection, 1
[223] *Ibid*
[224] J. Kokott and C. Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3, no. 4 (November 1, 2013): 222–28, https://doi.org/10.1093/idpl/ipt017.
[225] CJEU, Case C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294, para. 74 and 64
[226] CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238.
[227] ECtHR, Gaskin v. United Kingdom, App no. 10454/83 (7 July 1989)
[228] Mostert et al., From Privacy to Data Protection, 46

take steps to safeguard personal data. While the right to privacy is merely a negative obligation, authorities must refrain from arbitrarily invading the private affairs of individuals.[229] The right to data protection is more comprehensive and systematic than the right to privacy, which is more individualistic. The right to data protection is governed by explicit principles, objectives, and constraints. In addition to the technical aspect of data security protection, accountability of data processors is also required. Thus, the right to data protection transcends the notion of individuals asserting or enforcing their rights.[230]

ii. Intellectual property protection

The protection of intellectual property rights is crucial in cyberspace. The digitization of works of intellectual property has led to the creation of digital products which can travel over the networks. This has enabled intellectual property to migrate so efficiently to the Internet. This migration of intellectual property onto the Internet can be seen with respect to each species of rights (patents, software) but predominantly the migration is best visible in case of copyright and trademarks. From a socio-cultural standpoint, advancements in technology have sparked a clash of conflicting values, norms, and ideas regarding the concept of culture, cultural production, and cultural consumption. Despite efforts by most governments in developed countries to strengthen international legal intellectual property protections, file sharing continues to evolve in new forms. Concurrently, industries have intensified their efforts to implement protective technologies aimed at preventing unauthorized copying. However, this has only initiated an ongoing battle between technological advancements that facilitate bypassing copy protection and usage control, and innovations, such as digital rights management software, which allow industries to dictate the terms of digital product use. This unresolved conflict

[229] Bart Van Der Sloot, "Privacy as Human Flourishing Could a Shift towards Virtue Ethics Strengthen Privacy Protec-Tion in the Age of Big Data?," 2014, http://nbn-resolving.
[230] Mostert et al., From Privacy to Data Protection, 52

highlights that technological self-protection has its limitations when societal consensus is lacking.

iii. Social media platforms

Platform governance involves legal, political, and economic relationships shaping interactions among users, technology companies, governments, and other stakeholders, and is shifting away from self-regulation towards increased government intervention.[231] However, platform regulation is not following a predefined script but is shaped by local circumstances, politics, and concepts like data nationalism. The current state of platform regulation is messy and lacks guaranteed outcomes. Efforts such as the EU Digital Market Act, intended to promote competition, have faced resistance from big platforms like Apple and Google. While proponents of big tech support competition, they resist government regulatory oversight. Governments have benefited from platform complicity in exchange for a business-friendly regulatory environment, likening access to information to essential utilities like water and electricity, advocating for platforms to be regulated similarly. However, in the absence of global regulatory standards, developing countries struggle to negotiate or restrict platform activities. Platform regulation intersects with other aspects of digital regulation, with internet governance providing a broader framework. While internet governance tends towards specific legislation targeting crimes like money laundering and terrorism, it lacks a comprehensive regulatory strategy. Governance differs from regulation in its systematic rule-making approach, contrasting with regulation's establishment of legal boundaries and enforcement mechanisms. Regulation inevitably accompanies digital disruption and innovation, raising questions about what to prioritize for the public good and what to leave for market dynamism and innovation. A new consensus is emerging to shift self-regulation towards co-regulation, which entails sharing decision-making responsibilities between companies and government entities. In this model, governments play a role in

[231] Pradip Ninan Thomas, *Platform Regulation, Exemplars, Approaches, and Solutions* (Oxford University Press, 2023), https://doi.org/10.1093/oso/9780192887962.002.0004.

structuring self-regulation while allowing companies some autonomy in decision-making. Self-regulation grants technology companies a high degree of flexibility, enabling them to quickly intervene and remove harmful content without lengthy legislative processes. In the co-regulation approach, governments set up non-state regulatory regimes involving multiple stakeholders, including industries, advertisers, consumer organizations, and public interest groups. This approach varies across regions: the US aims to improve competition among social media companies to break monopolies, the EU introduces public interest norms through the Digital Services Act, China prohibits content against public interest, and Indonesia's policies sometimes limit internet access, particularly through internet shutdowns.[232]

iv. E-commerce

The Internet plays an increasingly significant role in economic transactions, serving as a rapid cross-border technology that facilitates communication processes associated with commercial activities, many of which ultimately occur offline.[233] While e-commerce offers opportunities to reduce transaction costs and expand business contacts globally, it also presents challenges, particularly regarding the need for safe and secure online transactions to establish trust in business relationships, especially in international commerce. However, the convenience of conducting business online also opens avenues for various forms of cybercrime, with e-commerce being a primary target. Effective regulation is essential to combat cybercrime, but existing regulations tend to be national and vary significantly between countries. Achieving globally harmonized regulations specific to the internet is unlikely due to diverse social, political, and legal contexts.[234] As a result, e-commerce has developed self-regulatory mechanisms to foster trust and facilitate commercial transactions. eBay, an online auction platform, exemplifies this approach.

[232] Daniela Stockmann, "Tech Companies and the Public Interest: The Role of the State in Governing Social Media Platforms," *Information, Communication & Society* 26, no. 1 (January 2, 2023): 1–15, https://doi.org/10.1080/1369118X.2022.2032796.
[233] Feick and Werle, Regulation of Cyberspace, 10
[234] U Sieber, "The Emergence of Information Law: Object and Characteristics of a New Legal Area," in *Law, Information and Information Technology*, ed. Eli Lederman and Ron Shapira (Kluwer Law International, 2001).

Initially a small, self-regulated community, eBay grew rapidly into a profitable business by establishing an online market between sellers and bidders, charging fees for completed exchanges.[235] However, growth brought the challenge of fraudulent behaviour from sellers or buyers. In response, eBay implemented a "Feedback Forum" for mutual ratings and customer support in 1996, expanding to a dedicated security team of 800 employees nine years later. This team utilizes in-house monitoring and data-mining software to detect and deter criminals. The mutual rating system, initially simple, has evolved into a sophisticated tool enabling customers to assess the trustworthiness of potential partners, continually enhanced by eBay's "Trust & Safety" teams. This self-regulatory instrument empowers customers to evaluate risk and decide on transactions while assisting the company in identifying and penalizing fraudulent behaviour to maintain platform integrity.[236]

v. Illegal content and conduct

The classification of content or behaviour as illegal or harmful, along with policies aimed at safeguarding collective symbolic values and specific groups such as minors, is not unique to the Internet. Like in other domains, national cultural and legal norms dictate their definition. What constitutes hate speech, extremist propaganda, glorification of violence, or pornography varies from one country to another, sometimes being prohibited in one and protected as free speech in another. Illegal or harmful conduct on the internet spans from traditional cybercrimes like hacking to more aggressive acts like cyberbullying, which can have severe consequences. The Internet amplifies the impact of such activities by enabling exponential dissemination, rapid spread, and global reach. This sheer volume leads to new effects on individuals, communities, and organizations. For instance, bullying, traditionally confined to physical spaces like schoolyards, has migrated to online platforms, making it easier to spread among children while evading the supervision of parents and teachers.

[235] Feick and Werle, Regulation of Cyberspace, 10

[236] J Goldsmith, "The Internet, Conflicts of Regulation, and International Harmonisation," in *Governance of Global Networks in the Light of Differing Local Values*, ed. Christoph Engel and Kenneth H. Keller (Law and Economics of International Telecommunications – Wirtschaftsrecht der internationalen Telekommunikation, 2001).

Perpetrators often use technical means to conceal their identity and may exploit differences in legal regulations between jurisdictions to evade consequences. This is particularly evident in highly profitable industries like internet-based pornography and gambling, which operate transnationally, catering to clients and participants worldwide. Cybercrime has become a major threat to individuals, organizations, and governments in recent years. As technology continues to advance, so do the methods and techniques used by cybercriminals, making it increasingly difficult for law enforcement agencies to combat this type of crime. In response to this growing threat, many states have taken steps to strengthen their legal and institutional frameworks to counter cybercrime. One of the key international instruments in this regard is the Budapest Convention on Cybercrime, which was adopted in 2001 by the Council of Europe and has been ratified by over 60 countries to date. The Convention provides a comprehensive legal framework for addressing cybercrime, including provisions on substantive criminal law, procedural law, and international cooperation. Although there have been developments of state's participation and adoption of the Convention, there has been very few that analyses its compliance and effectiveness.

B. Lessig's Regulability Theory (LRT)

1. Re-interpreting Lessig's Theory

Lawrence Lessig's Code: Version 2.0 offers one of the most enduring conceptual frameworks for understanding how behaviour is regulated in cyberspace.[237] Lessig rejects the notion that cyberspace is "naturally" free from governance simply because it is decentralized or lacks a single controlling authority. Instead, he argues that it is shaped; often quite deliberately, by constraints embedded in its design, infrastructure, and social practices. While governments may not always directly impose these constraints, the architects of digital systems, platform operators, and infrastructure providers exert a form of regulatory power through the environments they create.[238]

[237] Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Cambridge: Basic Books, 2006).
[238] *Ibid*

For Lessig, cyberspace is not merely a technological apparatus, a communications protocol, or a storage platform. It is a technology-enabled social space where communities interact beyond the ordinary limits of time and geography. Yet this social space rests on a physical and technical foundation: communication infrastructures and layered internet protocols (data link, network, transport, application), operationalized through software code. Because code is a human creation, it is malleable and thus open to regulation.

Lessig draws an analogy between code in cyberspace (what he calls "West Coast Code) and law in physical space ("East Coast Code"). Both shape behaviour, but through different mechanisms, and both can serve as instruments of governance. Lessig conceptualizes four distinct yet interdependent modalities of regulation: law, social norms, market, and architecture. These "regulators" act upon what he metaphorically calls the "pathetic dot"; the individual whose behaviour they constrain. The regulation of this dot is the sum of the four modalities acting together.[239] Changes in any one modality alter the overall regulatory environment: shifts in technology can produce shifts in norms, just as changes in market conditions can alter the application of law. Some constraints reinforce each other, while others may undermine one another; certain technologies may erode the force of norms and legal rules, while others may strengthen them. A complete view of regulation must therefore consider the four modalities not in isolation but as a system of interaction.

Each modality imposes a different type of cost on the regulated individual. Norms constrain through the social stigma a community imposes; markets constrain through the price they exact; architecture constrains through the physical or technical barriers it creates; and law constrains through the punishments it threatens. In combination, they form a dynamic regulatory environment in which the effect of each modality is shaped by its relationship to the others. Central to Lessig's theory is the recognition that architecture, expressed as code, can embed values similarly to law. For example, authentication-rich systems in e-commerce enhance the "regulatability" of cyberspace, enabling greater state and corporate control. Because code writers effectively determine what is possible in digital spaces, Lessig calls for social oversight to ensure that values embedded in cyberspace architecture reflect deliberate, collective choices rather than the unexamined preferences of a small set of private actors.[240]

[239] Lessig, Code, 119
[240] *Ibid*

Central to Lessig's theory is the recognition that architecture; expressed in cyberspace as code; can embed values in the same way that law can. The increasing use of authentication-rich systems in domains such as e-commerce, for example, enhances the "regulatability" of cyberspace, enabling greater state and corporate control. A clear example of this dynamic can be seen in the European Union's ICT regulatory approach, where policy frameworks for the single digital market operationalize governance objectives through both legal measures and architectural design. As noted by Balász Rátai, the foundations of EU ICT regulation closely mirror the structure of Lessig's Regulatability Theory.[241]

Thus, in the context of this study, Lessig's framework is reinterpreted as an analytical tool to map the governance of cyberspace. While the original theory describes general regulatory mechanisms, this study applies it to systematically analyse governance instruments issued by states, regional bodies, and international organizations. This reinterpretation aligns the four modalities with observable governance practices and documents, allowing empirical mapping of their scope, source, and effects across national, regional, and global levels.

i. Law

Law constitutes a formal legal constraint that regulates individual and collective behaviour through codified rules backed by the threat of sanction. It operates by prescribing permissible conduct, prohibiting certain actions, and specifying the conditions under which actions may occur.[242] Compliance is induced by the possibility of enforcement; those who violate the law are subject to punishment, whether in the form of fines, imprisonment, or other legal penalties. This threat of sanction serves as a deterrent, prompting individuals to reconsider before engaging in prohibited activities. In this way, law functions as an external constraint, shaping behaviour through authoritative command and the coercive capacity of the state.[243]
In the context of cyberspace, the law modality encompasses the body of legal norms that govern online conduct, such as copyright legislation, defamation laws, and obscenity regulations. These legal instruments threaten ex post sanctions for the

[241] Balazs Ratai, "Understanding Lessig - Implications for EU Cyberspace Policy," *International Review of Law, Computers & Technology*, 2005, 277–86, https://papers.ssrn.com/abstract=905866.
[242] Arttu Ruismäki, "Applying Lessig's Pathetic Dot Theory on Regulation of Digital Video Game Distribution Platforms" (Hanken School of Economics, 2022).
[243] Lessig, Code, 122

infringement of rights or the breach of statutory provisions in the digital environment. In this dissertation, the law modality refers to the formal, codified legal frameworks that regulate cyberspace activities. These include treaties, conventions, statutes, and other binding legal instruments at the international, regional, and national levels. Analysing governance through this modality involves identifying the number and scope of these legal instruments, their enforcement mechanisms, and their jurisdictional reach. This highlights how states and intergovernmental organizations attempt to impose order in cyberspace through rules that are legally binding and enforceable. Examples include international conventions on cybercrime, national data protection laws, and bilateral or regional agreements on cybersecurity cooperation. These legal frameworks establish explicit behavioural expectations and create accountability mechanisms through courts, regulatory bodies, or arbitration systems.

ii. Norms

Norms function in a manner similar to law, but they are unwritten social rules that prescribe what is considered appropriate or ethical behaviour within a given community.[244] They establish expectations for conduct and signal to individuals which actions are acceptable, and which are frowned upon. For instance, individuals might refrain from speaking loudly in a quiet public space, avoid interrupting someone during a conversation, or dress in a manner appropriate to a formal event. These behavioural constraints do not stem from codified legal provisions but from shared understandings within the community. The sanctions for violating norms are not legal penalties such as fines or imprisonment; rather, they take the form of social consequences; disapproval, criticism, reputational damage, or ostracism. In this way, norms regulate behaviour by leveraging the individual's desire for social acceptance and fear of communal disapproval.[245] In the context of cyberspace, norms are sets of shared expectations, values, and informal rules that shape online behaviour. These may be community-specific, such as the etiquette within an online forum, professional standards in digital workspaces, or the moderation policies

[244] *Ibid*
[245] *Ibid*

embedded in social media cultures; or they may reflect broader societal values, such as norms around protecting personal privacy, refraining from harassment, or attributing credit for creative works. However in this context, **the norms modality** is interpreted to not only encompasses social norms, but also ethical frameworks, and cultural practices that influence governance. Norms shape what is considered appropriate or legitimate behaviour in cyberspace, even in the absence of formal rules or technical restrictions. This modality is reflected in national and international policies on privacy, freedom of expression, and surveillance, where cultural values and political ideologies play a significant role in shaping regulatory preferences. Normative governance is often diffuse and informal but no less powerful, as seen in the global discourse on digital human rights and responsible state behaviour in cyberspace.

iii. Market

Market operates as a regulatory constraint by influencing behaviour through economic factors such as price, cost, and quality. Access to goods or services is determined by an individual's ability and willingness to pay; if the price rises, affordability decreases, and conversely, lower prices increase accessibility. Quality variation can also expand or limit available choices, shaping consumer preferences and behaviour. Unlike law, which relies on ex post sanctions, market constraints operate ex ante, influencing decisions before an action is taken. For instance, when the cost of a product or service exceeds an individual's budget, the decision not to purchase is shaped by market forces rather than by legal or social pressure. Governments and policymakers frequently employ market mechanisms to guide behaviour, such as imposing higher taxes on environmentally harmful goods to discourage their consumption or offering subsidies to promote renewable energy adoption.[246] In the context of cyberspace, market constraints manifest through pricing structures, subscription models, bandwidth limitations, and monetization strategies that influence online participation. Paid access to certain platforms or digital services can exclude individuals or groups unable or unwilling to meet the cost, while free or subsidized services expand participation. In this dissertation**,** the

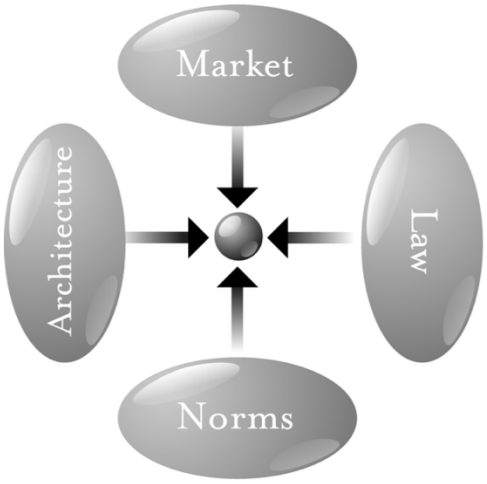
[246] *Ibid*

market modality captures how economic forces are shaped by trade agreements that incorporate digital trade provisions, intellectual property protections, and cross-border data flow rules further entrench market-driven regulatory norms. Policies aimed at strengthening or weakening the private sector's role. such as antitrust measures, industrial policies, or public-private partnerships, also reflect the market's influence on governance outcomes.

iv. Architecture

Architecture is a regulatory modality that operates ex ante, constraining behaviour through the design and functionality of physical or technological systems. It encompasses the material or structural features that determine what actions are possible or impossible within a given environment. In the physical world, architecture can take the form of tangible barriers, such as a fence preventing entry into private property, or immutable natural laws, such as gravity preventing unaided human flight. By shaping the conditions of interaction, architecture predetermines choices and directs behaviour before any action is taken.[247] In cyberspace, architecture is expressed through code; the software and hardware design choices that define the boundaries of user activity. Code establishes what actions are technically possible, impossible, easy, or difficult. The architecture modality in this dissertation includes instruments on data localization infrastructure that determines where and how data is stored, as well as the technical standards that ensure interconnectivity and interoperability across networks and platforms. Architectural decisions: such as encryption protocols, access controls, and routing practices, are often made by private sector actors and technical communities, but they have profound regulatory consequences, determining what is possible or impossible in cyberspace.[248]

[247] *Ibid*
[248] Denardis Laura, The Global War for Internet Governance. Yale University Press, 2014. https://doi.org/10.2307/j.ctt5vkz4n.



Picture 1 - Lessig's Regulability Theory (LRT)

By mapping cyberspace governance documents and practices across these four modalities, this study captures the full spectrum of regulatory mechanisms, from codified legal instruments and market structures to embedded technical designs and evolving social norms. This approach reveals that cyberspace governance is not monolithic but rather a complex and fragmented system where multiple forms of regulation interact, sometimes reinforcing and sometimes contradicting one another.

To operationalize Lessig's modalities in this governance mapping, each governance mechanism will be analysed based on the type and source of the regulatory instrument. This involves identifying the institution responsible for the document (e.g., states, international organizations, and national governments), the legal subject (whether the governance applies to states, IOs, NGOs, or other actors), the document type (such as treaties, strategies, conventions, or guidelines), and the source of international law where applicable (such as treaties, customs, or judicial decisions). These institutional and legal attributes provide the first analytical lens to classify governance documents according to their regulatory form.

In addition, the analysis considers the scope of governance, which refers to the governance type (policy, structure, legislation, cooperation) and the topic or content area being regulated. For example, a document addressing cybersecurity capacity-building represents a different governance scope than one establishing binding data protection rules. By examining both the instrument type and the substantive focus of governance activities, the mapping captures not only what type of regulation is being exercised but also over what subject matter and in what governance context.

These dimensions (type/source of instrument and scope of governance) are then cross-referenced with Lessig's modalities of regulation, allowing for a layered analysis. For instance,

a legal treaty addressing cybersecurity standards may reflect both Law and Architecture, while a regional code of conduct promoting ethical AI use may fall under Market and Norms. This cross-analysis highlights where governance mechanisms operate predominantly through formal law, where they are driven by market forces or technical infrastructure, and where they are shaped by shared values and norms. It also enables the identification of overlaps and gaps, revealing areas where regulation is fragmented across modalities, or where one regulatory modality dominates over others.

This approach is also linked to the broader analytical goal of this dissertation: to reveal not only the fragmented nature of global cyberspace governance but also the regulatory emphasis of different actors and instruments. By applying Lessig's modalities alongside governance classification criteria (institution, legal subject, governance type, and content area), the mapping provides a multidimensional view of how cyberspace is regulated, who is doing the regulating, and through what means. This enables a clearer understanding of how global governance in cyberspace operates across legal, technical, economic, and normative dimensions; thus, addressing both the diversity of regulatory actors and the complexity of regulatory mechanisms.

C. Fragmentation and regime complexes in international law

1. Fragmentation of International Law

The observation that international law consists of fragmented pockets of normative and institutional activity is longstanding. Despite the ambitious integrative promise of the United Nations, there has never been a single world legislature or appellate court capable of forging a unified, hierarchical legal order; and states have never exhibited a sustained, collective will to create one. Instead, at critical junctures and often for strategic reasons, states have framed discrete problems and responded by crafting new legal rules and empowering international organizations to address them.[249]

"Special regimes" can be conceived on a spectrum of breadth. In the narrow sense, a regime exists where a cluster of primary rules is accompanied by its own secondary rules on breach and responses to breach; for example, the diplomatic law framework articulated by

[249] Margaret A Young, "Introduction: The Productive Friction between Regimes," in *Regime Interaction in International Law*, ed. Margaret A Young (Cambridge University Press, 2012).

the ICJ in Tehran.[250] In a broader sense, a regime denotes a set of special rules, rights and obligations focused on a subject or territory (say, a river basin treaty or an agreement on particular weapons), potentially grounded in one treaty, several treaties, and supplemented by custom or subsequent practice. In the broadest sense, an entire functional field; "law of the sea," "international humanitarian law," "human rights law," "environmental law," "trade law," and so on, operates as a regime that aggregates treaties, custom, soft law, and practice into a recognisable body of rules and principles. [251]

These definitional moves embed different assumptions; many echoed in international relations (IR) scholarship; about what regimes are and how they interact. Because those assumptions shape analytical utility, they deserve explicit treatment when studying regime interaction. [252]

Four families of assumptions are especially important: who the relevant actors are; what institutional forms regimes entail; when in the law-making cycle regimes are analysed; and why systems-level or emergent practices matter. Clarifying these "who/what/when/why" dimensions sharpen our grasp of regimes and improves the study of their interactions. [253]

Actors (the "who"). Two of the ILC's three conceptions remain state-centred: regimes are built from international norms and practices authored and consented to by states, sometimes binding all states (e.g., near-universal treaties) and sometimes only subsets of them. This mirrors the consent-based foundations of regime thinking in IR, despite other disciplinary differences. By contrast, in the ILC Study Group's broadest conception, states are not the only formative influences. Analogous to work on private and transnational regulation, "private regimes" may crystallize around functionally specialized issues and need not reflect, and may even sideline, state interests.[254]

In IR, regimes are commonly defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations".[255] Givens IR's realist background, this is typically read to

[250] *Ibid*
[251] *Ibid*
[252] *Ibid*
[253] *Ibid*
[254] Dyson, M. (2005). The Idea of Public Law. By Martin Loughlin. [Oxford: Oxford University Press. 2003. xii, 163,
[255] Matthew Dyson, "The Idea of Public Law by Martin Loughlin," *The Cambridge Law Journal* 64, no. 2 (July 23, 2005): 503–4, https://doi.org/10.1017/S0008197305226946.

prioritize state intentions in regime creation. [256] The idea fuelled a large literature under "regime theory",[257] which initially took a normative turn even before constructivist accounts matured.[258] Much of this work analysed single regimes rather than their interaction, though research on regime complexes; overlapping, non-hierarchical arrangements has grown.[259] The IR definition has, in turn, influenced international legal scholarship.[260]

Other conceptions extend the actor set beyond states. The ILC's broadest notion, focused on functional specialisation or teleology (e.g., environmental or trade law), implies that aims and activities of non-state participants help constitute regimes.[261] This directs attention to how "professional mindsets" shape regime interaction,[262] as technical experts, NGOs, international secretariats, tribunal members, and other communities of practice become integral to both regime definition and cross-regime dynamics.

Institutions (the "what"). The ILC's definitions do not foreground international organisations, yet the broader conceptions often presuppose institutional backbones for rule-making, administration, and oversight. Historically, intergovernmental rules tied to geographic spaces have relied on administrative bodies.[263] Renewed attention to the normative influence of international organisations in governance; across legal and interdisciplinary literatures, has driven studies of "linkages," "global administrative law," "new governance," and fragmentation.[264] Case-based work, especially in environmental law, shows how institutional interplay illuminates specific legal arrangements.[265] In practice, many regimes include or depend on an "institutionalised system of dealing with a particular

[256] Young, Introduction: The Productive Friction, 197
[257] Stephen D Krasner, *International Regimes*, ed. Stephen D Krasner (Cornell University Press, 1983).
[258] Anne-Marie Slaughter Burley, "International Law and International Relations Theory: A Dual Agenda," *American Journal of International Law* 87, no. 2 (April 10, 1993): 205–39, https://doi.org/10.2307/2203817.
[259] Kal Raustiala and David G. Victor, "The Regime Complex for Plant Genetic Resources," *International Organization*, March 2004, https://doi.org/10.1017/S0020818304582036.
[260] Young, Introduction: The Productive Friction, 139
[261] *Ibid*
[262] Martti Koskenniemi, "The Fate of Public International Law: Between Technique and Politics," *The Modern Law Review* 70, no. 1 (January 4, 2007): 1–30, https://doi.org/10.1111/j.1468-2230.2006.00624.x.
[263] Young, Introduction: The Productive Friction, 8
[264] José E Alvarez, *International Organizations as Law Makers*, ed. José E Alvarez (Oxford University PressOxford, 2006), https://doi.org/10.1093/acprof:oso/9780198765639.003.0001.
[265] Olav Schram Stokke, *Governing High Seas Fisheries*, ed. Olav Schram Stokke (Oxford University Press, 2001), https://doi.org/10.1093/acprof:oso/9780198299493.001.0001.

field of behaviour".[266] A synthetic approach therefore treats regimes as sets of norms, decision-procedures, and organisations clustered around functional issue-areas.[267]

Stages (the "when"). International law is continuously made, implemented, and enforced, and these phases are not neatly sequential; law can be "made" informally before negotiation or formalisation.[268] Yet fragmentation debates often zoom in on conflict resolution among norms, a late-stage focus that presumes consolidated rules.[269] The ILC's broadest conception invites a more dynamic lens, recognising that a functionally specialised field (such as trade) undergoes ongoing normative evolution through multilateral bargaining and practice. IR regime definitions, with their emphasis on convergent principles, norms, rules, and procedures; can accommodate multiple stages, but sometimes at the cost of overlooking juris-generative power. For interaction studies, we need a flexible sense of stages and attentiveness to cross-fertilisation among them.[270]

Systems/emergence (the "why"). Broad regime labels risk essentialising fluid bodies of law: the ILC's widest definition is particularly vulnerable if diverse and conflicting professional perspectives are flattened into a single vision.[271] The regime idiom can also obscure general international law and distort system-level understanding,[272] making popular metaphors; "ships," "islands," "arenas," "platforms", misleading. Still, regimes exhibit notable stickiness: specialised courts, institutions, and professions entrench durable patterns of reasoning and practice.[273] Sometimes that intransigence is deliberate, reflecting efforts by powerful states to protect advantages.[274] Functional differentiation generates path dependence, higher transaction costs, and "tunnel vision",[275] even "solipsistic" or "imperial" tendencies within regimes.[276] Being mindful of these risks supports a hybrid definition: regimes are sets of norms, decision-making procedures, and organisations clustered around

[266] Young, Introduction: The Productive Friction, 9
[267] *Ibid*
[268] Young, Introduction: The Productive Friction, 313
[269] *Ibid*
[270] *Ibid*
[271] *Ibid*
[272] Young, Introduction: The Productive Friction, 258-259
[273] Young, Introduction: The Productive Friction, 257
[274] Eyal Benvenisti and George W Downs, "The Empire's New Clothes: Political Economy and the Fragmentation of International Law," *Stanford Law Review* 60, no. 2 (2007): 595–631.
[275] Young, Introduction: The Productive Friction, 11
[276] *Ibid*

functional issue-areas; and they are typically dominated by characteristic modes of behaviour, assumptions, and biases that shape both their internal development and their interactions with neighbouring regimes.

2. Regime interaction in creating, implementing and enforcing international law

The development of international law has historically occurred through the creation of autonomous, issue-specific regimes designed to address discrete problems, such as trade liberalisation or the exploitation of fisheries. These regimes: ranging from the trade regime to the law of the sea, differ in mandates, structures, and state membership, and generally operate without strong central coordination. The resulting institutional diversity and pluralism creates a governance environment where global problems rarely fit neatly within the boundaries of a single regime, producing both the potential for conflicting norms and the more mundane, yet pervasive, reality of overlapping institutional activity. While much of the fragmentation literature has concentrated on conflict resolution between regimes, particularly in judicial fora, the ongoing processes of inter-regime interaction remain comparatively under-explored. [277]

In this context, a hybrid definition of regimes as "sets of norms, decision-making procedures and organisations coalescing around functional issue-areas and dominated by particular modes of behaviour, assumptions and biases",[278] offers a conceptual lens for analysing regime interaction. The governance of global fisheries provides a clear example, as it operates at the intersection of multiple overlapping regimes: the law of the sea regime, centred on sustainable utilisation through key instruments such as UNCLOS and the Fish Stocks Agreement;[279] the FAO fisheries management regime, which addresses issues like illegal, unreported and unregulated fishing and promotes responsible practices;[280] the CITES species protection regime, underpinned by trade-sanctioning mechanisms; and the WTO trade

[277] Young, Introduction: The Productive Friction, 16
[278] Young, Introduction: The Productive Friction, 9
[279] United Nations Convention on the Law of the Sea (1982) 21 ILM 1261 (1982) (in force 16 November 1994)., Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks (1995) 34 ILM 1547 (in force 11 December 2001).
[280] Young, Introduction: The Productive Friction, 87

regime, whose subsidy disciplines directly impact the economics of fishing.[281] These regimes are not exhaustive, and their interaction must be understood with caution, avoiding the essentialisation of their characteristics and recognising the ongoing evolution of their mandates. [282]

Four features of these regimes significantly shape their interaction. First, they were developed at different historical moments, creating temporal misalignments. Second, they are administered by institutions with varying enforcement capacities and authority.[283] Third, membership is not uniform across regimes, leading to partial overlaps in state participation.[284] Fourth, they reflect divergent preferences within the international legal system, meaning their normative aims may conflict. Although the International Law Commission (ILC) has examined such tensions primarily in terms of conflicting norms before tribunals,[285] the fisheries context reveals that many challenges of regime interaction arise in the day-to-day institutional and normative overlap during law-making, implementation, and enforcement.

Regime interaction is perhaps most visible in dispute settlement, as in the WTO Appellate Body's reference to CITES in defining "sustainable development" in the US–Shrimp case,[286] or the threatened parallel proceedings in the Swordfish dispute.[287] Yet it also plays a decisive role at other stages. In law-making, for example, WTO negotiations on fisheries subsidies have incorporated perspectives from the law of the sea and FAO regimes, partly to address criticisms of the WTO's "ecological blind spot".[288] These negotiations have been shaped by multi-actor engagement; including UNEP, NGOs such as WWF, trade and fisheries delegates, and technical experts, leading to proposals for innovative institutional arrangements, such as using FAO standards as peer-review benchmarks. Similarly, in implementation, inter-regime cooperation, such as the CITES–FAO data-sharing MoU, can

[281] Agreement Establishing the World Trade Organization (signed 15 April 1994) in WTO, The Legal Texts (Cambridge University Press, 1999) 3 and associated WTO- covered agreements
[282] Young, Introduction: The Productive Friction, 18
[283] *Ibid*
[284] *Ibid*
[285] ILC Study Group, 'Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, Conclusions of the Work of the Study Group' (A/CN.4/L.702) (18 July 2006)
[286] Appellate Body Report, United States – Import Prohibition of Certain Shrimp and Shrimp Products, WT/DS58/AB/R (circulated 12 October 1998) (DSR 1998:VII, 2755)
[287] M.A Orellana, "The Swordfish Dispute between the EU and Chile at the ITLOS and the WTO," *Nordic Journal of International Law* 71, no. 1 (2002): 55–81, https://doi.org/10.1163/157181002400497867.
[288] C. Hutchison, "Ecological Sensitivity and Global Legal Pluralism: Rethinking the Trade and Environment Conflict," *Journal of Environmental Law* 18, no. 1 (December 2, 2005): 172–76, https://doi.org/10.1093/jel/eqi043.

both enhance technical capacity and entrench regime hierarchies, with fishing states leveraging procedural clauses to prioritise soft-law commitments over binding obligations.[289]

The impediments to regime interaction are significant. Functional compartmentalisation, grounded in the "principle of speciality," can artificially restrict the competence of international organisations, failing to recognise the cross-cutting nature of complex global issues.[290] The lack of domestic policy coordination further constrains interaction, with disparities in national capacity limiting coherent engagement across regimes.[291] Regime insularity manifest in closed negotiations, exclusionary working groups, and resistance to observer participation reinforces fragmentation; and reflects broader concerns about sovereignty and legitimacy.

The legal basis for regime interaction can be categorised into three models. The first, parallel membership, requires that all member states of interacting regimes share mutual commitments before norms can influence each other.[292] While consistent with a strict consent-based view of international law, this model risks enabling minority vetoes over normative development.[293] The second, mutual agreement, allows for interaction through explicit treaty provisions or standalone agreements, as seen in CITES' openness to IGO and NGO participation, and the proposed WTO–FAO fisheries subsidies framework. [294] However, legitimacy concerns persist, particularly when exogenous standards are incorporated without consensus.[295] The third, institutional arrangements, encompasses both formal mechanisms; such as MoUs between secretariats; and informal exchanges of norms and information.[296] While these arrangements can facilitate mutual learning in a post-

[289] Young, Introduction: The Productive Friction, 87
[290] Use of Nuclear Weapons in Armed Conflict (1999) (I) ICJ Rep 66.
[291] UN Doc A/55/274, Annex I, para. 15.
[292] Andreas L Paulus, "Legitimacy of International Law and the Role of the State Legitimacy of International Law and the Role of the State THE LEGITIMACY OF INTERNATIONAL LAW AND THE ROLE OF THE STATE INTRODUCTION: FRAGMENTATION AND THE ROLE OF THE STATE," *Michigan Journal of International Law*, vol. 25, 2004, https://repository.law.umich.edu/mjilhttps://repository.law.umich.edu/mjil/vol25/iss4/13.
[293] Panel Report, EC – Measures Affecting the Approval and Marketing of Biotech Products Panel Report WT/DS291/R, WT/DS292/R, WT/DS293/R (circulated 29 September 2006) (DSR 2006:III, 847).
[294] FAO Guiding Lines Regarding Relationship Agreements Between FAO and IGOs (Resolution of 10th session of FAO Conference).
[295] Agreement on the Application of Sanitary and Phytosanitary Measures (signed 15 April 1994) in WTO, The Legal Texts (Cambridge University Press, 1999) 59.
[296] Young, Introduction: The Productive Friction, 97

sovereign, non-hierarchical governance environment, their legitimacy depends on ensuring inclusivity, transparency, and critical scrutiny of shared information.

By integrating these insights, the theoretical framework for regime complex analysis must move beyond a narrow focus on norm conflict toward a broader understanding of interaction across all stages of international law-making. This perspective situates fragmentation not merely as a problem of legal inconsistency, but as an inherent feature of the multi-level, multi-actor structure of international law, one that both constrains and enables governance innovation.

3. Regime complexity in cyberspace governance

The concept of a *regime complex* emerged to describe the proliferation of overlapping international institutions and agreements governing a particular issue area. Early formulations by ala and Victor[297] and Alter & Meunier[298] identified two defining features: (1) an array of elemental institutions; whether functionally or territorially defined, each making authority claims over the same issue area, and (2) the absence of hierarchy among them, meaning no definitive mechanism exists to determine which rules, norms, or decision-making procedures prevail in the event of conflict. Alter and Raustiala (2018) refine this definition as an array of partially overlapping, non-hierarchical institutions that together produce dense, and often contested, rule systems.

Henning et al. (2020) advance this framework by introducing two analytical dimensions: hierarchical authority relations and institutional differentiation; that shape how regime complex's function. At one end of the spectrum lies the *fragmented* ideal type, marked by non-hierarchical relations and low differentiation, producing rule conflicts, policy incoherence, and high opportunities for forum shopping.[299] At the other end lies the *integrated* complex, characterized by clear hierarchies, specialized institutional roles, and greater rule coherence. These dimensions serve as intervening variables: hierarchical

[297] Kal Raustiala and David G. Victor, "The Regime Complex for Plant Genetic Resources," *International Organization* 58, no. 02 (April 19, 2004), https://doi.org/10.1017/S0020818304582036.
[298] Karen J. Alter and Sophie Meunier, "The Politics of International Regime Complexity," *Perspectives on Politics* 7, no. 1 (March 2009): 13–24, https://doi.org/10.1017/S1537592709090033.
[299] Orsini, Amandine & Morin, Jean-Frédéric & Young, Oran. (2013). Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance?. Global Governance. 19. 10.1163/19426720-01901003.

complexes can reduce rule conflict, increase compliance, and coordinate actors more effectively, though they may be less adaptable to shifts in the geopolitical environment.

Nye (2014) further enriches the analysis of regime complexes by proposing four evaluative dimensions: depth (the hierarchical coherence of a set of norms), breadth (the scope of actor acceptance), fabric (the mix of state and non-state actor involvement), and compliance (the extent of adherence in practice). These dimensions illuminate not just structural features but also the functional performance of regime complexes.

Comparative studies show that regime complexes vary in complexity.[300] Low-complexity regimes, such as the Law of the Sea, international aviation law, and public international law; tend to have clear jurisdictional boundaries, a small number of core institutions, and relatively high normative convergence. Mid-complexity regimes: including international humanitarian law, human rights law, monetary and financial law, trade law, and international criminal law, feature greater institutional diversity and some overlaps, but still retain central coordinating norms or institutions. High complexity regimes: such as international investment law and environmental law, are marked by extensive institutional proliferation, functional and normative overlap, and the absence of unifying hierarchy, producing space for forum shopping, norm contestation, and conflicting obligations.[301] By these criteria, the cyber-regime complex clearly belongs in the high-complexity category: it spans multiple issue areas (security, trade, human rights, infrastructure, and technical standards), involves a vast array of state and non-state actors, and lacks a central coordinating authority.

Raymond describes the cyber-regime complex as a sprawling, decentralize governance environment, where decisions are made by heterogeneous public and private actors; ranging from states and intergovernmental organizations to standards bodies and private firms, that often operate autonomously, even when nominally linked by authority relations. Governance is further complicated by the *nested "club goods"* structure of cyberspace: all Internet users belong simultaneously to the global club of Internet users, national clubs governed by domestic law, and service-provider clubs governed by contractual terms, alongside specialized technical clubs such as ICANN and the IETF. This nested architecture means that

[300] Laura Gómez-Mera, "International Regime Complexity," in *Oxford Research Encyclopedia of International Studies* (Oxford University Press, 2021), https://doi.org/10.1093/acrefore/9780190846626.013.648.
[301] *Ibid*

decisions in one part of the complex can have far-reaching spillover effects on others, amplifying coordination challenges.[302]

The political dynamics of the cyber-regime complex are shaped not only by its technical architecture but also by strategic contestation. Raymond & Sherman (2024) identify the rise of authoritarian multilateralism in cyberspace governance: a process in which authoritarian states such as Russia and China promote state-centric multilateral governance modalities to reshape the normative underpinnings of the liberal order. These states engage in *liberal mimicry* and *norm retrieval* to reorient existing multilateral institutions and, in some cases, create new ones aligned with sovereignty-centric, illiberal governance preferences. This strategy exploits the non-hierarchical, overlapping structure of the regime complex to promote alternative normative orders.[303]

Faude & Große-Kreul (2020) shift attention to the normative legitimacy of regime complexes, arguing that legitimacy depends not only on the quality of internal decision-making but also on how institutions manage the negative spillovers their rules create for others. In a regime complex, institutions are embedded in interdependent structures where rule overlap generates pressure for *inter-institutional justificatory practices*. These practices can "break open" the partial orders of justification found in single institutions, enabling marginalized actors to contest harmful spillovers and, under some conditions, fostering normative progress.[304]

Underlying all regime complex dynamics is the reality that states construct regimes on the basis of their interests, which in turn reflect the preferences of domestic constituencies under conditions of complex interdependence. Power within regime complexes derives from asymmetrical interdependence: states with greater capacity to affect others and more favourable "no-agreement" alternatives enjoy stronger bargaining positions. Information,

[302] Mark Raymond, "International Regime Complexes," in *Handbook of Research Methods in International Relations*, ed. R Huddleston, Thomas, Jamieson, and Patrick James (Edward Elgar Publishing, 2022), 183–97, https://doi.org/10.4337/9781839101014.00020.
[303] Mark Raymond and Justin Sherman, "Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice," *Contemporary Security Policy* 45, no. 1 (January 2, 2024): 110–40, https://doi.org/10.1080/13523260.2023.2269809.
[304] Benjamin Faude and Felix Groβe-Kreul, "Let's Justify! How Regime Complexes Enhance the Normative Legitimacy of Global Governance," *International Studies Quarterly* 64, no. 2 (June 1, 2020): 431–39, https://doi.org/10.1093/isq/sqaa024.

beliefs, and the distribution of relevant power resources further shape outcomes, influencing both the design of institutions and the strategic behaviour of actors navigating the complex.

In cyberspace, this combination of high complexity, decentralization, power asymmetries, and normative contestation produces a governance environment that is both richly interconnected and deeply fragmented. Regime complex theory thus provides a critical framework for understanding not only the structural features of cyberspace governance but also the political, normative, and functional dynamics that drive its evolution.

D. Defining and Operationalising Easternisation

The term 'easternization' is an uncommon one. To date, it has not yet been used by legal scholars particularly in the context of international law. It would make sense since it is not a legal term. I first came across the word in Gideon Rachman's book titled "Easternisation: War and Peace in the Asian Century" published in 2016. As a word that has the same ending (suffix) as westernization, modernization, civilization, to which some I have heard of, but it was the first time for me seeing it paired with the adjective 'eastern'.[305]

In Rachman's book, his discussion on the phenomenon of 'easternization' are viewed from the context of global world and economic order. The main premise is that the global power centre is shifting from the West to the East. The starting point of this change was the global economic crisis, which meant a decline for the West and a strengthening for the East. Rachman considers that the strongest power is China, which may become the new global power centre, and he explores the fact of the West-East shift accordingly, from the point of view of America, Latin-America, Europe, Russia, Africa, the Middle East, East Asia, Southeast Asia, and Australia, too. Rachman suggests that the decline of Western centrality is attributed, in part, to the rapid development of Asian cities like Shanghai and Singapore. Drawing parallels with cyclical patterns in Chinese history, where dynasties rose and fell, he contrasts this with what he sees as a more linear trajectory in American history.

However, there is little to no mention on how the concept of 'easternization' has also been manifested in the context of international legal order. This is obvious because international law scholars are more familiar with concept of western imperialism, colonization which are challenged by critiques of Third World Countries of International law (TWAIL). The TWAIL doctrine,

[305] Jain, Easternization of the West

however, is one that is too specific and 'theoretical' towards the critique of western international law. Because of the premise of my thesis is aimed at proving a mere 'shift' of international law formation from the dominated western/European states to eastern (south-east) Asian states, I would avoid in incorporating the discussion of TWAIL. Instead, I am proposing the use of the term 'easternization' using my own interpretation which would be analysed in the international law context.

Before developing this doctrinal definition, it is useful to note how other authors have conceptualized easternisation. Sushil Jain highlighted the historical shift of global power from East to West and argued that the traditional role of imperial states is evolving as newly developed Pacific nation-states emerge. "Easternization," a term akin to westernization, modernization, and civilization, signifies the influence of the East on the Western world in population, immigration, economy, religion, and philosophy. Previously controlled by Western imperial nations, the East now critiques Western value systems and introduces Eastern concepts in various aspects, such as culture, arts, and infrastructure. The concept of Easternization challenges the notion of Western superiority.[306]

In this dissertation, easternisation in international cyberspace law *is understood as a legally observable process whereby Asian regional institutions and states develop and institutionalize governance frameworks that selectively engage with existing Western-led norms while advancing regionally grounded regulatory philosophies.* This process does not displace established international legal structures, but contributes to a pluralized legal order in which multiple, coexisting approaches to authority, legitimacy, and regulation operate in parallel. This process is evidenced by five indicators: (i) the share of outputs in the form of legal and normative instruments originating in Asia compared to traditional Western institutions; (ii) the bindingness profile of such instruments, highlighting the region's reliance on soft law and voluntary cooperation; (iii) cross-reference flows, tracing whether ASEAN instruments primarily import norms from Western regimes or generate autonomous standards; (iv) implementation uptake, showing how ASEAN-level norms are incorporated into domestic law and policy; and (v) forum-shifting patterns, where Asian states increasingly privilege regional or alternative venues over universal ones. Together, these criteria establish easternisation as a doctrinally grounded and empirically testable concept, distinct from broader notions of regionalisation or pluralisation.

[306] *Ibid*

The first indicator is norm-setting share. This refers to the relative contribution of ASEAN and its member states to the production of normative instruments in cyberspace governance compared to global and regional Western institutions. Measuring norm-setting share allows us to observe whether Southeast Asia is simply responding to external models, or whether it is increasingly providing original inputs into the global legal order. An increase in the proportion of ASEAN-originated frameworks would demonstrate a tangible shift in normative authority toward the region.

A second indicator is the binding versus non-binding mix. ASEAN's well-documented reliance on soft law, consensus, and political declarations stands in contrast to the more legalistic and binding approaches of the European Union and, to a lesser extent, the United Nations. By systematically comparing the relative balance of binding and non-binding instruments across regions, this study demonstrates how ASEAN's approach reflects a distinct governance philosophy. This divergence matters for easternisation because it shows not only that ASEAN is producing instruments, but that it is doing so in a way that reconfigures expectations of what international law in cyberspace looks like.

The third indicator is cross-referencing practices. Instruments produced by ASEAN and its member states often reference or incorporate existing international or regional frameworks, particularly those originating from the UN and EU. Examining the extent and manner of these references provides insight into whether ASEAN is primarily importing external norms, thereby reinforcing Western primacy, or whether it is developing autonomous rules and frameworks. Limited reliance on external references, or the selective reinterpretation of them, signals a growing capacity for independent norm production, a core element of easternisation.

Finally, the fourth indicator is institutional centrality. Within the broader regime complex of cyberspace governance, institutions vary in their visibility, recognition, and influence. ASEAN's centrality is assessed by examining how its instruments and institutions interact with, complement, or are acknowledged by other global and regional actors. A higher degree of centrality would indicate that ASEAN is not only producing instruments for its own region but also becoming a reference point within the global regime complex. This would mark a significant departure from the historical marginality of Southeast Asia in international lawmaking.

Together, these four indicators provide a framework to distinguish easternisation from broader processes of regionalisation or pluralisation. By applying them to cyberspace governance, the

thesis demonstrates how Southeast Asia's governance practices constitute not only a regional adaptation, but also a redistribution of normative authority that challenges the West's historical primacy in international lawmaking.

CHAPTER IV
EASTERNISATION OF INTERNATIONAL LAW: FRAGMENTATION AND REGIME COMPLEX OF CYBERSPACE GOVERNANCE

A. Mapping of International cyberspace governance under LRT

This first section presents the results of a comprehensive mapping of international cyberspace governance instruments through the analytical lens of Lessig's Regulatability Theory (LRT). Central to this approach is the classification of documents based on Lessig's four regulatory modalities: Law, Market, Architecture, and Norms; each representing a distinct mechanism through which behaviour in cyberspace is shaped and controlled. However, rather than applying this typology in isolation, the mapping adopts a multidimensional classification framework designed to capture the institutional, legal, and functional complexity of cyberspace governance.

To that end, the documents were coded across several analytical categories. These include temporal distribution (by year) to trace policy momentum over time; institutional level (national, international, regional, etc.) to assess the vertical layering of governance; and legal subject (states vs. international organizations) to determine who the primary norm-setting actors are. The mapping also categorizes documents by governance function (e.g., policy, legislation, cooperation, structural frameworks), document type (such as strategies, laws, conventions, MoUs), and source of international law (treaties, customs, general principles, judicial decisions) to identify the legal basis and normative weight of each instrument.

Moreover, each document was examined for its main and supporting regulatory scope, allowing for the identification of thematic priorities such as cybersecurity, privacy, infrastructure, or cross-border data flows. A separate dimension captured the governance type; whether the instrument establishes norms, creates binding obligations, coordinates institutional arrangements, or enables cooperation. Finally, all of these classifications are cross-referenced with Lessig's modalities, enabling a layered understanding of how law, market forces, technological architecture, and social norms are embedded in formal governance instruments.

The data was synthesized from official institutional repositories; including UNIDIR Cyber Policy Portal,[307] the UN Official Document System,[308] EUR-Lex,[309] and ASEAN's documentation archives,[310] and visualized using Tableau to facilitate comparative and temporal analysis. Through this mapping, the section identifies empirical trends, normative gaps, and regional divergences in the design and function of cyberspace governance regimes. These findings serve as the empirical foundation for subsequent chapters on regime fragmentation, governance asymmetry, and the evolving easternisation of international law in digital domains.

1. Total number of documents

The mapping of international cyberspace governance under Lessig's Regulatability Theory (LRT) began with an extensive collection of publicly available instruments, policies, and legal texts that engage with the governance of cyberspace. Drawing from a diverse range of repositories; including international organization databases, national archives, and institutional publications, over 200 documents were initially identified as potentially relevant. However, this preliminary set underwent a rigorous filtering process to ensure consistency with the analytical framework and classification system designed for this study.

Documents were excluded based on several criteria: academic articles and scholarly commentary (unless officially adopted by institutions), informal correspondence or non-binding communications, and duplicate or superseded versions of the same instrument. This filtration ensured that only formal instruments with identifiable legal, normative, architectural, or market-related implications were retained. Following this verification process, the final corpus comprises 148 eligible documents. These documents constitute the foundational dataset for the subsequent mapping and analysis, enabling a structured assessment of how cyberspace is governed across multiple levels; international, regional, and national, through the lens of Lessig's four modalities.[311]

[307] UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/
[308] United Nations Official Document System, https://documents.un.org/
[309] European Union EUR-Lex, https://eur-lex.europa.eu/homepage.html
[310] ASEAN Legal Instruments Database, https://asean.org/legal-instruments-database/
[311] *See* Annex I for full list of documents and criteria mapping

2. Temporal distribution of documents

The 148 documents mapped in this study span a period of nearly four decades, ranging from 1986 to 2025. This temporal breadth reflects the evolving trajectory of international cyberspace governance, which has gradually intensified in both volume and complexity over time. A significant increase in document production can be observed beginning in the early 2010s, aligning with the global recognition of cyberspace as a critical domain for security, economic development, and human rights.[312]

The peak year is 2021, during which 17 documents were issued; marking the most active year in terms of international and regional governance outputs related to cyberspace. This surge may be associated with a post-pandemic policy reorientation, heightened geopolitical tensions in digital domains, and the acceleration of digital transformation globally.[313] The dataset reveals relatively sparse activity in the 1990s and early 2000s, with only a few foundational instruments introduced during this period. Notable upticks occurred around the years 2000, 2015, and 2018–2019, each reflecting distinct policy moments: from early technical regulation to mid-decade norm development, to the emergence of new governance frameworks involving multistakeholder collaboration.

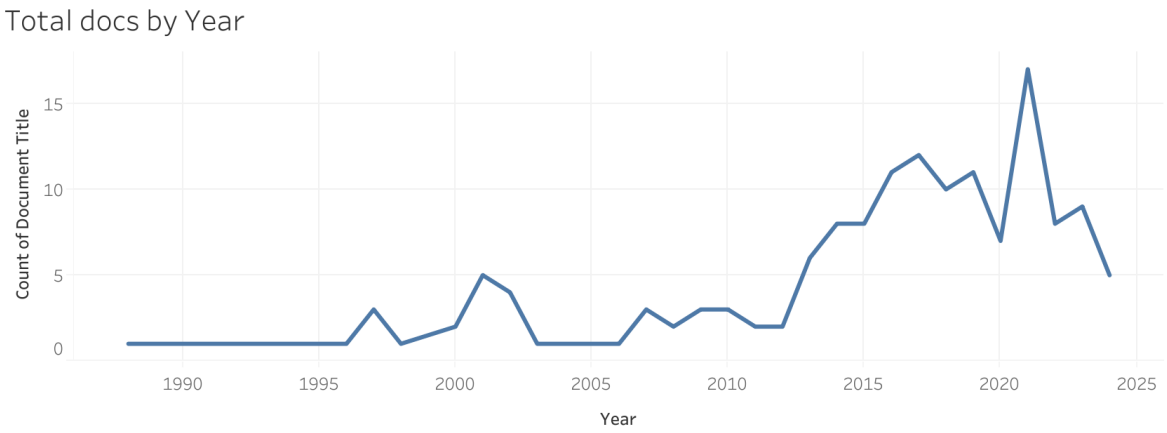


Figure 1 - Temporal Distribution of Documents

[312] Nye, The Regime Complex, 7
[313] *Ibid*

Documents were sourced from credible institutional repositories including the UNIDIR Cyber Policy Portal,[314] United Nations Official Document System (ODS),[315] EUR-Lex (EU law database),[316] and the ASEAN Document Database.[317] This multi-source approach ensures a comprehensive and representative coverage of governance instruments across different levels and regions. From a governance trend perspective, the post-2015 period marks a clear acceleration, suggesting the emergence of a more fragmented yet dynamic governance landscape, increasingly populated by a mix of legally binding instruments, strategic policies, and cooperative frameworks

Full Data
17 rows 2 fields

Show Fields

Tableau Mapping Year	Tableau Mapping Document Title
2021	Report of the Open-ended working group on developments in the Field of Information and Telecommunications in the Context of International Security A/AC.290/2021/CRP.2
2021	Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (A/76/135)
2021	Compilation of Preliminary Conclusions and Recommendations from the UNODC Expert Group on Cybercrime
2021	General Assembly Resolution 79/243 Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharin...
2021	Cybersecurity Strategy Guide – Second Edition
2021	Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law
2021	Private Sector Engagement in Responding to the Use of ICT for Terrorist Purposes
2021	ASEAN Security Outlook 2021
2021	ASEAN Digital Integration Index (ADII) – First Report
2021	ASEAN Digital Masterplan 2025 (ADM 2025)
2021	ASEAN Digital Masterplan 2025 (ADM2025)
2021	Computer Misuse Act 1993 (2020 Revised Edition)
2021	Cybersecurity Certification Guide
2021	The Singapore Cybersecurity Strategy 2021
2021	National Security Policy (NSP)
2021	Pelan Strategik MINDEF 2021–2025
2021	BSSN Regulation No. 3/2021 on Cybersecurity and Media Literacy

Figure 2 Count of Documents issued in 2021

3. Regional distribution and east vs west comparison

The mapping also classifies all 148 documents based on their region of origin, specifically from the United Nations (UN), the European Union (EU), and ASEAN Member States. This regional categorization enables an initial assessment of the geopolitical contours shaping cyberspace governance. Among these, the United Nations system produced the most documents, contributing 40 in total. These include General Assembly resolutions, Group of Governmental Experts (GGE) reports, and outputs from

[314] UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/
[315] United Nations Official Document System, https://documents.un.org/
[316] European Union EUR-Lex, https://eur-lex.europa.eu/homepage.html
[317] ASEAN Legal Instruments Database, https://asean.org/legal-instruments-database/

institutional bodies such as the UN Human Rights Council and the International Telecommunication Union (ITU).

The UN's role as a norm-setting platform is clearly reflected in the volume and diversity of instruments it has generated. However, when documents are grouped by broader geopolitical orientation; Western (UN and EU) versus Eastern (ASEAN Member States), a noteworthy pattern emerges.[318] **Of the total, 88 documents originate from** Eastern actors, primarily ASEAN regional institutions and individual member states. In contrast, 60 documents come from Western sources, namely the UN and EU combined. This Eastern majority (88:60) in document count may be interpreted as a signal of growing normative and regulatory activity outside the traditional Western-centric governance centers. It suggests that Southeast Asian states are not merely passive recipients of international norms, but active contributors to, and in some cases, originators of cyberspace governance frameworks.[319]

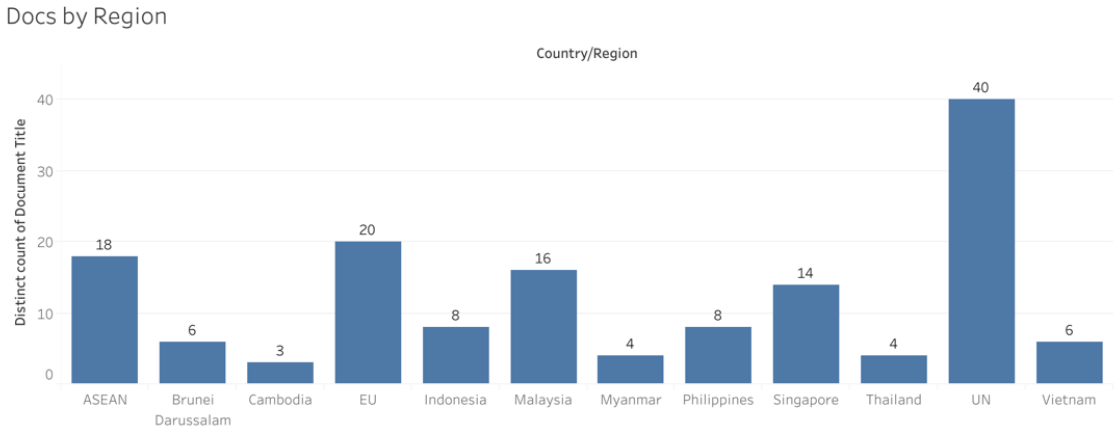


Figure 3 Documents by region

[318] For the purposes of this study, the "Western" region refers to governance instruments originating from the United Nations system and the European Union, both of which have historically been at the forefront of global norm-setting and institutional development in cyberspace governance. While the UN is nominally universal, its primary normative outputs in this domain—particularly those related to multilateral processes and democratic values—tend to reflect Western legal and political traditions. In contrast, the "Eastern" region is defined here as encompassing ASEAN Member States and ASEAN as a regional organization. This grouping represents the perspectives of Southeast Asian countries, many of which have taken distinctive approaches to cyberspace governance, often emphasizing sovereignty, developmental priorities, and non-interference. Though this East–West dichotomy is an analytical simplification, it helps to reveal broader structural dynamics and normative divergences in the emerging global governance landscape.

[319] Xuechen Chen and Yifan Yang, "Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance," *International Spectator* 57, no. 3 (2022): 48–65, https://doi.org/10.1080/03932729.2022.2066841.

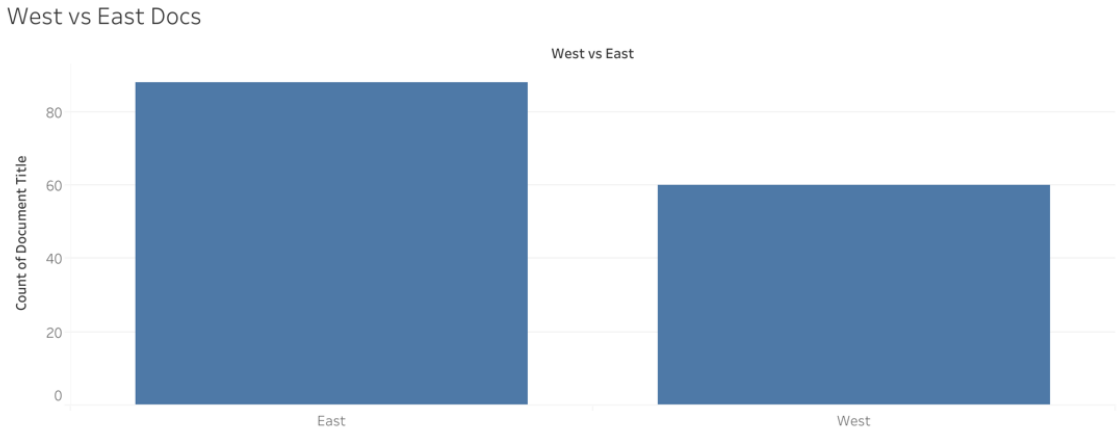


Figure 4 Documents by region (west vs east)

This imbalance also sets the stage for a deeper discussion on the easternisation of international law, as emerging actors from the Global East increasingly shape regulatory narratives and institutional practices. Such regional disparities not only underscore the fragmentation of global governance regimes but also point toward the possibility of plural legal orders developing concurrently, each shaped by regional values, institutional capacity, and strategic interests.

4. Documents by level and legal subject

The mapped dataset reveals important patterns in the institutional levels and legal subjects responsible for producing cyberspace governance instruments. These classifications were designed to align with the foundational categories recognized under international law, particularly those delineated by the UN Charter and subsequent jurisprudence concerning legal personality and treaty-making authority.[320] In terms of institutional level, the majority of documents (65 out of 148) are national-level instruments, reflecting the central role of states in articulating domestic responses to global cybersecurity, data governance, and digital infrastructure challenges.

These national strategies, laws, and regulations highlight both the localization of cyberspace governance and the limited reach of universal norms. Following national instruments, international-level documents rank second (43 documents), encompassing resolutions, conventions, and strategic frameworks adopted through global multilateral fora. Regional-level instruments (30 documents) and EU-specific regional documents (7 documents) also form a significant portion of the dataset, further emphasizing the role of

[320] Statute of the International Court of Justice, art. 38(1), 59 Stat. 1055, 33 UNTS 993 (1945).

regionalization in filling normative or institutional gaps. Notably, trilateral, multilateral, and bilateral instruments remain minimal in number (together contributing fewer than 5 documents) suggesting that while cooperation exists, it has not yet materialized in the form of robust treaty-based governance at these intermediate levels.[321] This further supports the observation that cyberspace governance remains fragmented and asymmetrical, both vertically (across levels) and horizontally (across regions).

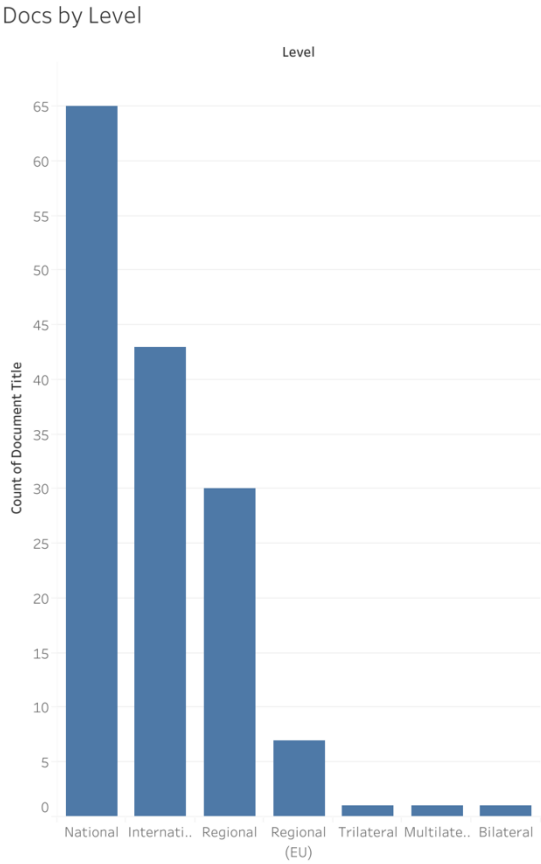


Figure 5 Documents by level

As for legal subjects, the mapping reveals a clear dominance of state actors, who are responsible for producing 98 documents, in contrast to international organizations, which account for approximately 50 documents. This dominance illustrates that states remain the primary architects of cyberspace governance, even as international organizations attempt to coordinate, standardize, or frame collective action. While the broader discourse

[321] Worku Gedefa Urgessa, "Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin," *Computer Law & Security Review* 36 (April 2020): 105368, https://doi.org/10.1016/j.clsr.2019.105368.

on cyberspace governance increasingly includes non-state actors, particularly through multistakeholder models, the scope of this mapping was intentionally narrowed to include only those actors that hold recognized legal status under international law; specifically States and International Organizations.

Although initial consideration was given to including Non-Governmental Organizations (NGOs) and private sector actors, the final categorization was kept intentionally conservative.

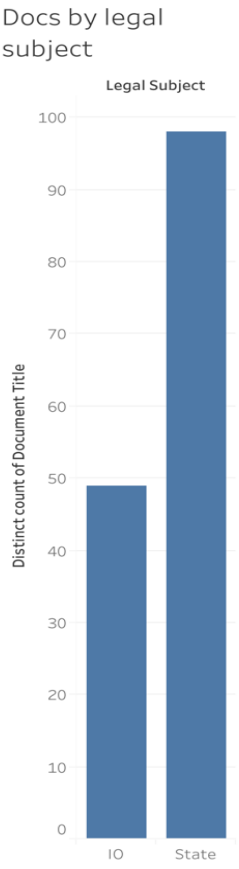


Figure 6 Documents by Legal Subject

This decision was influenced by the nature of the datasets used (UNIDIR, UN repositories, EUR-Lex, ASEAN archives), which predominantly feature instruments formally issued or endorsed by state or intergovernmental bodies. This approach reinforces the study's grounding in formal international legal structures, even as it acknowledges the parallel influence of informal and hybrid governance mechanisms.

5. Documents by source of international law

This classification examines the extent to which cyberspace governance instruments possess binding legal authority under the framework of international law, as codified in Article 38(1) of the Statute of the International Court of Justice (ICJ).[322] According to this provision, international law is derived from four main sources: (a) international conventions (treaties), (b) international custom, (c) general principles of law recognized by civilized nations, and (d) judicial decisions and the teachings of highly qualified publicists.

The data reveals that the overwhelming majority of instruments fall under the category of general principles of law (98 documents). These include strategic frameworks, principles-based guidelines, and normative declarations that, while not legally binding, carry considerable persuasive authority and often serve as precursors to formal regulation. In contrast, only 15 documents were categorized as treaties or conventions, illustrating the limited treaty-based architecture governing cyberspace at the global level. Notably, most of these treaties originate from the European Union, such as the Budapest Convention on Cybercrime, the General Data Protection Regulation (GDPR), and various directives on cybersecurity and personal data.

From the United Nations system, only a single binding instrument was identified: the International Telecommunication Regulations (ITRs)[323]; an infrastructure-focused treaty with indirect relevance to cyberspace governance. Additionally, one important draft treaty, the UN Draft Convention on Cybercrime, was included due to its anticipated normative significance, despite not yet being adopted.

ASEAN contributed three treaties, including the e-ASEAN Framework Agreement[324] and the ASEAN Agreement on Electronic Commerce,[325] both of which signal regional efforts to establish cooperative digital governance norms. Strikingly, no instruments were categorized under "international custom", suggesting that state practice and *opinio juris* in cyberspace have not yet crystallized into universally accepted customary rules.

A small number of documents (4 in total) were linked to judicial decisions or authoritative legal writings, typically cited in explanatory reports or used as interpretative

[322] ICJ Statute Art 38 (1)
[323] International Telecommunication Regulations, Dec. 9, 1988, 1589 UNTS 3.
[324] e-ASEAN Framework Agreement, Nov. 24, 2000, 2216 UNTS 233.
[325] ASEAN Agreement on Electronic Commerce, Jan. 22, 2019.

references rather than as binding precedents. An additional classification category: national laws, was created to account for the large number of instruments emerging from ASEAN member states.

While not a formal source of international law under Article 38(1), these national laws were included due to their increasing extraterritorial influence, cross-border interoperability relevance, and cumulative contribution to regime complexity. Their inclusion is particularly significant for tracing the fragmentation of cyberspace governance and the easternisation of regulatory authority, as they reflect how Southeast Asian states are independently shaping norms outside of dominant Western treaties or UN-led processes.

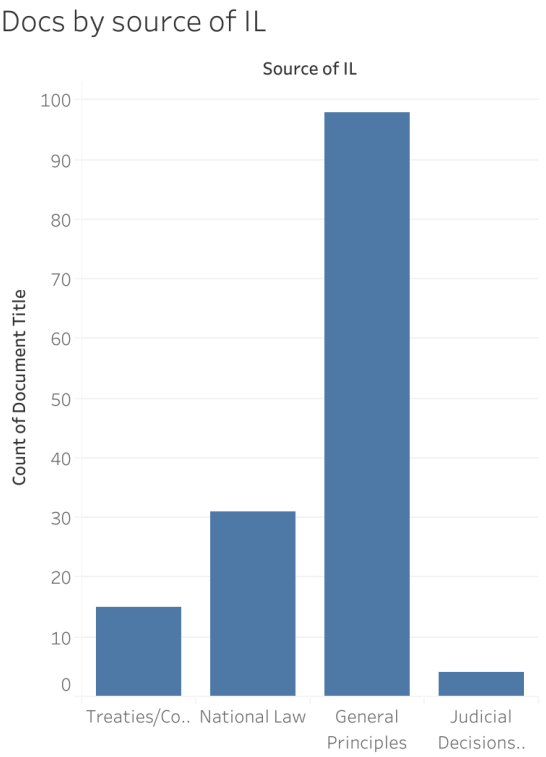


Figure 7 Documents by Source of International Law

6. Binding vs non-binding documents by region

An important dimension of the mapping involves assessing the legal force of governance instruments; specifically, whether they are binding or non-binding in nature. This distinction provides insight into the normative strategies adopted by different regions

and institutions in shaping cyberspace governance. Across all regions, the data shows a clear dominance of non-binding instruments, highlighting a global tendency to rely on soft law, voluntary frameworks, and strategic guidance rather than formalized, enforceable obligations. However, the degree and implications of this reliance vary by region.

The European Union (EU) stands out as the region with the highest proportion of binding instruments, with approximately 45% of its cyberspace-related documents carrying legal force. This reflects the EU's supranational legal architecture and its ability to issue directives, regulations, and treaties with binding effect on its member states, such as the General Data Protection Regulation (GDPR) and NIS Directive on cybersecurity.

ASEAN, by contrast, has a moderate binding ratio; with around 37.5% of its instruments being legally binding. However, what is more notable is the high absolute number of documents (nearly 90 in total), showing ASEAN's growing engagement in digital governance. While ASEAN lacks the strong supranational enforcement mechanisms of the EU, it has nevertheless produced binding agreements like the e-ASEAN Framework Agreement and ASEAN Agreement on Electronic Commerce, indicating a pragmatic mix of soft law and legal harmonization.

The United Nations demonstrates the lowest ratio of binding instruments, with approximately 95% of its documents being non-binding. This heavy reliance on soft law reflects both the political constraints of the UN system and the consensus-based nature of its outputs. Most UN instruments in the dataset, such as General Assembly resolutions, Group of Governmental Experts (GGE) reports, and Human Rights Council guidelines, fall into the category of normative declarations and voluntary codes of conduct, which nonetheless play a key role in agenda-setting and confidence-building.

This distribution underscores a core dynamic of cyberspace governance: while binding law remains limited, non-binding instruments serve as critical tools for norm diffusion, capacity-building, and regional adaptation. The contrast in legal form across regions also illustrates the pluralistic and asymmetrical nature of global cyberspace governance; adding empirical support to claims of regime fragmentation and the emergence of regionally distinct governance logics.

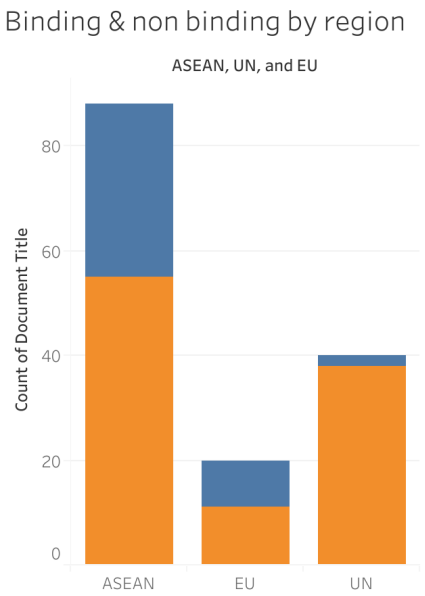


Figure 7 Documents by binding and non-binding nature

7. Documents by type

The mapping also disaggregates cyberspace governance instruments based on their document type, offering further insight into the legal form, policy intent, and strategic function of each instrument. This classification is especially relevant for understanding the binding authority and regulatory modality of different governance tools.

Out of the 148 documents in the dataset, 44 are classified as binding legal instruments, including various forms of domestic and international law. These consist of Acts (18), Regulations (6), Laws (6), Conventions (4), Directives (3), and Agreements (2), alongside Presidential/Ministerial Regulations, Decrees, and Bills; most of which were adopted at the national level, particularly by ASEAN Member States. These types of instruments serve to establish enforceable obligations, reflect formal legislative processes, and often function under the "Law" modality of Lessig's theory.

By contrast, the majority; 104 documents, are non-binding in nature. These are dominated by document types such as Reports (20), Cooperation agreements or memoranda (14), Resolutions (12), Strategy documents (11), and Communiqués (5). These instruments typically do not impose legal obligations, but rather articulate shared

principles, institutional commitments, or strategic directions. Their prevalence demonstrates a clear reliance on soft law and informal mechanisms of influence, particularly in the domains of international and regional cooperation.

The data illustrates the global preference for flexible and adaptive instruments, especially in response to the rapid evolution of digital technologies and cross-border cyber threats. Reports and strategies, in particular, often set the discursive and normative agenda for future action without committing states or institutions to specific legal duties.

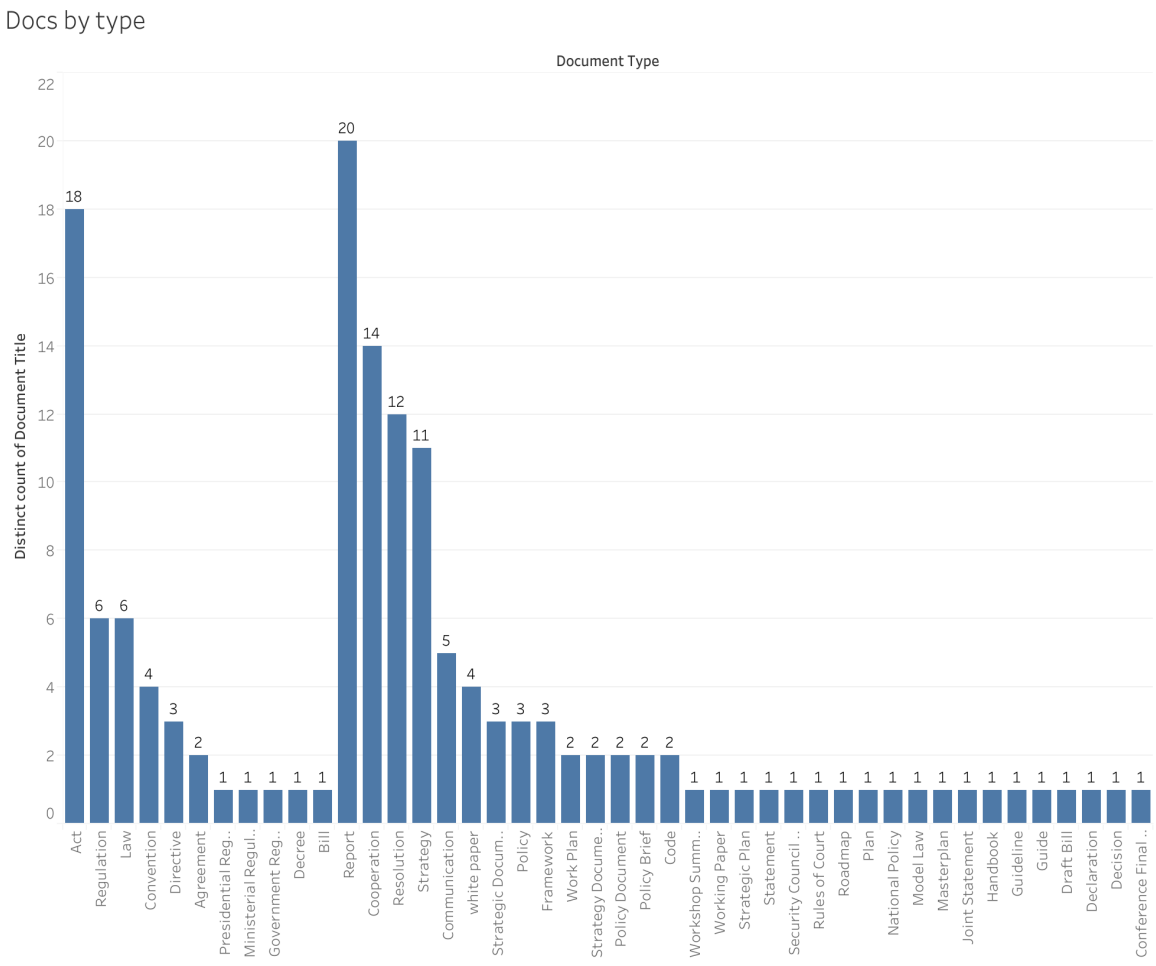


Figure 8 Document by type

This distribution of document types reinforces broader patterns noted earlier: **binding** authority remains relatively limited in the global cyberspace regime, while non-binding tools serve as the dominant medium for policy coordination, norm diffusion, and capacity

building; especially in multilateral settings such as the UN or ASEAN. These findings further underscore the asymmetry between law-making capacity and normative ambition, which lies at the heart of contemporary regime fragmentation and the gradual shift toward regional governance innovation, particularly in the Global East.

8. Governance function and type

To provide a multidimensional understanding of how cyberspace is governed, this study classifies governance instruments not only by their policy intent but also by the form and mechanism through which regulation is exercised. Two intersecting frameworks were used for this purpose. First, drawing from the UNIDIR Cyber Policy Portal, documents were categorized by governance function; distinguishing whether an instrument primarily serves a policy-setting, structural, legislative, or cooperative role.[326] Second, the instruments were analysed through a regulatory theory lens, identifying the dominant governance type as either legal, institutional, or algorithmic.

In terms of governance function, the largest portion of documents (61 in total) are classified under policy. These include national cybersecurity strategies, institutional position papers, and implementation frameworks, all designed to articulate a states or institution's vision and priorities for cyberspace governance. These documents reflect the normative ambition of policymakers and the effort to frame agendas even in the absence of binding authority.

Legislation is the second most prevalent function, with 48 documents representing national laws, EU regulations and directives, and formal legal instruments adopted by states or international organizations. These instruments provide a legal basis for cyber operations and security, ranging from data protection laws to cybercrime legislation. The prevalence of legal instruments signals an increasing reliance on rule-based governance, particularly at the national and regional levels.

The cooperation function accounts for 20 documents, including bilateral and multilateral agreements, joint statements, and activity-based frameworks. These instruments often have a soft-law character, but they play a crucial role in facilitating cross-border trust, interoperability, and capacity building; especially in forums where binding commitments may be politically difficult to achieve.

[326] Glossary, UNIDIR Cyber Policy Portal, https://cyberpolicyportal.org/glossary

Meanwhile, structure-related documents number 19, and focus on institutional arrangements such as the establishment of national Computer Emergency Response Teams (CERTs), the designation of key cyber policy positions, and the creation of specialized agencies. These reflect the operational dimension of governance; how authority is allocated, who is responsible for implementation, and what institutional capacity is in place to respond to cyber threats.

Complementing this functional mapping is an analysis of the type of governance mechanism employed. Here, the most dominant category is institutional governance, encompassing 88 documents. These include strategies, resolutions, cooperation frameworks, and communiqués that emerge from international organizations, regional bodies, and national governments. Institutional governance reflects the political and procedural dynamics of rulemaking; often involving multistakeholder input, consensus-building, and norm diffusion, rather than legal compulsion.

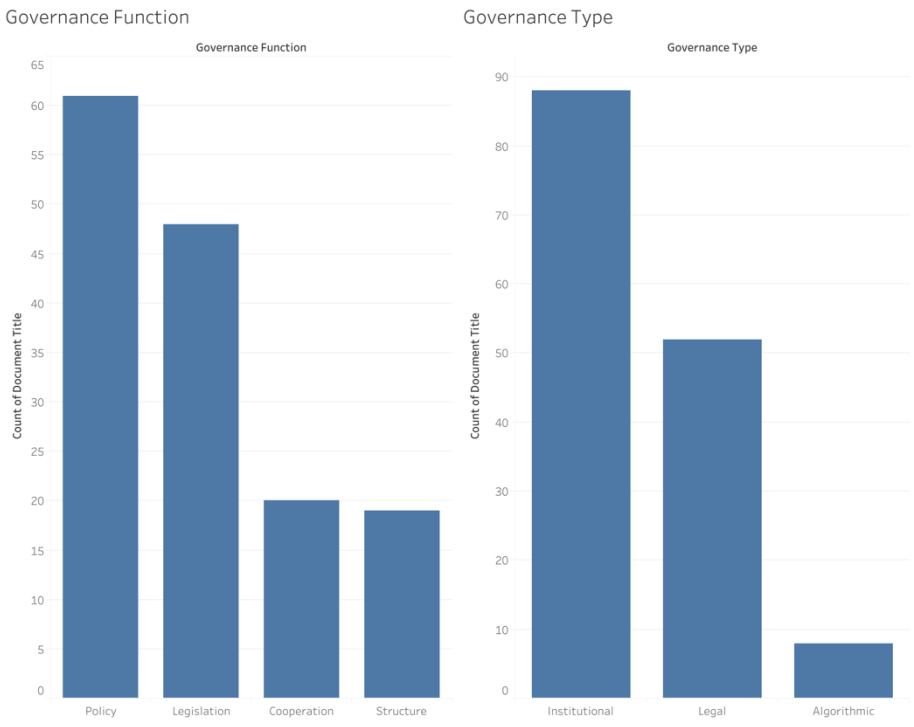


Figure 9 Documents by governance function and type

Legal governance, comprising 52 documents, captures the traditional rule-of-law approach, where states or institutions impose obligations through statutes, treaties, or judicial decisions. These instruments are binding in nature and backed by enforcement or

compliance mechanisms. Legal governance is particularly salient in the EU context, where supranational structures enable the imposition of uniform rules, as well as in national settings where cybersecurity laws are being codified.

Although less frequent, algorithmic governance appears in 8 documents and represents a distinct but critical layer of control. In this type, regulatory logic is embedded directly into technical infrastructure, through software code, encryption protocols, or system architecture. Rather than relying on institutions or formal law, algorithmic governance exerts control by constraining possible actions through design. It reflects the idea, famously articulated by Lawrence Lessig, that "code is law."[327] While underrepresented in quantitative terms, these instruments are highly influential in practice, particularly in platform governance, network security, and digital authentication systems. Together, the analysis of governance function and type illustrates the hybrid and layered nature of cyberspace governance.

Policy and institutional approaches dominate in terms of frequency, reflecting the importance of agenda-setting and soft coordination. At the same time, legal instruments play an essential role in codifying standards and setting enforceable norms, while the emerging category of algorithmic governance points to the growing power of technological architecture in shaping digital behaviour. These distinctions provide critical insight into the fragmented yet interdependent nature of regulatory authority in cyberspace and set the stage for further analysis on modality dominance, regional divergence, and the potential easternisation of global cyber norms.

9. Scope of governance

An essential component of this mapping exercise is the categorization of each document's main and supporting scope of governance; defined by the thematic policy area it addresses. This classification captures not only the regulatory focus of each instrument but also the overlapping and intersecting issues that characterize cyberspace governance. The scope categories are based on the "Mapping of International Internet Public Policy Issues" report developed by the Commission on Science and Technology for Development (CSTD) at its Eighteenth Session, following a recommendation from the United Nations

[327] Lessig, Code, 1

Economic and Social Council (ECOSOC).[328] This framework divides internet-related governance issues into seven broad clusters: (1) Infrastructure and standardization, (2) Security, (3)Human rights, (4) Legal, (5) Economic, (6) Development, (7) Sociocultural issues

Using this structure, each governance instrument in the dataset was analysed for both its main scope and any supporting scope(s). This dual classification helps to surface cross-cutting relationships and policy interdependencies that characterize the fragmented landscape of cyberspace governance.

The data shows that security overwhelmingly dominates as the main scope of governance, appearing in 76 documents. This confirms the long-observed securitization of cyberspace at both national and international levels, where cybersecurity threats and defence imperatives serve as core drivers of governance efforts. These security-focused documents are evenly distributed across major institutions (UN, EU, and ASEAN), but it is worth emphasizing that ASEAN member states are particularly active contributors, with each member state producing at least one instrument focused on cybersecurity.

The second highest main scope is infrastructure and standardization, with (27 documents). These typically address technical interoperability, digital infrastructure policy, and national cybersecurity frameworks. Their prominence suggests that regulatory focus is increasingly shifting toward the architectural layer of cyberspace.

The third most frequent main scope is development (12 documents), reflecting the growing alignment of cyberspace policy with national development strategies, capacity-building goals, and the digital inclusion agenda. These instruments were led by the UN, particularly through the Groups of Governmental Experts (GGEs), followed by regional contributions from ASEAN.

Other scopes, including economy (8), human rights (6), and socio-cultural (1), are less frequent as primary scopes but gain salience when mapped as supporting scopes. When combining main and supporting classifications, deeper insights emerge into the interconnected nature of cyberspace governance.

[328] Intersessional Panel of the Commission on Science and Technology for Development, "The Mapping of International Internet Public Policy Issues Database," 2015., https://unctad.org/meeting/cstd-2014-2015-inter-sessional-panel

For example, the most frequent combined scope is security + infrastructure and standardization, appearing in 28 documents. The EU is the largest contributor to this dual focus (8 documents), but ASEAN member states also actively frame security and infrastructure together in their national policies.

The next most common combination is security + development, with the UN leading through its multilateral initiatives, followed by ASEAN (3 documents) and the EU (1 document). This reflects how developmental considerations are increasingly integrated into the security agenda in global and regional policy circles.

The reverse configuration, infrastructure and standardization as the main scope and security as the supporting one; appears in 15 documents, with the UN (8 documents) as the primary source. Interestingly, no such instruments were found from the EU, highlighting regional divergence in scope emphasis.

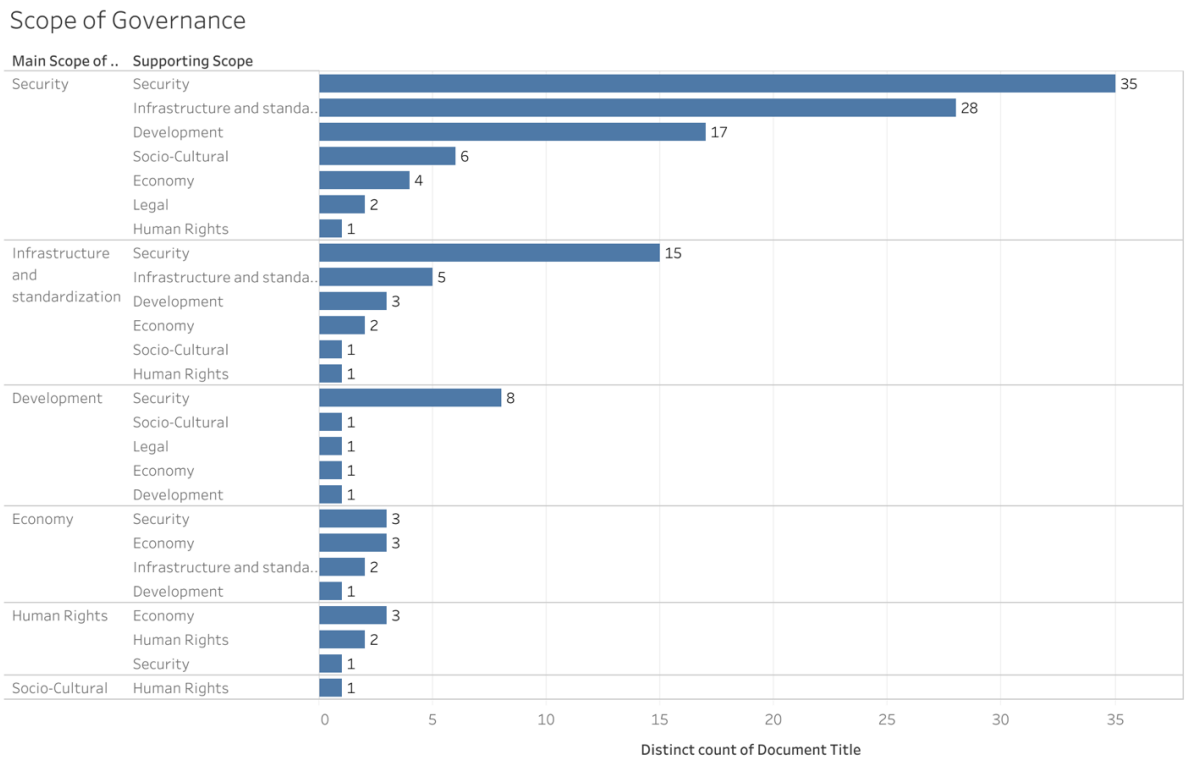


Figure 10 Documents by Scope of Governance

Other significant pairings include development (main) + security (supporting), largely from ASEAN, and infrastructure (main) + infrastructure (supporting), contributed by the UN, EU, and Brunei Darussalam.

Less common combinations such as security + economy, infrastructure + development, and human rights + economy; appear in only a handful of documents but still offer valuable insights. For example, all economy-focused instruments were contributed by ASEAN and its member states, underscoring the region's integration of digital governance with broader economic policy.

Meanwhile, human rights focused instruments appear in just six documents, with sources split across the UN, EU, and ASEAN, often accompanied by supporting scopes like economy or security. The only document with socio-cultural as the main scope, supported by human rights, came from Singapore.

Overall, this scope mapping reveals both concentrations and dispersions in cyberspace governance. While security is the undisputed focal point, a substantial number of documents span across issue areas; particularly where security intersects with infrastructure, development, or economic policy. This complex layering of policy concerns is a critical empirical indicator of functional fragmentation, which will be discussed further in later chapters. Moreover, the strong presence of ASEAN member states across multiple scope combinations reflects the region's evolving approach to multidimensional governance, blending sovereignty, development, and economic priorities into a distinct eastern normative framework.

10. Governance Modalities: Mapping Cyberspace Regulation through Lessig's Framework

Building on the conceptual foundation established in Demystifying Lessig's Theory, this section applies Lessig's four modalities: Law, Norms, Architecture, and Market, to the mapped corpus of cyberspace governance instruments. The analysis proceeds in four stages. First, the overall modality mapping establishes a benchmark by classifying all 148 documents: spanning UN, EU, ASEAN, and individual ASEAN member states, into their dominant regulatory modality. This provides a baseline distribution of constraints, interpreted in Lessig's terms as different forms of cost (legal sanction, social stigma, technical barrier, or economic limitation) and highlights how the interplay of these modalities creates the regulatory environment for cyberspace. Second, the regional mapping disaggregates the dataset to examine the UN, EU, and ASEAN separately. This reveals distinctive institutional patterns, such as the UN's norm-heavy approach, the EU's

legal assertiveness, and ASEAN's reliance on architecture and norms, that reflect each actor's mandate, governance capacity, and political culture. Third, the ASEAN member state mapping compares the regional benchmark with national-level contributions from ASEAN states. This captures vertical fragmentation within the regional governance framework and shows how national inputs shift the overall modality balance, revealing divergences between collective regional commitments and domestic regulatory priorities. Finally, the synthesis section integrates findings from all three datasets to identify cross-cutting patterns, interdependencies, and tensions between modalities. Here, the analysis explores how certain modalities reinforce or undermine others, and how modality imbalances influence both governance effectiveness and the fragmentation of international cyberspace regulation. This synthesis also provides the conceptual bridge to the following chapter's focus on fragmentation, while setting the stage for re-designing Lessig's original "pathetic dot" diagram to reflect the empirical realities uncovered in this study.

a. Overall mapping of modalities

1. Law: The Dominant Modality

The Law modality emerges as the most dominant, represented in 52 documents. This reflects the persistence of formal legal instruments, such as treaties, conventions, national laws, and regional directives, as the cornerstone of cyberspace regulation. **Both the UN and the EU contribute significantly to this category, albeit through different means**. Although the UN has very few binding instruments, its non-binding reports and strategic documents frequently invoke or align with existing legal frameworks, granting them quasi-legal character. The EU, by contrast, possesses a supranational legislative authority, enabling it to issue binding regulations and directives (e.g., GDPR, NIS Directive), which firmly anchor it in the Law modality.

Strikingly, **no ASEAN-wide instrument appears in the Law category. This aligns with ASEAN's consensus-driven, non-interventionist ethos, which**

prioritizes political alignment over legal formalism.[329] While ASEAN member states do produce national laws relevant to cyberspace, the regional institution itself has not yet advanced any binding legal framework, underscoring its continued reliance on soft coordination mechanisms.

2. **Norms: The Second Pillar**

The Norms modality accounts for 38 documents, many of which originate from the UN, particularly through the UN Groups of Governmental Experts (GGEs). Of the 38, 7 GGE-produced instruments demonstrate the UN's norm-building function, which emphasizes responsible state behaviour, confidence-building, and multistakeholder governance. **Norms are often embedded in non-binding declarations, strategic frameworks, and guiding principles; instruments that influence behaviour without legal coercion**.

In contrast to its legal assertiveness, the EU contributes only one document explicitly situated within the Norms modality: its Framework Agreement on Partnership and Cooperation with Malaysia (2022).[330] This suggests the **EU's preference for embedding norms within enforceable legal instruments, rather than treating them as stand-alone regulatory tools.**

ASEAN, meanwhile, contributes a modest but meaningful set of 6 norm-based documents, including the ASEAN Declaration to Prevent and Combat Cybercrime, various Ministerial and Leader-level Statements, and outputs from ARF and policy meetings with Japan. These instruments reflect a collective identity-building process and affirm ASEAN's increasing norm-setting role in regional cyberspace governance, albeit in non-binding form. National contributions to the Norms category; especially from ASEAN member states, primarily take the form of strategies, white papers, and defense documents, further evidencing the diffusion of values through informal mechanisms.

[329] Charter of the Association of Southeast Asian Nations, Nov. 20, 2007, 2624 UNTS 223.
[330] European Union and Government of Malaysia, Framework Agreement on Partnership and Cooperation between the European Union and Its Member States, of the One Part, and the Government of Malaysia, of the Other Part, Brussels: European Union, 2022. Available https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=legissum:464600.

3. **Architecture: Infrastructure as Regulation**

The Architecture modality appears in 21 documents, emphasizing governance by design and technical infrastructure. This includes instruments related to data governance frameworks, cybersecurity protocols, standards, and digital infrastructure planning. While the EU contributes 4 documents (including the EU Data Governance Act), and the UN adds 3 (such as UNIDIR reports and ITU conference outcomes), **most contributions come from ASEAN member states, in the form of national master plans, ICT blueprints, and digital transformation framework**s. These are typically non-binding but nonetheless enforce behavioural outcomes through their technical specifications.

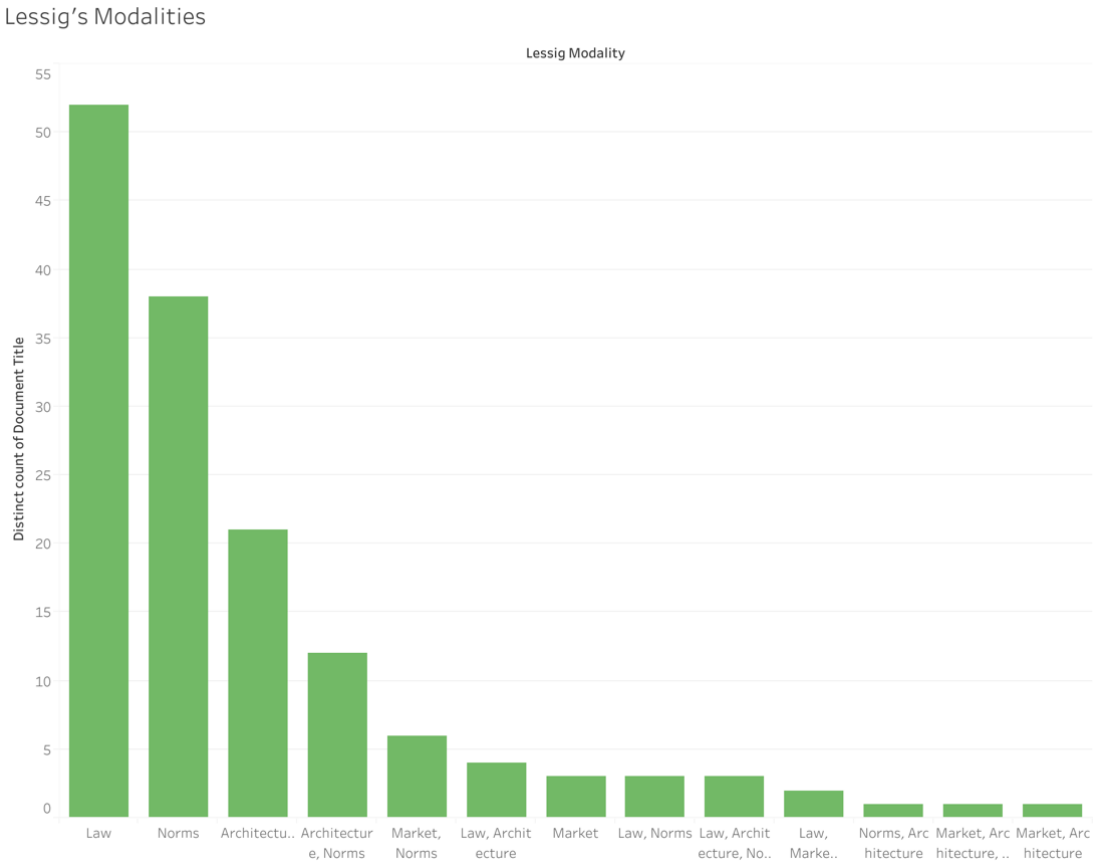


Figure 11 Documents generally mapped by LRT

4. **Market: The Least Emphasized Modality**

Surprisingly, **the Market modality is the least represented, with only 3 standalone instruments, all of which come from ASEAN member states; notably Singapore and Malaysia**. These instruments focus on digital economy policies, data governance initiatives, and private sector engagement frameworks, highlighting how market actors shape governance through trade, standards, and platform control. The limited count may reflect either data source bias (as formal market instruments are less likely to appear in legal or policy databases) or an underdeveloped regulatory engagement with market actors, especially outside the EU and US contexts.

b. Inter-modality observation

While Lessig's four modalities: Law, Market, Architecture, and Norms, are analytically distinct, many cyberspace governance instruments operate across multiple modalities simultaneously, reflecting the complex, layered nature of digital regulation. These hybrid instruments illustrate how regulatory authority in cyberspace is often exercised not through a single channel, but through overlapping legal mandates, economic structures, infrastructural designs, and normative frameworks.

One of the most prominent hybrid categories is the combination of **Architecture and Norms**, represented by 12 documents. **This pairing underscores how technical standards and system design choices are embedded with normative assumptions**: about privacy, accessibility, sovereignty, or security. **The EU is the largest contributor in this category, with six instruments that blend architectural control (e.g., technical interoperability mandates) with high-level value commitments** (e.g., rights-based access, accountability standards). ASEAN follows closely with five documents, such as digital masterplans and national strategies that incorporate technical specifications for data flows, cybersecurity infrastructure, or digital ID systems, while also referencing ASEAN principles on responsible behaviour and regional trust. The UN contributes a single document to this category, highlighting the relative scarcity of technical-normative integration at the multilateral level.

Another notable hybrid is Market and Norms, with six instruments, nearly all of which originate from ASEAN. These include policy frameworks such as the ASEAN

Framework on Personal Data Protection,[331] the Framework on Digital Data Governance,[332] and the e-ASEAN Framework Agreement.[333] These instruments are not merely economic initiatives; they embed normative values such as data ethics, regional trust, and cross-border accountability into economic infrastructure. In this sense, they reflect a distinctive approach to governance in Southeast Asia, where market-building is simultaneously used as a tool for norm diffusion, particularly in the absence of enforceable legal authority.

The combination of Law and Norms, though rarer, is particularly significant. With three documents (two from the UN, one from the EU), this pairing illustrates how formal legal instruments often derive legitimacy from prevailing norms or are constructed in response to widely accepted ethical frameworks. For instance, UN cybercrime resolutions that emphasize due process or human rights protections demonstrate how law can be a vessel for norm consolidation. Similarly, EU instruments often embed fundamental rights within the text of legal directives, illustrating a model of value-based legalism in cyberspace governance.

Equally represented are instruments combining Law and Architecture, all three of which come from the UN. These documents focus on how technical infrastructures such as digital routing systems or CERT frameworks, are tied to legal mandates and international agreements. This category reinforces the notion that infrastructural governance is not purely technical, but increasingly embedded within broader rule-based frameworks, especially in areas like international telecommunications and cyber incident response.

Two particularly expansive instruments fall under the Law + Market + Norms category. The first is the EU Cybersecurity Strategy, which not only establishes binding legal standards for cybersecurity and resilience but also engages the private sector through public-private partnerships and articulates a clear normative vision grounded in democratic values and rights. The second is ASEAN's Framework for Negotiating

[331] ASEAN Telecommunications and Information Technology Ministers (TELMIN), ASEAN Framework on Personal Data Protection, Singapore: ASEAN, 2016.
[332] Association of Southeast Asian Nations (ASEAN), ASEAN Framework on Digital Data Governance, Jakarta: ASEAN, 2018.
[333] e-ASEAN Framework Agreement, Nov. 24, 2000, 2216 UNTS 233,

the Digital Economy Framework Agreement (DEFA),[334] which incorporates legal commitments, market integration goals, and references to responsible data governance. These comprehensive instruments reflect a mature, integrated approach to cyberspace governance, in which multiple regulatory forces are mobilized simultaneously.

Finally, three unique documents represent more complex hybrid configurations:

- The "Report of the High-Level Panel on Digital Cooperation"[335] falls under Norms + Architecture, highlighting how system design principles (such as decentralization or interoperability) are infused with normative ideals like inclusivity and digital trust.
- The "ASEAN Digital Masterplan"[336] exemplifies Market + Architecture + Norms, demonstrating how ASEAN envisions regional digital integration through infrastructure investment, economic alignment, and ethical guidelines.
- The UN's report on "Private Sector Engagement in Responding to the Use of ICT for Terrorist Purposes"[337] exemplifies a Market + Architecture pairing, showing how economic actors and technical systems are mobilized in tandem to address digital threats, without relying on formal law.

These hybrid modalities are crucial for understanding the evolving complexity of global cyberspace governance. They reveal how regulation is rarely exercised through a singular channel, and how institutions often blend modalities to enhance legitimacy, effectiveness, or adaptability. Moreover, the regional variation in hybrid usage (for example, ASEAN's focus on Market-Norm and Architecture-Norm combinations or the EU's preference for Law-cantered hybrids) offers further evidence of regulatory divergence and the emergence of regionally distinct governance logics.

[334] ASEAN Economic Community Council (ACC) and ASEAN Coordinating Committee on Electronic Commerce (ACCEC), Framework for Negotiating the ASEAN Digital Economy Framework Agreement (DEFA), Jakarta: ASEAN, 2023.
[335] United Nations, High-Level Panel on Digital Cooperation, The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation., New York: United Nations, 2019.
[336] Association of Southeast Asian Nations (ASEAN). *ASEAN Digital Masterplan 2025, Jakarta: ASEAN, 2021.
[337] United Nations, Counter-Terrorism Executive Directorate (CTED), Private Sector Engagement in Responding to the Use of ICT for Terrorist Purposes, New York: United Nations, 2021.

Overall, this modality mapping reveals a clear regulatory asymmetry**: Law and Norms dominate, Architecture is rising, and Market is marginal**. **Regionally, the UN leads in norm diffusion and hybrid frameworks, the EU Favors legal-regulatory instruments, and ASEAN shows growing initiative in norm-building and infrastructure-based governance**; **with limited legal authority but expanding strategic vision**. These findings further support the emerging narrative of regional divergence and set the foundation for the following analysis on regime complexity, modality layering, and the potential easternisation of international cyberspace governance.

c. Mapping of modalities by region

Building on the overall benchmark analysis, which aggregated all 148 documents from UN, EU, ASEAN, and individual ASEAN member states, this section focuses exclusively on regional-level instruments produced by the UN, EU, and ASEAN. This filtered view removes national-level variation, providing a clearer picture of how international and regional institutions prioritize regulatory modalities in cyberspace governance. In Lessig's terms, the "pathetic dot" of international cyberspace governance is shaped here by the regulatory forces of Law, Norms, Market, and Architecture, each operating at institutional and cross-institutional levels. Comparing this to the benchmark reveals significant shifts in modality dominance once national-level contributions are removed.

1. **Norms as the predominant regional regulatory tool**

   When focusing exclusively on UN, EU, and ASEAN-level instruments, norms become the most prominent modality, displacing law from its benchmark dominance. **The UN's 15 documents (many from GGEs) highlight its role as a global norm entrepreneur, while ASEAN's six documents reflect its consensus-based, non-binding approach to governance. The EU's single entry signals its tendency to embed normative content within binding legislation rather than standalone normative frameworks.** In Lessig's terms, these instruments rely on ex-post

social regulation, where compliance is driven by reputation, legitimacy, and peer pressure rather than legal sanction.

2. **Legal Authority seconds in regional contexts**

   Law remains central but falls to second place with 18 documents (UN 10, EU 8). The UN's legal contributions often take the form of non-binding resolutions tied to existing treaties, demonstrating how law can be reinforced by normative legitimacy. The EU, in contrast, operates with binding authority through regulations and directives, reflecting its supranational capacity to harmonize member state obligations. **ASEAN's absence confirms its reluctance to advance binding regional legal frameworks, reinforcing its reliance on softer governance tools**.

3. **Embedding norms into infrastructure**

   The Architecture × Norms hybrid emerges strongly at 12 documents (EU 6, ASEAN 5, UN 1). Here, governance is exercised by embedding behavioural expectations directly into technical design. EU initiatives like the Data Governance Act pair interoperability and security requirements with transparency principles, while ASEAN's ICT master plans set both infrastructure and ethical use guidelines. Lessig's theory explains this as a fusion of ex-ante technical constraints with the value-laden guidance of norms.

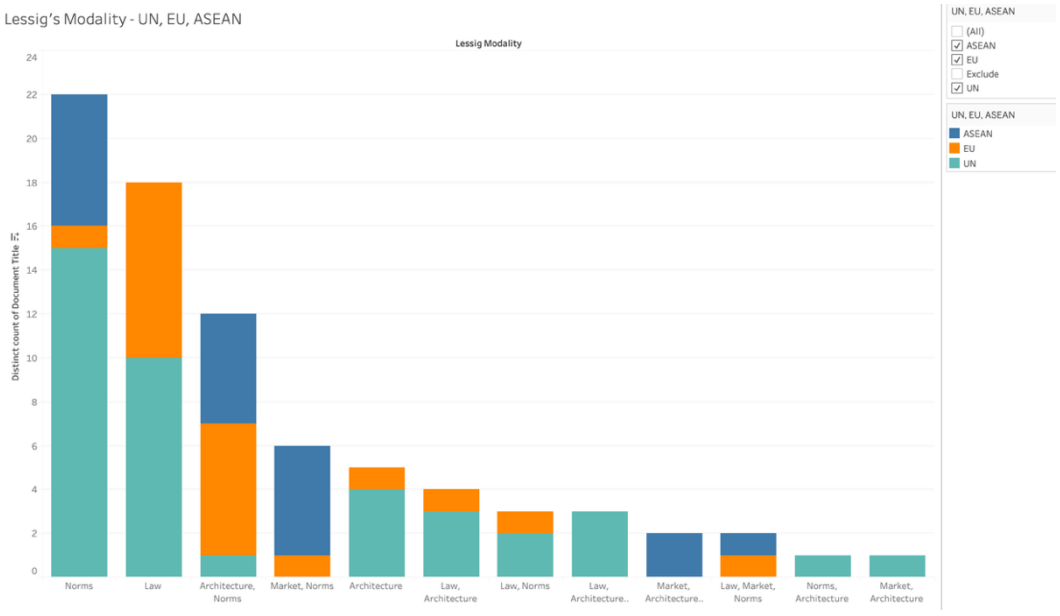


Figure 12. Documents Mapped by LRT based on Region

4. **Aligning market incentives with normative commitments**

   The Market × Norms hybrid appears in six documents (ASEAN 5, EU 1), with ASEAN leading through digital economy strategies, public–private partnerships, and responsible data governance initiatives. These frameworks incentivize compliance by aligning commercial benefits with shared values, exemplifying Lessig's notion that market structures can be deliberately shaped to reinforce norms. The EU's limited presence here reflects its preference for embedding market governance within enforceable legal instruments.

5. **Complex hybrid modalities**

   Other modality combinations illustrate the interdependence Lessig describes. Pure Architecture (UN 4, EU 1) remains rare, suggesting that technical design is typically paired with legal or normative frameworks. Law × Architecture (UN 3, EU 1) and Law × Norms (UN 2, EU 1) indicate deliberate integration of legal authority with design or social consensus. Triple hybrids such as Law × Architecture × Norms (UN 3) demonstrate multi-layered regulatory strategies, while niche pairings like Market × Architecture or Norms × Architecture show targeted regulation through both technical and non-technical constraints.

d. National-level inputs: How ASEAN Member States Reshape the Modality Balance

1. **Legal instruments resurge with national lawmaking capacity**

   When ASEAN member states are added back into the corpus, Law again becomes the top modality; reproducing the benchmark pattern and reversing the norms-led profile seen in the "regional-only" cut. **The key driver is the substantial contribution of national instruments from ASEAN countries (34 documents).** In Lessig's terms, this confirms that ex post, sanction-backed regulation is most active and relevant where

states possess clear legislative competence and enforcement capacity. National parliaments and regulators can pass statutes, amend sectoral codes, and mandate compliance in ways regional bodies (especially consensus-based ASEAN) typically cannot. The result is a vertical rebalancing: once domestic lawmaking enters the picture, the governance ecology shifts toward formal legal constraint, with norms and architecture acting more as supporting modalities than primary ones.

2. **Normative governance expands, but as a complement to law**

   With member states included, Norms remain the second pillar, and ASEAN states now slightly edge the UN (16 documents). Strategically, these are national strategies, white papers, and defense or policy statements that diffuse expectations about "responsible" behaviour, incident response, and cooperation; ex post social constraints that travel via legitimacy and reputation rather than penalties. Read through Lessig, this shows how **domestic actors use norms to buttress law: norms frame acceptable conduct and socialize agencies and firms into compliance cultures, while statutes and regulations supply the teeth.** Compared to the regional-only view (where norms led), the addition of national material reveals interdependence: norms flourish, but their practical effect is amplified because law is now close at hand.

3. **Governing by design scales up the national layer**

   Architecture climbs as ASEAN member states contribute 16 documents, outnumbering UN and EU entries. Much of this output takes the form of ICT master plans, cybersecurity standards, data governance frameworks, and sectoral technical blueprints. In Lessig's model, architecture regulates ex ante by making certain behaviours easy or hard; through authentication requirements, network segmentation, logging baselines, or protocol choices. The strong national showing reflects two dynamics. First, many technical instruments sit at the boundary between cyberspace governance and more general statutory domains (telecommunications, criminal procedure, critical-infrastructure protection), so architectural

mandates often ride alongside or within those laws. Second, the work of implementation; procurement specifications, configuration baselines, certification schemes, naturally occurs at the domestic level, where states can standardize systems in public networks and nudge private adoption. The upshot is a clearer Law ↔ Architecture reinforcement loop: statutes compel controls; controls make compliance automatic.

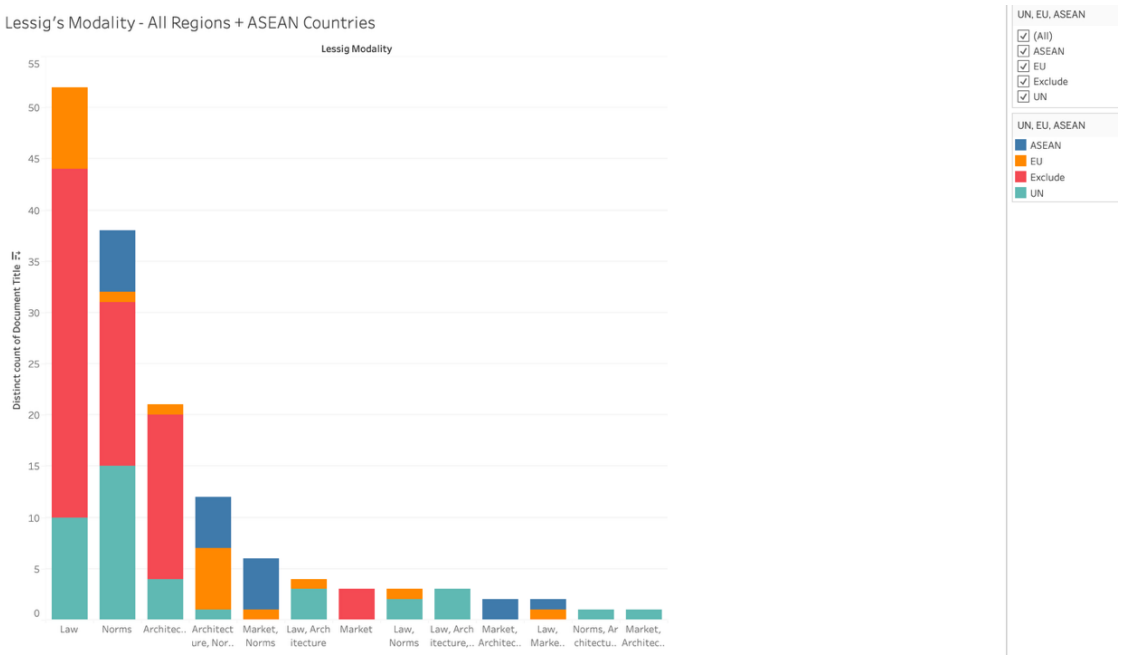


Figure 13 Documents mapped by LRT - AMS Included

4. **Market instruments remain sparse- but they are national**

As in the benchmark, Market is the least emphasized modality, and here it appears only in ASEAN member states (3 documents); notably Singapore and Malaysia, covering a National Policy on Industry 4.0, a cybersecurity certification guide, and an operational-technology (OT) cybersecurity competency framework. In LRT terms, these are ex ante economic constraints that steer behaviour via pricing, eligibility, or capability requirements (e.g., certification as a market access condition, or skills frameworks that shape labour supply). Their national locus makes sense: market structure, industrial policy, and skills pipelines are domestic levers, and ASEAN's regional layer lacks both the mandate and

instruments to operationalize them. The scarcity also underscores a documentation bias; market rules often live in trade, competition, and industrial policy channels that are less visible in legal/policy repositories, yet the pattern is consistent with the regional cut: market regulation is not the principal tool in international cyberspace governance.

5. **What the national re-insertion reveals**

   Bringing ASEAN member states back into the analysis shows how scale redistributes modality weight. **Law surges because the capacity to punish is clearest domestically**; **Architecture grows because implementation lives close to systems**; **Norms expand but mainly as legitimating and socializing companions to law and design**; **Market appears selectively where industrial and skills policy bite**. This is the Lessig interdependence thesis in practice: national law enables and demands Architecture; Norms make both governable within organizations and professions; Market occasionally aligns incentives but is not the dominant lever. The contrast with the regional-only view (norms-led) exposes vertical fragmentation: regional actors coordinate principles; states operationalize them through statutes and systems. Where those layers align, regulation is coherent; where they diverge, gaps will exist; strong national technical baselines without shared regional interoperability, or rich UN norms without matching domestic enforcement.

e. Synthesis: Modality balance, Interdependence, and Fragmentation Across Scales

The sequential mapping of Lessig's four modalities across the benchmark, regional-only, and national-inclusive datasets reveals a dynamic regulatory landscape in international cyberspace governance: one in which the balance between Law, Norms, Architecture, and Market shifts depending on the institutional scale under examination. In Lessig's terms, the "pathetic dot" of cyberspace governance is constrained by the same four regulators, but the relative weight and interaction of these constraints change

as the locus of authority moves from global and regional bodies to domestic governments.[338]

1. **From Legal Dominance to Normative Leadership — *Vice versa***

   In the benchmark view (all documents, all levels), Law clearly dominates. This is driven not by the UN or ASEAN at the institutional level, but by the legislative capacity of states (especially ASEAN member states) whose 34 national documents anchor the dataset in formal, sanction-backed regulation. However, when the scope is narrowed to regional-only instruments (UN, EU, ASEAN), Norms overtake Law, underscoring that international and regional bodies; particularly the UN and ASEAN, rely heavily on consensus, peer pressure, and legitimacy rather than binding compulsion. Reintroducing national-level instruments reverses this shift: Law surges back into dominance, revealing that legislative competence is the strongest single driver of legal modality weight. This swing between Law and Norms across scales is a textbook example of vertical fragmentation, where the same governance system looks radically different depending on which layer of authority is examined.

2. **Architecture as a Scale-Sensitive Modality**

   Across all views, Architecture; governance by technical design, remains secondary to Law and Norms, but its profile changes markedly with scale. At the regional level, Architecture appears primarily through hybrids with Norms (Architecture × Norms), reflecting design principles embedded with value commitments (e.g., EU interoperability rules with transparency norms, ASEAN ICT master plans with responsible-use guidelines). At the national level, however, Architecture expands substantially, driven by ICT master plans, cybersecurity standards, and data governance frameworks that states can directly implement. This confirms Lessig's interdependence thesis: legal authority at the national level mandates architectural controls, and those controls in turn make

[338] Lessig, Code, 121-123

legal compliance automatic; forming a Law–Architecture reinforcement loop largely absent at the regional layer.[339]

3. **Market: Marginal but Targeted**

   In all three cuts, Market remains the least represented modality, and almost exclusively appears in the national-inclusive datasets. This pattern reflects both mandate limitations (regional bodies lack authority over industrial and competition policy) and visibility bias (market rules are often housed in trade and industrial policy channels not captured in cyberspace governance repositories). Where it does appear; Singapore's Industry 4.0 strategy, Malaysia's cybersecurity certification and OT competency frameworks, it functions as an ex ante economic constraint that aligns market access, skills, and investment flows with cybersecurity objectives. At the regional scale, Market × Norms hybrids are ASEAN's niche: aligning economic integration with trust-building and ethical data governance.

4. **Hybrid Configurations and Interdependence**

   Hybrid modalities (documents that combine two or more of Lessig's regulators) are not peripheral but central to cyberspace governance across all scales. The Architecture × Norms combination is a constant, though its composition changes: EU-led at the regional scale, nationally led in Southeast Asia. The Market × Norms hybrid is almost entirely an ASEAN phenomenon, both regionally and nationally, and represents a distinctive Southeast Asian approach to embedding normative values into economic frameworks. Law × Norms and Law × Architecture appears more frequently at the UN level, where legal authority is often coupled with value framing or technical implementation to enhance legitimacy and compliance. These hybrids embody Lessig's observation that constraints are distinct yet interdependent; each modality can support, undermine, or enable others.

[339] Lessig, Code,119-126

5. Fragmentation in Modality Balance

The three datasets together demonstrate that fragmentation in cyberspace governance is not only thematic or institutional but modal. At the regional layer, governance is norm-heavy, legally thin, and technically integrated via hybrid tools. At the national layer, governance is law-heavy, technically operationalized, and only selectively market-oriented. These differences create vertical mismatches: norms without enforcement at the top, legal mandates without cross-border coordination at the bottom, and architectural solutions that lack regional interoperability. Where modalities align across layers, such as UN norms embedded into national laws; the system is coherent; where they diverge, governance gaps emerge.

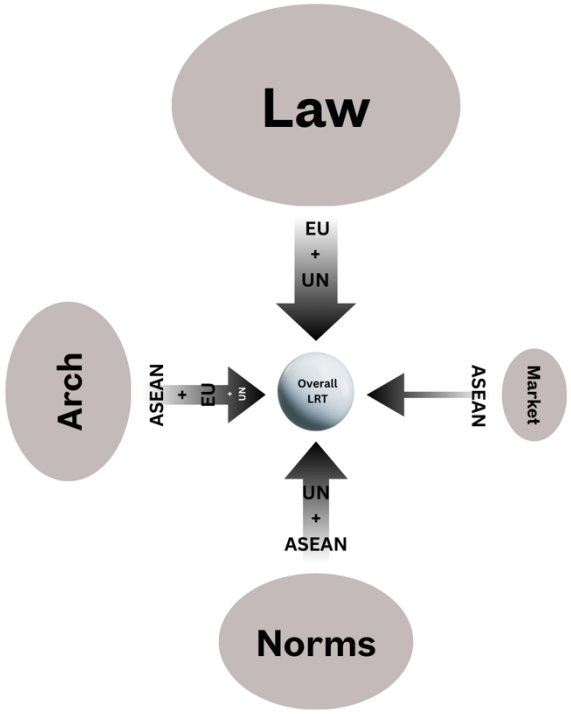


Figure 14 – Overall mapping of LRT modalities

Law dominates (EU + ASEAN states), followed by Norms (UN + ASEAN). Architecture is led by ASEAN with some EU input, while Market is least represented, appearing only in ASEAN.

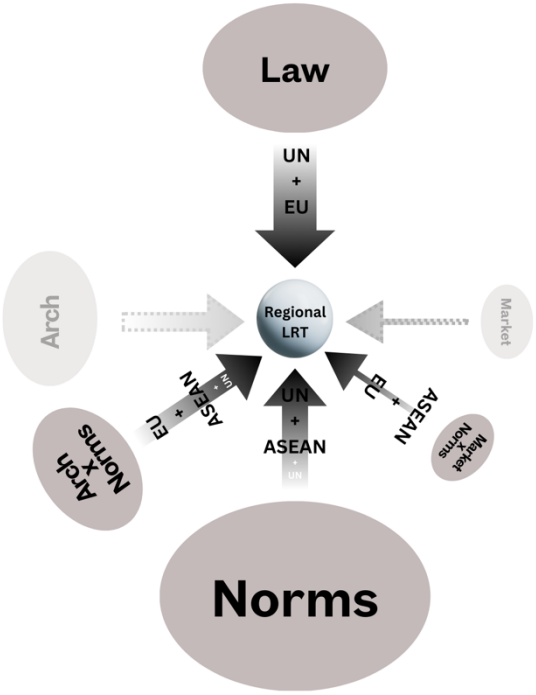


Figure 15 Regional Mapping of LRT Modalities

In the regional context, Norms dominate, with the UN contributing most and ASEAN adding several instruments, while the EU plays only a minor role. Law comes next, driven by UN resolutions and EU directives. Architecture shifts into hybrid form (Architecture × Norms), led by the EU and ASEAN with little from the UN. Market also appears only in hybrid form (Market × Norms), where ASEAN contributes the majority and the EU provides limited support.

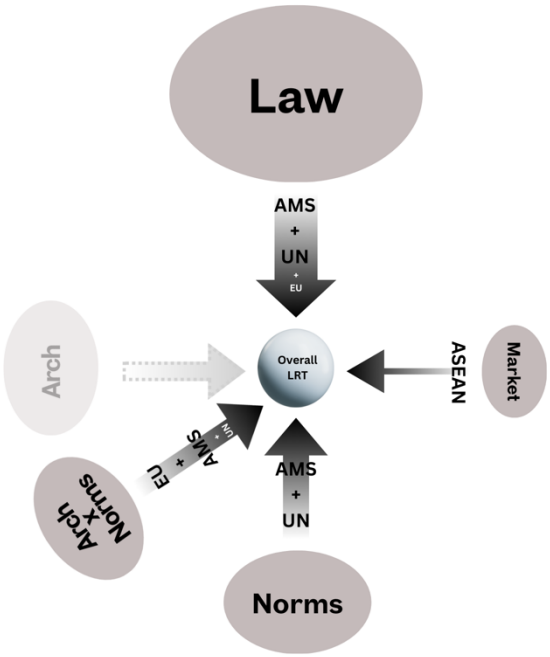


Figure 16 Overall LRT Modality mapping - AMS Included

When ASEAN member states are added, Law regains dominance, reflecting extensive national legislation on data protection and cybersecurity. Norms remain strong, with strategies and declarations diffused across both regional and national levels. Architecture expands significantly at the domestic layer through ICT masterplans and technical standards, creating a Law–Architecture reinforcement loop. Market, though still the least represented, appears through national industrial and digital economy policies, almost exclusively from Singapore and Malaysia.

B. Fragmentation in Cyberspace Governance

The governance of cyberspace has evolved into a deeply fragmented and complex regime landscape, shaped by overlapping institutions, contested norms, and competing regulatory visions. Rather than a coherent legal regime, the global order of cyberspace is best described as a regime complex; a dispersed and non-hierarchical arrangement of legal, technical, and political frameworks involving states, international organizations, private actors, and civil society.[340] This complexity has emerged not only from the rapid expansion of cyberspace into diverse policy domains (such as trade, security, human rights, and infrastructure), but also from the growing divergence in how key actors define and pursue cyber governance.

At its core, this fragmentation operates along multiple and intersecting dimensions.[341] Institutionally, global cyber governance is distributed across various overlapping bodies; from the United Nations and regional organizations (such as the EU and SCO) to private standard-setting bodies like the IETF and ICANN. As Raymond (2016) conceptualizes, the cyber domain resembles a "nested set of club goods," governed through diverse and often uncoordinated authority structures. This structural decentralization gives rise to **vertical** fragmentation, where national, regional, and international mechanisms coexist without a clear hierarchy or enforcement mechanism; resulting in policy contradictions and jurisdictional frictions.[342]

Thematically, the expansion of cyberspace governance into domains beyond core technical infrastructure, such as content regulation, economic policy, and human rights, has further multiplied the actors and interests involved.[343] This thematic diversification amplifies fragmentation, as institutions with vastly different mandates engage in cyber-related norm production, often with minimal coordination. Such proliferation increases the potential for institutional redundancy, normative inconsistency, and scope overlap.

[340] Kouliopoulos, Report: Case Study of Cyber Governance, 5
[341] Alter and Meunier, The Politics of International Regime Complexity, 13
[342] Raymond, Managing Decentralized Cyber Governance, 125
[343] Nye, The Regime Complex, 5

A second axis of fragmentation concerns normative and legal contestation. As Zwingel (2022)[344] and Stadnik (2017)[345] show, key global actors operate based on incompatible strategic narratives and legal models. Liberal democracies (e.g., the EU and US) emphasize multistakeholder participation, open internet principles, and human rights as foundational cyber norms. In contrast, authoritarian powers such as Russia and China promote a sovereigntist, state-centric conception of cyber governance grounded in information control and strategic stability. These conflicting ideational positions drive normative fragmentation, as states engage in forum shifting, promote competing standards, and resist universal agreements. This dynamic is compounded by legal fragmentation, as parallel norm-setting efforts produce diverging interpretations of binding law; especially in areas such as cybercrime, attribution, and the applicability of international humanitarian law.

The regime complex is further complicated by what Raymond and Sherman (2024) describe as a "double transformation" of multilateralism, wherein authoritarian states adopt formal multilateral procedures to push illiberal norms while liberal actors reconfigure multilateralism through hybrid multistakeholder approaches. This procedural divergence reinforces modality-based fragmentation, as governance practices increasingly diverge in their reliance on law, norms, technical architectures, and market mechanisms; mirroring the four modalities theorized by Lessig.[346]

Collectively, these dynamics point to a fragmented governance ecosystem in which institutional mandates, legal interpretations, normative foundations, and regulatory modalities frequently collide. The result is a cyberspace regime that lacks coherence, consistency, and enforceability, posing critical challenges to global stability, norm convergence, and effective policy coordination.

The following section presents empirical evidence of this fragmentation, organized across four analytical axes: (1) **institutional fragmentation**, reflected in the diversity and overlap of governing bodies; (2) **thematic fragmentation**, indicated by the uneven expansion of

[344] André Barrinha and Rebecca Turner, "Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India," *Contemporary Security Policy* 45, no. 1 (January 2, 2024): 72–109, https://doi.org/10.1080/13523260.2023.2266906.
[345] Ilona Stadnik, "What Is an International Cybersecurity Regime and How We Can Achieve It?," *Masaryk University Journal of Law and Technology* 11, no. 1 (June 30, 2017): 129–54, https://doi.org/10.5817/MUJLT2017-1-7.
[346] Mark Raymond and Justin Sherman, "Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice," *Contemporary Security Policy* 45, no. 1 (2024): 110–40, https://doi.org/10.1080/13523260.2023.2269809.

cyber governance across issue areas; (3) **vertical fragmentation**, seen in the misalignment of governance across national, regional, and international levels; and (4) **modality-based fragmentation**, captured through the differential application of Lessig's four regulatory modalities: law, norms, market, and architecture. This multi-dimensional mapping provides a grounded understanding of how fragmentation manifests in practice and how it reshapes the evolving global order of cyberspace governance.

1. Institutional fragmentation: cross-regional patterns and functional gaps

The institutional mapping reveals that each regime/region possesses a network of bodies that collectively cover a range of governance functions, including policymaking, legislative action, cooperation, and structural roles. While all three regions (UN, EU, ASEAN) have institutions fulfilling both legislative and policymaking mandates, their distribution and specialization patterns differ significantly.

The United Nations (UN) exhibits the broadest institutional diversity, with numerous bodies serving overlapping yet distinct functions. The main UN organs: the General Assembly (UNGA), Security Council (UNSC), and the Secretary-General, all contribute to policymaking and cooperative functions. Legislative authority within the UN context typically manifests through resolutions, which, while not legally binding in the traditional sense, carry significant normative influence.[347] The UNGA tends to focus on thematic areas such as crime, privacy, and rights-related aspects of cyberspace governance, whereas the UNSC concentrates on infrastructure protection and security imperatives. Beyond these central bodies, specialized agencies such as the International Telecommunication Union (ITU) manage technical and standardization work, while the UN Office on Drugs and Crime (UNODC) addresses cybercrime, and the Group of Governmental Experts (GGE) advances norm-setting. This layered distribution of roles results in high intra-organizational fragmentation, with multiple bodies operating in parallel on intersecting mandates.

The European Union (EU), by contrast, demonstrates a far more centralized institutional structure. Legislative functions are concentrated in the European Parliament and the Council

[347] Marko Divac Öberg, "The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ," *European Journal of International Law* 16, no. 5 (November 1, 2005): 879–906, https://doi.org/10.1093/ejil/chi151.

of the EU, supported by the European Commission, which primarily handles policymaking, cooperation, and implementation.[348] The institutional network is relatively compact, with fewer overlapping mandates compared to the UN. One notable outlier is the Council of Europe, which, while operating beyond the EU's formal structure, plays a pivotal legislative role in the adoption of the Budapest Convention on Cybercrime.[349] Overall, the EU's fragmentation is less horizontal and more hierarchical, with clear lines of authority and functional separation between its legislative and executive bodies.

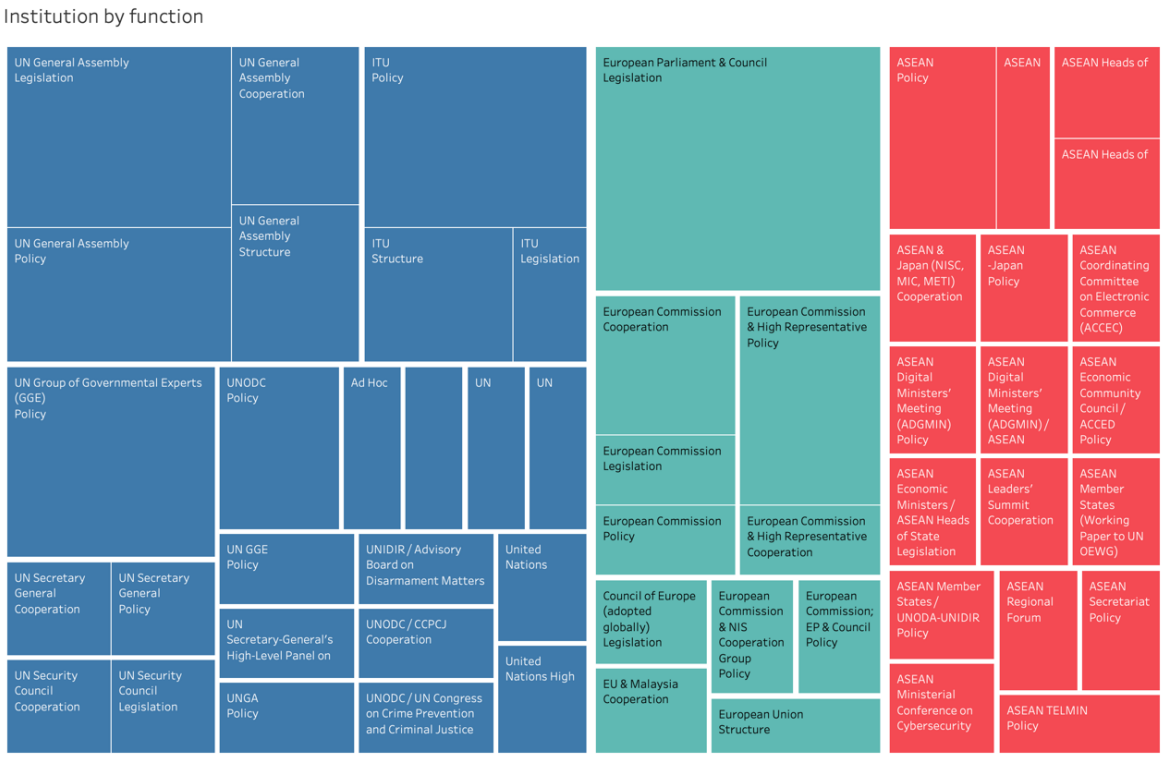


Figure 17 Institutional Fragmentation - Institutions mapped by functions

ASEAN occupies a middle ground in terms of the number of bodies but remains heavily weighted toward political and cooperative functions. Most ASEAN-level governance is driven by the ASEAN Heads of State, Ministerial Meetings, Leaders' Summits, and Regional Forums, which set broad policy agendas and coordinate regional cooperation.

[348] Eva G. Heidbreder and Gijs Jan Brandsma, "The EU Policy Process," in *The Palgrave Handbook of Public Administration and Management in Europe* (London: Palgrave Macmillan UK, 2018), 805–21, https://doi.org/10.1057/978-1-137-55269-3_42.
[349] Peter Csonka, "The Council of Europe's Convention on Cyber-Crime and Other European Initiatives," *Revue Internationale de Droit Pénal* Vol. 77, no. 3 (September 17, 2007): 473–501, https://doi.org/10.3917/ridp.773.0473.

Legislative output is minimal, with the sole example being the e-ASEAN Framework Agreement concluded by the ASEAN Heads of State. Technical and legal governance roles are less developed compared to the UN or EU, reflecting ASEAN's consensus-based and non-binding approach to regional governance.

Taken together, the comparison reveals a clear pattern of institutional diversity and concentration across regions. **The UN exhibits the widest institutional spread, encompassing political, legislative, technical, and cooperative bodies with overlapping mandates**. **The EU's institutional architecture is more centralized, with legislative authority concentrated in the European Parliament and Council, and policymaking and coordination handled largely by the European Commission**. **ASEAN, by contrast, is dominated by political and ministerial forums, with cooperation mechanisms far outweighing legislative instruments and almost no specialized technical or enforcement bodies at the regional level**.

These differences underscore how institutional fragmentation is not only about the number of bodies but also about functional scope and depth.[350] **The UN's broad coverage creates complex overlaps, the EU's concentration limits diversity but strengthens vertical coherence, and ASEAN's diplomatic-heavy structure results in gaps in legal and technical capacity**. This variation reflects deeper regional governance philosophies and directly shapes how each bloc approaches cyberspace regulation, norm development, and enforcement.

These differences are further reflected when institutional type is examined in relation to governance function. Across the global regime complex, technical and standardization bodies, such as telecommunications agencies and cybersecurity certification authorities; are primarily engaged in policymaking and structural functions, providing the technical underpinnings of cyberspace governance. Political and deliberative organs are more evenly distributed across policymaking, legislative, and cooperative functions, serving as the primary arenas for negotiating norms, adopting resolutions, and facilitating intergovernmental dialogue. Operational and enforcement-oriented institutions tend to be

[350] Cuihong Cai and Ruoyang Zhang, "Fragmentation of Global Cybersecurity Governance: Quasi-Public Goods and Multi-Level Conflicts," *Global Political Economy* 4, no. 1 (March 2025): 32–50, https://doi.org/10.1332/26352257Y2024D000000016.

concentrated in legislative and cooperative domains, particularly in areas such as cybercrime prevention, infrastructure protection, and law enforcement coordination. Meanwhile, normative and expert development groups function almost exclusively within the policymaking sphere, advancing voluntary norms, principles, and confidence-building measures that operate alongside formal legal instruments.

This distribution highlights that fragmentation arises not only from the existence of multiple institutions, but also from the uneven alignment of institutional types with governance functions. Technical bodies may be present in some regions but absent in others, political organs may dominate in consensus-driven frameworks, and operational agencies may exist only within certain legal cultures. As a result, similar governance functions, such as legislation or cooperation; are often carried out by institutions of fundamentally different types, with varying mandates, levels of authority, and operational capacities. This structural mismatch reinforces asymmetries in global governance capacity, shaping the way norms are produced, laws are enforced, and technical standards are implemented across different regional and international settings.

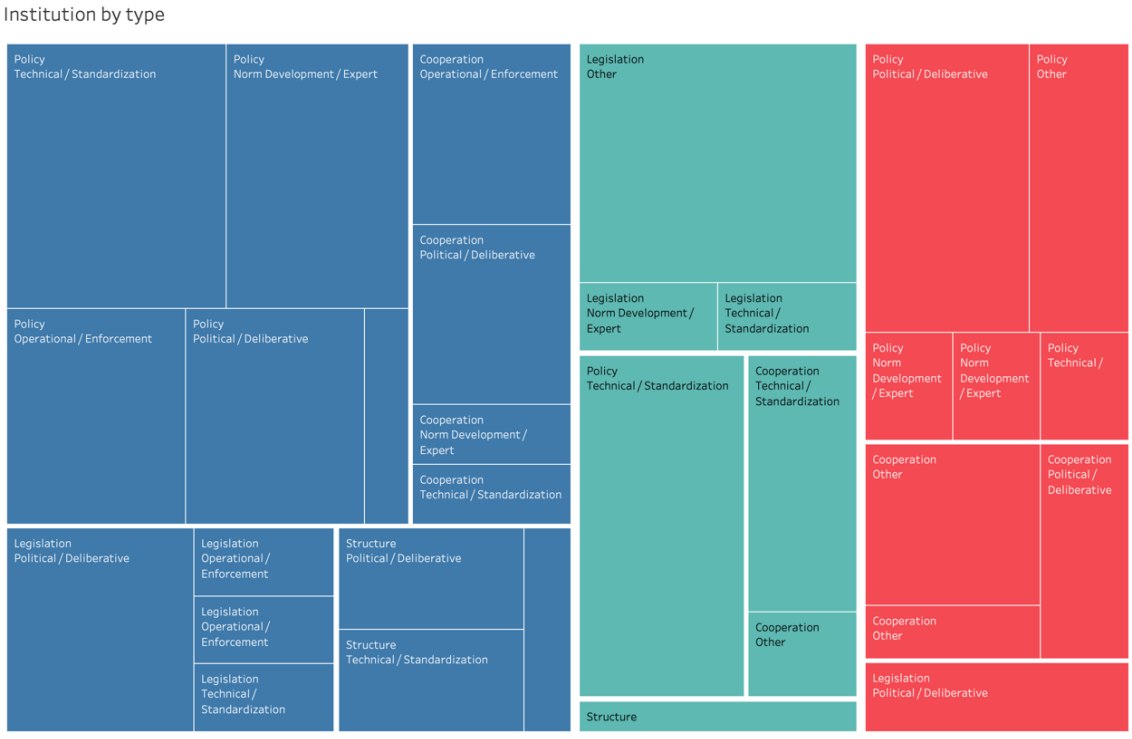


Figure 18 Institutional Fragmentation - Institutions mapped by type

2. Divergence of Thematic Priorities in Cyberspace Governance

Thematic fragmentation in cyberspace governance reveals not only which issues dominate the regulatory agenda of different regions, but also the degree of legal authority attached to each theme. Security emerges as the most governed aspect across all regions, with the UN producing the largest number of instruments, followed by the EU and ASEAN. However, the legal formality of these instruments differs sharply. Both the UN and ASEAN rely overwhelmingly on non-binding measures in security governance, with only a single potentially binding instrument under the UN (a draft cybercrime convention; still under negotiation).[351] ASEAN's security regulation is embedded in cooperative declarations, policy frameworks, and ministerial statements. The EU, in contrast, maintains a more balanced mix of binding and non-binding security rules. Its binding legislation includes the NIS2 Directive,[352] the Directive on combating fraud and personal data misuse,[353] and the Cybersecurity Act,[354] while non-binding measures cover cybersecurity strategies and sectoral cooperation initiatives.

A similar pattern is visible in infrastructure and standardization, where the UN and ASEAN again depend heavily on non-binding instruments. For the UN, this is exemplified by the International Telecommunication Regulations and ITU technical recommendations. ASEAN's principal binding rule in this domain is the e-ASEAN Framework Agreement, complemented by various cooperative frameworks. The EU's approach mirrors its security governance model, with non-binding outputs like the EU Cyber Resilience Strategy, CIIP communications, and the Internal Security Strategy, alongside binding acts such as the Data Governance Act, NIS2 Directive, and Cybersecurity Act; reflecting how infrastructure and security are often addressed in tandem in EU lawmaking.

---

[351] UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, "Draft Convention on Cybercrime," UN Doc. A/AC.291/L.15 (23 Aug. 2024)

[352] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), OJ L 333, 27.12.2022, p. 80–152.

[353] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4.5.201

[354] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019

Development presents a striking point of convergence: all three regions address it exclusively through non-binding measures. The UN leads in volume with twelve instruments, followed closely by ASEAN with ten, while the EU produces only three, indicating that development is not a major thematic focus at the EU level. In these cases, instruments tend to focus on capacity building, narrowing the digital divide, and enhancing regional cooperation.

The economy theme offers an interesting reversal of dominance. ASEAN leads with two binding agreements; the e-ASEAN Framework Agreement and the ASEAN Agreement on Electronic Commerce; marking one of the few thematic areas where ASEAN produces more legal instruments than the UN or EU. The EU contributes a single binding measure, the Directive on Combating Fraud and Counterfeiting of Electronic Payments. By contrast, there is no dedicated UN instrument explicitly targeting the economic dimension of cyberspace governance, despite relevant norms being embedded in WTO agreements and other international frameworks.

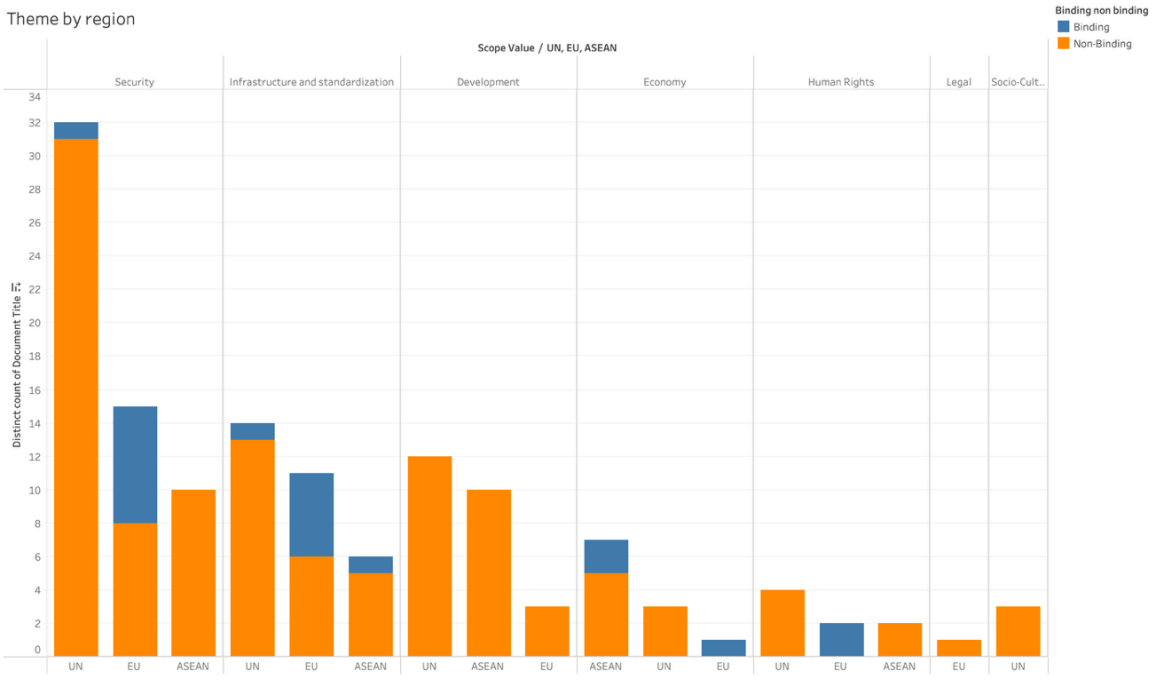


Figure 19 Thematic Fragmentation - Theme by region

In human rights, the EU takes the lead with robust binding legislation, most notably the Directive on Personal Data Protection and the GDPR package (Regulation 2016/679). The UN addresses human rights through non-binding instruments, focusing on the right to

privacy, child online protection, and digital cooperation. ASEAN, while less prolific, has introduced region-specific frameworks such as the ASEAN Framework on Personal Data Protection and the Framework on Digital Data Governance.

The socio-cultural domain remains the least developed in terms of legal authority, with the UN as the only active actor producing non-binding resolutions. These include the Resolution on the Creation of a Global Culture Strategy and initiatives for private sector engagement in countering the use of ICT for terrorism. Neither the EU nor ASEAN has dedicated instruments in this thematic space, underscoring its marginal position in regional cyberspace governance agendas

Thus, these patterns demonstrate that thematic fragmentation is not simply about coverage breadth, but about how each region allocates binding authority across different themes. The UN exhibits broad thematic reach but a heavy reliance on non-binding norms, the EU focuses on fewer themes but uses binding law more consistently, and ASEAN's presence is concentrated in non-binding cooperation frameworks; except in select economic and infrastructural areas where it asserts binding commitments. This divergence in thematic priorities and legal weight reinforces asymmetries in governance capacity and complicates the creation of harmonized global regulatory frameworks.

3. Vertical Fragmentation: Binding Authority Across Governance Levels

Vertical fragmentation in cyberspace governance reveals clear differences in how authority is distributed across bilateral, multilateral, and regional levels. Across both datasets, the bilateral layer is virtually absent, with only a single non-binding EU instrument appearing in the mapping. This absence suggests that, unlike in some other regulatory domains, state-to-state arrangements are not a significant pathway for developing cyber governance norms or rules.[355]

At the multilateral level, the UN overwhelmingly dominates in both volume and breadth, but its output is heavily skewed toward non-binding instruments. Only two binding multilateral UN documents appear in the dataset, underscoring the organization's reliance

[355] Arun Sukumar, Dennis Broeders, and Monica Kello, "The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy," *Contemporary Security Policy* 45, no. 1 (January 2, 2024): 7–44, https://doi.org/10.1080/13523260.2023.2296739.

on consensus-driven resolutions, frameworks, and guidelines that aim for universal legitimacy rather than direct enforceability. While this approach allows for broad participation and norm diffusion, it also limits the capacity for coercive compliance. By contrast, the EU and ASEAN have almost no multilateral presence; only one binding instrument from the EU and none from ASEAN; highlighting their focus on governance within regional rather than global settings.

At the regional level, the patterns diverge sharply. The EU emerges as a regional legislator, with a relatively balanced mix of binding and non-binding rules. Its binding directives and regulations, such as those on cybersecurity, data governance, and critical infrastructure, create high internal coherence and legal certainty among member states, though their effect is geographically limited. ASEAN, on the other hand, functions as a regional facilitator, producing a substantial number of instruments but with a strong bias toward non-binding commitments. This reflects its diplomatic and consensus-based governance style, prioritizing flexibility and inclusiveness over enforceability. The UN's regional footprint is minimal, consistent with its global mandate.

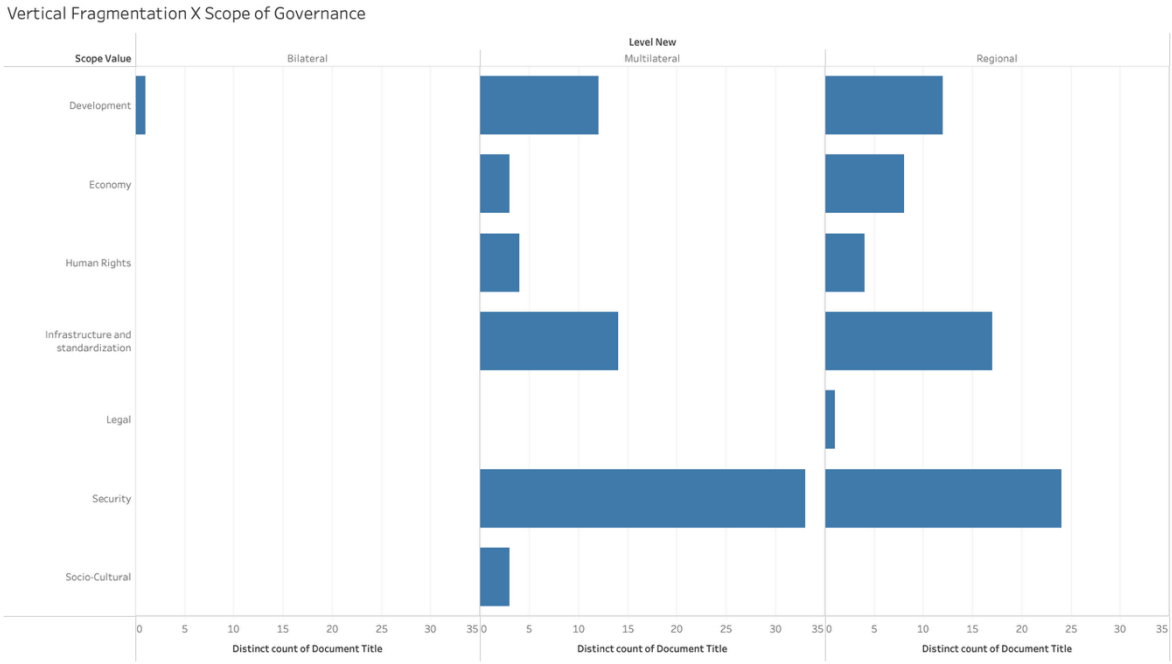


Figure 20 Vertical Fragmentation - Scope of governance

Viewed collectively, these patterns point to an uneven layering of authority: global norms under the UN offer broad coverage but limited enforceability, EU regional rules

provide narrower coverage yet carry strong binding force, and ASEAN's cooperative frameworks encourage participation while leaving substantial gaps in legal obligation. This vertical imbalance deepens the fragmentation of the cyberspace governance regime, as both the regulatory weight and enforceability vary not only between regions but also across governance levels.

4. Fragmentation based on LRT Modalities

i. Law based fragmentation

The law-based fragmentation data reveals a stark contrast in how regions operationalize the "Law" modality within cyberspace governance. The UN demonstrates a strong reliance on general principles (16 in total) alongside only two pure-law treaties or conventions. This pattern underscores the UN's role as a global norm-setter, producing broad but often non-binding legal reference points. The heavy weighting toward general principles, rather than binding instruments, mirrors ASEAN's own approach and positions the UN as a soft-law anchor in the global governance landscape.

The EU, in contrast, exemplifies a codified, treaty-driven legal model. Nine binding treaties or conventions and two general principles indicate a strong preference for harmonized enforceable instruments. This approach reflects the Western tradition of legal integration and vertical coherence, which stands in sharp opposition to ASEAN's minimal formal law output. The EU's legal depth also highlights a significant axis of vertical fragmentation, as its binding law structures are absent from ASEAN's governance architecture.

ASEAN's footprint in pure law sources is minimal; only one binding convention classified as pure law; revealing both structural and philosophical divergences. Structurally, this scarcity reflects limited regional legal machinery capable of producing binding instruments. Philosophically, it reflects ASEAN's consensus-based diplomatic culture, which prioritizes political and cooperative instruments over enforceable law. This combination of legal minimalism and political pragmatism suggests that ASEAN's divergence from Western models is not merely a result of

capacity constraints, but a deliberate governance choice aligned with its broader regional identity.

Taken together, these patterns reinforce the fragmentation of the international cyberspace regime. The EU's binding-law-heavy model, the UN's norm-oriented legal framework, and ASEAN's political-legal minimalism represent distinct regulatory philosophies coexisting in the same governance space. For the purposes of this research, ASEAN's position; closer to the UN's soft-law orientation than to the EU's hard-law codification, serves as empirical evidence of the easternization of international law, where regional governance frameworks redefine legitimacy and authority away from the Western treaty-centric model. This evidences a shift toward a more regionally driven and fragmented regime in which Southeast Asia is carving out an alternative pathway for cyberspace regulation.

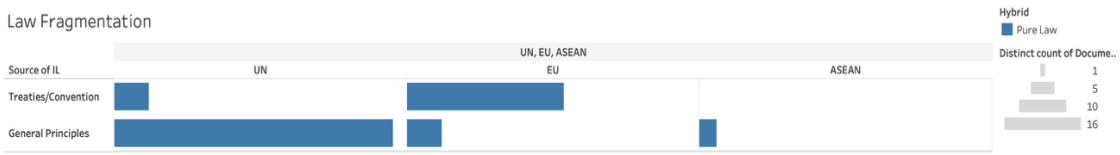


Figure 21 Law Fragmentation

ii. Norm based fragmentation

The distribution of norm-based instruments across regions reveals a pronounced concentration within the UN system, with institutional security and institutional development emerging as its dominant thematic clusters. These instruments, while non-binding in nature, carry significant normative weight by articulating standards, guidelines, and principles that shape global discourse on cyberspace governance. The **UN's normative influence extends beyond security into areas such as economic governance, human rights, infrastructure and standardization, and socio-cultural dimensions**, demonstrating a breadth of thematic engagement unmatched by other regions. However, **this breadth also reflects a reliance on soft law approaches, which, while fostering broad participation, lack direct enforceability**.

ASEAN's norm-based contributions, though smaller in absolute numbers, are heavily concentrated in security and development. This focus mirrors the bloc's strategic priorities of regional stability and economic modernization, while also

highlighting its consensus-based diplomatic culture. In this sense, ASEAN's normative instruments serve a dual function: they act as political commitments that reinforce regional cohesion, and they provide flexible frameworks that accommodate varying national capacities. Despite their modest volume compared to the UN, these norms are regionally significant, particularly when viewed against ASEAN's limited legal and technical capacity at the regional level.

The EU's presence in the norm-based modality is marginal, with its governance framework largely anchored in binding legal rules rather than soft norms. The few norm-oriented documents that do exist complement its legislative instruments, often providing interpretive guidance or policy framing in support of its legal acquis. This reflects a broader regulatory philosophy in which norms play a secondary role, primarily serving to facilitate the implementation of binding measures rather than operating as standalone governance tools.

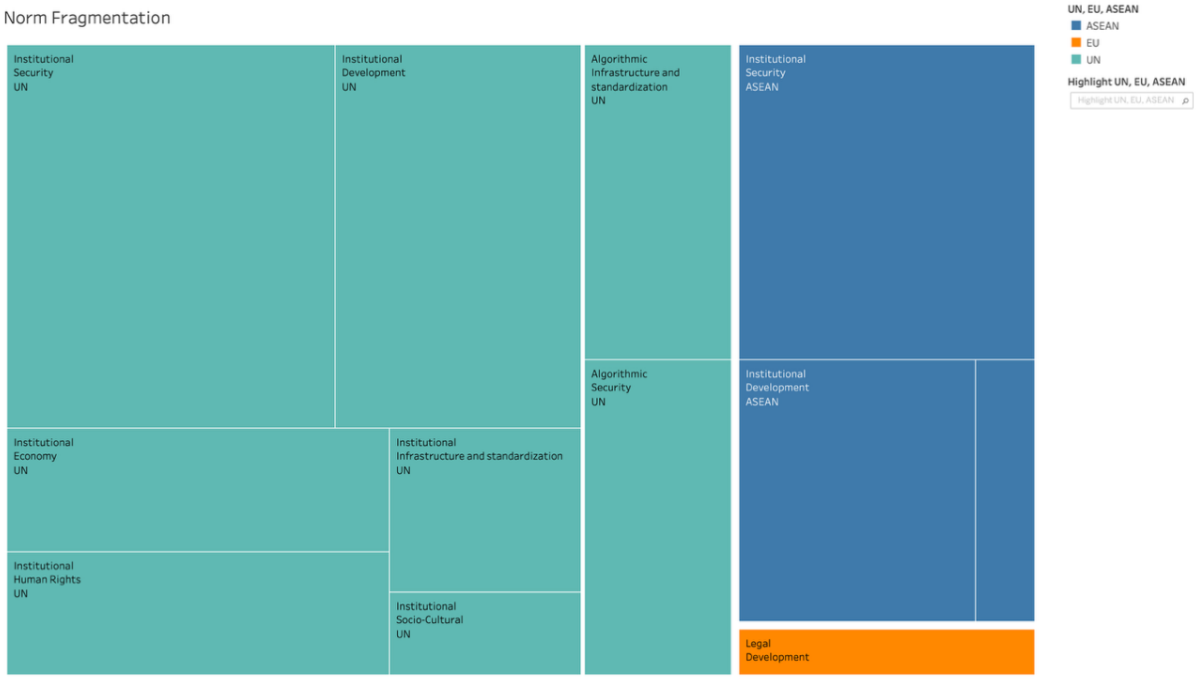


Figure 22 Norm Fragmentation

It is important to note that this visualization captures only pure norm-based instruments, excluding hybrid documents that combine normative provisions with legal or architectural elements. As a result, the extent of cross-modality interaction (such as norms embedded in legally binding agreements or standards) may be

understated here. Nonetheless, the distribution patterns point to an asymmetry in normative authority: the UN dominates the global norm-setting space, ASEAN channels its limited resources into politically salient thematic areas, and the EU relies on norms mainly as a supporting layer to its legal framework. Together, these differences reinforce the fragmented nature of cyberspace governance, where the role and weight of norms vary sharply by region and institutional philosophy.

iii. Architecture based fragmentation

The architecture-based fragmentation dataset reveals that only the UN and the EU have a visible footprint in this modality, with ASEAN entirely absent. This absence underscores a significant regional gap in shaping the "code layer" of cyberspace governance; technical standards, system design, and infrastructural safeguards remain largely outside Southeast Asia's direct regulatory reach. The result is a dependency on external frameworks, particularly those set by global bodies like the UN and, to a lesser degree, the EU.

Within this limited landscape, the UN emerges as the dominant authority in architecture governance, covering a broad range of thematic scopes. In **infrastructure and standardization**, two key instruments stand out: the *Resolution on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*[356] and the *Work of the Advisory Board on Disarmament Matters* as reported by UNIDIR.[357] These instruments not only frame global technical norms but also integrate them into broader security discourses, highlighting how architecture is used to underpin both resilience and strategic stability. In the **security** domain, the UN's architectural focus reinforces the link between technical standards and the protection of critical infrastructure. In development and socio-cultural governance, the *Plenipotentiary Resolution 130 – Strengthening ITU Role in Building Confidence and Security in the Use of ICTs* reflects the organization's attempt to embed architectural considerations into wider digital inclusion and trust-building agendas.

[356] UNGA Res. 58/199, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, UN Doc. A/RES/58/199 (30 Jan. 2004)
[357] UNGA, Work of the Advisory Board on Disarmament Matters: Report of the Secretary-General, UN Doc. A/79/240 (22 Jul. 2024)

By contrast, the EU's architectural governance is narrowly focused, represented by a single document, the *EU Data Governance Act*. While its scope is restricted to infrastructure and standardization, its provisions are highly specific, aiming to shape the data economy through standardized frameworks for intermediation services. The Act explicitly addresses the technical infrastructure necessary for connecting data subjects, holders, and users, with an emphasis on eliminating barriers for SMEs and start-ups. Furthermore, it mandates the creation of interoperable platforms, databases, and other infrastructures to facilitate data exchange. Throughout the instrument, standardization is geared toward data processing and governance, aligning architectural design with market efficiency and competitiveness within the EU's internal data space.

Figure 23 Architecture Fragmentation

This distribution of authority reflects a clear vertical asymmetry in architecture governance. At the global level, the UN not only defines overarching technical norms but also integrates them into security, development, and socio-cultural governance.[358] At the regional level, the EU's interventions are narrower and economically oriented, while ASEAN has yet to develop architectural frameworks of its own. This imbalance

[358] Maurer, Tim. Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security. Discussion Paper 2011-11. Science, Technology, and Public Policy Program, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011. https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

deepens fragmentation: global rules are expansive but externally set, regional rules (where they exist) are sector-specific, and Southeast Asia's absence prevents it from embedding regional priorities into the foundational infrastructure of cyberspace. In the context of the easternization debate, this modality shows a key limitation; without architectural self-reliance, ASEAN's ability to shape an independent regional governance model remains constrained, even if it advances in other modalities such as norms or cooperation.

iv. Market based fragmentation

The market modality in international cyberspace governance emerges not as a stand-alone regulatory approach but almost exclusively in hybrid form, intersecting with law, norms, and architecture. This means that no region (ASEAN, EU, or UN) produces a "pure" market instrument in isolation. Instead, market-oriented governance is embedded within broader frameworks that simultaneously invoke legal obligations, normative principles, and technical or infrastructural provisions. This hybrid nature reflects the practical reality that economic governance in cyberspace is inseparable from legal enforceability, value-based legitimacy, and technical implementation.

ASEAN dominates the scope of market governance among the three regions, with the largest thematic allocation to economy-related instruments. However, every one of these instruments exists as a hybrid between market, law, norms, and architecture. Key examples include the ASEAN Framework on Personal Data Protection, ASEAN Framework on Digital Data Governance, Framework for ASEAN Digital Economy, ASEAN Agreement on Electronic Commerce, and the ASEAN Digital Masterplan 2025. These instruments appear not only in the economic category but also under scopes related to infrastructure, development, and human rights. This indicates that ASEAN's market governance is not narrowly commercial; rather, it positions economic integration within a multi-dimensional governance approach aimed at boosting competitiveness while addressing cross-cutting issues like data security, infrastructure readiness, and societal inclusion.

The EU's market-related governance, while smaller in volume, is similarly hybridized, typically blending market, law, and norms. Unlike ASEAN's development

and integration-oriented economic governance, the EU's market frameworks are tightly bound to regulatory and security priorities. For instance, the EU Cybersecurity Strategy 2020 and the Joint Framework for Countering Hybrid Threats embed economic considerations, such as strengthening the EU's digital single market, within binding legal provisions and shared security objectives. This reflects the EU's tendency to frame market governance through a rules-based model that seeks both competitiveness and systemic resilience.

The UN contributes the least to market-based governance in quantitative terms, and its approach is almost entirely cross-matched with architecture. The market modality here appears in highly specific scopes, primarily security and socio-cultural governance. A notable example is the Working Paper: Private Sector Engagement in Responding to the Use of ICT for Terrorist Purposes by the UN Counter-Terrorism Executive Directorate (CTED), which focuses on mobilizing private sector capacity for security objectives. This signals that the UN's market-oriented initiatives are less about fostering open economic activity and more about aligning commercial actors with global security imperatives.

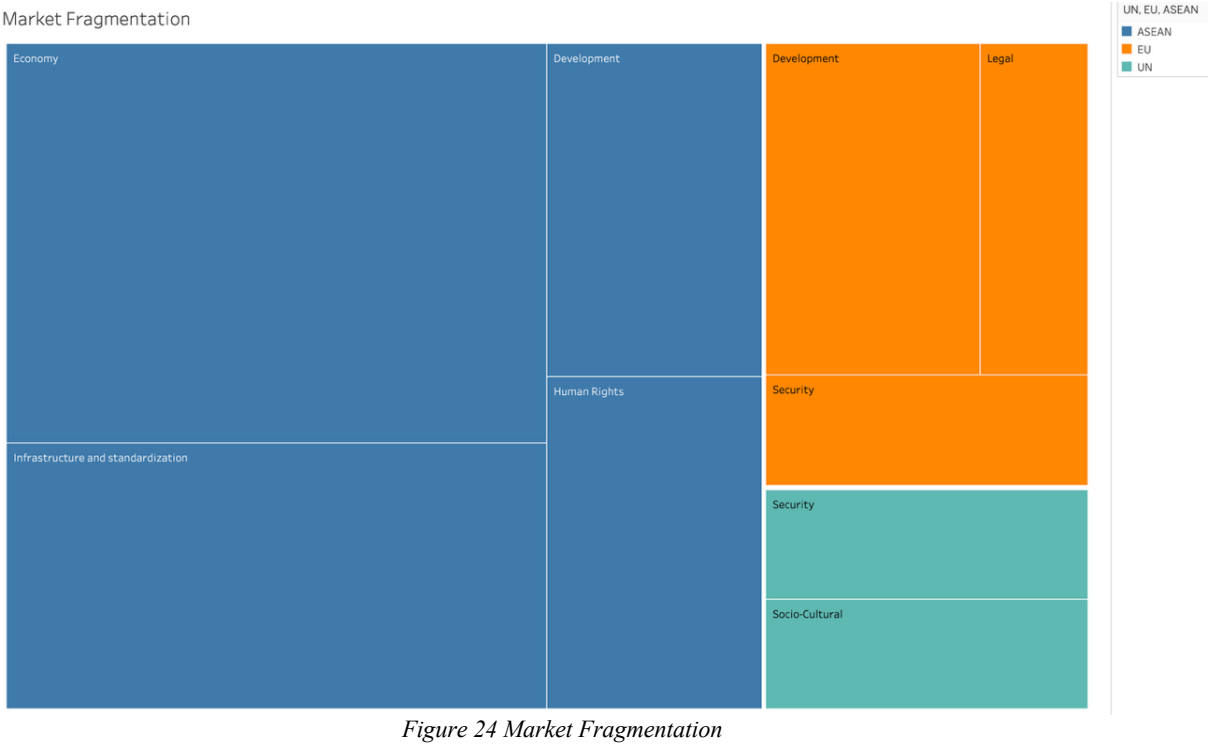


Figure 24 Market Fragmentation

Taken together, these patterns highlight a clear divergence in the role and scope of the market modality across regions. ASEAN's expansive, integrationist, and multi-sectoral economic governance departs from the EU's regulatory-security orientation and the UN's narrowly security-linked market initiatives. The hybrid nature of all market governance further suggests that economic activity in cyberspace is deeply entangled with legal, normative, and technical architectures; a finding that not only reinforces the interconnectedness of Lessig's modalities but also underscores how regional priorities shape distinct pathways in the emerging regime complex of cyberspace governance.

5. ASEAN's Role in the Fragmentation of Global Cyberspace Governance

ASEAN's approach to cyberspace governance reflects a deliberate preference for pragmatic, non-confrontational, and flexible solutions, even in the face of significant and geopolitically motivated cyber threats.[359] High-profile incidents; such as Chinese APT campaigns linked to the South China Sea dispute,[360] the Naikon intrusion following the disappearance of MH370,[361] and long-running APT30 espionage activities[362]; have underscored the region's vulnerability and strategic relevance. [363] Yet, rather than adopting confrontational or punitive measures, ASEAN has maintained a consensus-based diplomatic posture consistent with the "ASEAN Way," prioritizing cohesion and dialogue over binding enforcement.[364] This structural choice mirrors the empirical findings in the mapping: ASEAN's regional cyber instruments are overwhelmingly non-binding, concentrated in political and cooperative domains, and lack the coercive capacity characteristic of EU legislation.

[359] Eugene E.G. Tan and Benjamin Ang, "ASEAN Ambiguity on International Law and Norms for Cyberspace," in *Baltic Yearbook of International Law*, vol. 20 (Brill Nijhoff, 2022), 133–62, https://doi.org/10.1163/22115897_02001_008.
[360] Greg Austin, Kai Lin Tay, and Munish Sharma, "China's Cyber Influencing and Interference," *International Institute for Strategic Studies*, 2022, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/02/great-power-offensive-cyber-campaigns_04-china.pdf.
[361] Elise Viebeck, "Cyberattacks Followed Malaysia Airlines Flight Disappearance," The Hill, 2015.
[362] Fireeye Labs, "APT30 and The Mechanics of a Long-Running Cyber Espionage Operation," 2015.
[363] Elina Noor, "Positioning ASEAN in Cyberspace," *Asia Policy* 15, no. 2 (April 1, 2020): 107–14, https://doi.org/10.1353/ASP.2020.0033.
[364] Susy Tekunan, "The Asean Way: The Way To Regional Peace?," *Jurnal Hubungan Internasional* 3, no. 2 (2014): 142–47, https://doi.org/10.18196/hi.2014.0056.142-147.

Thematic patterns further illustrate ASEAN's distinctive contribution to fragmentation. In line with its strategic priorities, ASEAN's most developed areas of governance are security, infrastructure, and the digital economy. [365] While the dataset shows that ASEAN rarely produces binding instruments, the exceptions are notable: economic governance agreements such as the e-ASEAN Framework Agreement and the ASEAN Agreement on E-Commerce represent rare instances of hard law at the regional level. However, the legal depth of these instruments remains limited when compared to the EU's multi-thematic legislative acquis. ASEAN's breadth of thematic coverage is more comparable to the UN, but like the UN, this breadth is coupled with shallow legal authority, producing asymmetries in governance capacity.

Institutionally, ASEAN's governance network is dense at the political and ministerial levels, encompassing mechanisms such as the ASEAN Digital Ministers' Meeting (ADGMIN), the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the ASEAN Defence Ministers' Meeting (ADMM), and the ASEAN Regional Forum (ARF). [366] However, the mapping confirms that specialized technical and enforcement bodies are absent at the regional level. Even with initiatives such as the ASEAN Regional Computer Emergency Response Team (CERT) and the ASEAN Cybersecurity Cooperation Strategy 2021–2024, capacity remains uneven across member states. This gap is particularly acute in architecture-based governance, where ASEAN has no regional instruments at all, relying instead on external frameworks set by the UN or EU.

From a vertical perspective, ASEAN's activity is concentrated almost entirely at the regional level, with no binding multilateral contributions in the dataset and no bilateral agreements of substance. Instead, ASEAN participates in multilateral norm-setting through UN processes, such as the Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG). [367] This participation has yielded commitments to voluntary norms ; most notably, the 2015 UNGGE norms of responsible state behaviour in cyberspace, endorsed collectively by ASEAN in 2018, but without binding treaty obligations. The result

[365] Noor, Positioning ASEAN in Cyberspace, 58
[366] Sari, ASEAN Regional Effort, 3
[367] *Ibid* 6

is a vertical imbalance: ASEAN reinforces its regional identity and centrality in diplomacy but contributes little to enforceable multilateral law.

When viewed through Lessig's modalities, ASEAN's fragmentation footprint becomes more precise. In the **law** modality, ASEAN has minimal codified legal frameworks, with no regional cybersecurity convention and only isolated economic agreements as binding law. In **norms**, ASEAN plays a regionally significant role, particularly in security and development, using political commitments to maintain cohesion while preserving flexibility. [368] In **architecture**, ASEAN is absent, ceding standard-setting and infrastructural governance to external actors. The **market** modality, however, reveals ASEAN's strongest presence: hybrid instruments such as the ASEAN Framework on Digital Data Governance, ASEAN Model Contractual Clauses, and the ASEAN Digital Masterplan 2025 link economic integration with data protection, infrastructure readiness, and societal inclusion. [369] Yet, these instruments remain non-binding, limiting their structural impact.

Capacity and enforcement gaps compound these structural features. ASEAN's 77.6% internet penetration rate and rapidly expanding digital economy make it a prime target for cyberattacks, as noted by INTERPOL.[370] The cyber maturity gap; with Singapore leading, followed by Malaysia and Indonesia, slows the region's ability to adopt and implement higher-standard governance tools.[371] Even in high-profile incidents such as the Tokopedia data breach, ASEAN members have often looked to external legal models like the EU's GDPR rather than developing a unified regional framework.[372]

Overall, ASEAN's contribution to fragmentation lies in its creation of a distinct governance pole that blends wide thematic engagement, norm-heavy cooperation, and market-driven integration, while leaving gaps in legal enforceability, technical standard-setting, and multilateral binding authority. This approach departs from the EU's hard-law model and only partially overlaps with the UN's soft-law architecture, reinforcing a regime

[368] Noor, Positioning ASEAN in Cyberspace, 112
[369] Sari, ASEAN Regional Effort, 19
[370] *Ibid*
[371] Australia Strategic Policy Institute (ASPI). Cyber Maturity in the Asia-Pacific Region 2017. Barton, ACT: ASPI, 2017.https://adaspi.s3.apsoutheast2.amazonaws.com/201712/ASPI%20Cyber%20Maturity%202017_AccPDF_FA_opt.pdf.
[372] Sari, ASEAN Regional Effort, 11

complex in which Southeast Asia's regulatory philosophy both complements and complicates global cyberspace governance.

C. Regime complex of International Cyberspace Governance

1. Rule overlap

The analysis of rule overlap within the cyber regime complex reveals how governance across different thematic areas; ranging from security and infrastructure to human rights, economic regulation, and socio-cultural development, frequently converges and collides across institutions. Because cyberspace is inherently cross-cutting, no single regime can fully contain its governance; instead, institutional mandates and regulatory scopes overlap in ways that produce both synergies and tensions.[373] Security-related instruments often extend into infrastructure protection, while economic frameworks intersect with privacy and human rights, and development agendas overlap with socio-cultural and access-related concerns. These overlapping rule systems highlight the extent to which cyberspace governance is shaped not only by institutional diversity but also by the entanglement of issue areas themselves, creating a dense network of intersecting norms and obligations that reinforce the regime complex character of this field.

a. Security

Security emerges as the dominant governance scope across all three regions in the dataset, with thirty-five documents; more than double the count for the second-ranked scope, infrastructure (sixteen). The UN produces the largest share of security-related instruments (twenty-two), closely followed by the EU (twenty-four), with ASEAN trailing at five. **Within the UN, the General Assembly is the principal source of these instruments, issuing a series of resolutions that, while framed broadly in terms of protecting ICTs through international cooperation, concentrate substantively on combating cybercrime**. Resolutions such as 55/63,[374]

[373] Stephanie C. Hofmann and Patryk Pawlak, "Governing Cyberspace: Policy Boundary Politics across Organizations," *Review of International Political Economy* 30, no. 6 (November 2, 2023): 2122–49, https://doi.org/10.1080/09692290.2023.2249002.
[374] Resolution on Combating the criminal misuse of information technologies (A/RES/55/63)

56/121,[375] 57/239,[376] 75/282,[377] and 79/243[378] chart an evolving approach: from early calls for legal harmonization and capacity building to the current mandate for an Ad Hoc Committee to elaborate a comprehensive international convention on cybercrime. This trajectory is notable for its explicit acknowledgment of regional instruments; most prominently the Budapest Convention, **marking a rare instance where a global body references a regional framework in the security domain.**

Overlaps also appear between UN specialized agencies themselves. The ITU[379] and UNODC[380] both govern aspects of cybercrime and child protection, each producing studies and policy briefs that address similar concerns. While UNODC explicitly references ITU in its child protection work, the reverse is not observed, illustrating asymmetrical coordination even within the same institutional family.

By contrast, the EU's security governance is more inward-focused, with binding, technical, and enforcement-oriented measures; NIS2, the Cybersecurity Act, the EU Cybersecurity Strategy, Directive 2013/40/EU, and ENISA mandates, dominating the field. These instruments show little to no reference to UN norms or resolutions, with external coordination occurring primarily through NATO, as in the Cyber Defence Policy Framework and the Joint Framework on Countering Hybrid Threats.

ASEAN's security governance remains largely non-binding and consensus-based, with the ASEAN Declaration to Prevent and Combat Cybercrime[381] the sole regional instrument overlapping substantively with the UN's cybercrime agenda. However, ASEAN exhibits occasional direct engagement with UN processes, as in the ASEAN Working Paper on Needs-Based Cyber Capacity-Building Catalogue,[382] which aligns

[375] Resolution on Combating the criminal misuse of information technologies (A/RES/56/121)
[376] Resolution on the Creation of a global culture of cybersecurity (A/RES/57/239)
[377] General Assembly Resolution 75/282 Countering the Use of ICTs for Criminal Purposes
[378] General Assembly Resolution 79/243 Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes
[379] UNODC Comprehensive Study on Cybercrime, Compilation of Preliminary Conclusions and Recommendations from the UNODC Expert Group on Cybercrime, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children UNODC
[380] ITU Child Online Protection (COP) Policy Brief, ITU Global Cybersecurity Agenda – Chairman's Report
[381] Association of Southeast Asian Nations (ASEAN). ASEAN Declaration to Prevent and Combat Cybercrime. Adopted at the 31st ASEAN Summit, Manila, Philippines, November 13, 2017
[382] Association of Southeast Asian Nations (ASEAN). ASEAN Working Paper on Needs-Based Cyber Capacity-Building Catalogue. Submitted by ASEAN Member States to the Open-Ended Working Group on the Security of and in the Use of ICTs, 2021–2025

regional capacity-building priorities with the UN OEWG framework by matching ASEAN states' cyber capacity gaps with international providers. Another notable overlap is with the EU in the area of critical information infrastructure protection (CIIP), where both develop guidelines to strengthen resilience. The EU works through internal bodies such as ENISA and EPCIP, whereas ASEAN partners externally, notably with Japan, to produce regulatory checklists and best-practice frameworks.

Taken together, the security domain exhibits the regime-complex condition of rule overlap: a common governance objective; protecting cyberspace security pursued simultaneously by different institutional clusters, each employing distinct modalities and referencing patterns. The UN advances soft-law norms with occasional regional recognition; the EU codifies hard-law obligations with minimal external reference; ASEAN issues non-binding cooperative commitments, selectively linking to UN processes or external partners. This plural, non-hierarchical structure ensures that actors face multiple, sometimes competing, points of authority for security governance, a defining feature of fragmentation in the cyber-regime complex.

b. Infrastructure and standardization

In the governance of infrastructure and standardization, the mapping reveals a subtler but still discernible pattern of regime-complex overlap. The UN accounts for the largest share of instruments in this scope, with 11 documents compared to only two each from the EU and ASEAN. However, for the UN, infrastructure is rarely treated as a primary governance object; instead, it most often appears as a supporting scope embedded within broader security agendas. This is evident in a range of instruments such as A/72/327,[383] A/RES/64/211,[384] and UNSC Resolution 2341.[385]

[383] United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts. A/72/327, August 15, 2017. https://undocs.org/A/72/327.
[384] United Nations General Assembly. Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures. A/RES/64/211, March 8, 2010. https://undocs.org/A/RES/64/211
[385] United Nations Security Council. Resolution 2341 (2017): Protection of Critical Infrastructure Against Terrorist Attacks. S/RES/2341, February 13, 2017. https://undocs.org/S/RES/2341(2017)

Among UN outputs, only A/RES/58/199[386] explicitly addresses the protection of critical information infrastructure as its central aim. The single binding UN instrument in this area, the International Telecommunication Regulation,[387] provides a broad legal framework for telecommunication standards, charges, and principles of cooperation but predates most modern cyber-infrastructure issues.

By contrast, EU and ASEAN instruments in this field are more targeted toward specific infrastructure objects. The EU's Data Governance Act[388] establishes a legal framework for data-sharing architecture and technical standards, while the Cybersecurity of 5G Networks Toolbox[389] sets detailed strategic and technical risk-mitigation measures for member states' network rollouts. ASEAN's Digital Masterplan 2025[390] outlines regional broadband expansion, digital services, e-government, and inclusion, articulated through eight desired outcomes. This object-specific focus marks a clear difference from the UN's more general and security-linked framing. Still, overlaps emerge in certain subfields: between the EU and the UN in data-related governance, where the UN's A/HRC/27/37[391] report frames privacy in the digital age within human rights law, and the EU codifies technical rules for data-sharing; between the EU and ASEAN in broadband and 5G development, where both set frameworks that can be read alongside the UN's International Telecommunication Regulations; and between ASEAN and the UN, where the Digital Masterplan 2025 makes explicit reference to ITU standards, such as using ITU metrics to track e-government service use and broadband quality.

From a regulatory modality perspective, the UN's approach is dominated by norms and architecture (through ITU standards) with few bindings' legal anchors,

[386] United Nations General Assembly. Creation of a Global Culture of Cybersecurity. A/RES/58/199, January 30, 2004. https://undocs.org/A/RES/58/199

[387] International Telecommunication Union (ITU). Final Acts of the World Conference on International Telecommunications (WCIT-12): International Telecommunication Regulations. Dubai, UAE, December 2012. https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

[388] European Union. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance (Data Governance Act). Official Journal of the European Union, L 152, June 3, 2022

[389] European Commission. Cybersecurity of 5G Networks – EU Toolbox of Risk Mitigating Measures. Brussels: European Commission, January 29, 2020

[390] ASEAN Digital Masterplan 2025 (ADM 2025). Jakarta: ASEAN Secretariat, January 2021. https://asean.org/wp-content/uploads/2021/01/ASEAN-Digital-Masterplan-2025.pdf.

[391] United Nations Human Rights Council. The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights. A/HRC/27/37, June 30, 2014. https://undocs.org/A/HRC/27/37.

the EU combines law and architecture through binding technical standards enforced by regulation, and ASEAN primarily employs norms and architecture, with the latter often derived from external standard-setters like the ITU. This arrangement produces a multi-layered governance environment where states may be influenced by global norms, legally bound by regional technical measures, and guided by development-oriented infrastructure goals, all without a single hierarchical authority to reconcile these frameworks.

c. Development

In the development scope (covering issues such as broadband, internet access, transport networks, the digital divide, and capacity building) the dataset reveals a dense web of cross-regional references and alignments, with all three governance hubs (UN, EU, and ASEAN) producing instruments that interact in visible ways. ASEAN has the highest number of development-focused instruments (five), but four of these explicitly reference the UN's Group of Governmental Experts (GGE) cyber norms. This is most evident in the ASEAN Ministerial Conference on Cybersecurity (Third Edition),[392] which endorsed the 2015 UN GGE norms in principle and proposed a region-specific ASEAN cyber mechanism, and in the ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace, which operationalises the same 11 voluntary norms into actionable steps for member states. Other high-level statements such as the ASEAN Leaders' Statement on Cybersecurity Cooperation[393] and the ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs;[394] similarly cite UN GGE recommendations, while signalling an intent to tailor them to regional priorities. **The ARF work plan is explicit in stating that it does not intend to duplicate UN work, instead building on it with regionally designed capacity-building measures. This illustrates a pattern where ASEAN positions its**

[392] Association of Southeast Asian Nations (ASEAN). Chairman's Statement, Third ASEAN Ministerial Conference on Cybersecurity. Singapore, September 19–20, 2018. https://asean.org/chairmans-statement-of-the-3rd-asean-ministerial-conference-on-cybersecurity/

[393] Association of Southeast Asian Nations (ASEAN). ASEAN Leaders' Statement on Cybersecurity Cooperation. Issued at the 32nd ASEAN Summit, April 2018. https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf

[394] ASEAN Regional Forum (ARF). Work Plan on Security of and in the Use of Information and Communications Technologies. Adopted by ARF Foreign Ministers, Kuala Lumpur, August 6, 2015. https://cil.nus.edu.sg/wp-content/uploads/2019/02/2015-ARF-WP-on-ICT-Security.pdf

development agenda within an inherited UN normative frame but insists on maintaining distinct regional processes.

The UN's contribution to this scope (four documents) is shaped heavily by its institutional architecture. Two major resolutions: Plenipotentiary Resolution 174 (Busan, 2014)[395] and Plenipotentiary Resolution 130;[396] link development to security through the ITU's mandate for technical assistance, capacity building, and confidence-building. A significant standalone instrument, A/RES/74/197: ICTs for Sustainable Development,[397] positions ICT access and inclusion as drivers of the Sustainable Development Goals, explicitly linking digital cooperation to bridging the global digital divide. The Final Acts of the Plenipotentiary Conference (Bucharest, 2022) deepen this regional connection by empowering ITU regional offices to coordinate with subregional bodies and UN agencies in implementing digital-inclusion goals. However, the ITU's Asia-Pacific development initiatives focus primarily on least developed countries, small island developing states, and landlocked developing countries, without direct targeting of Southeast Asia, indicating that ASEAN's developmental priorities are not the primary focus of UN regional programming.

The EU's approach to development in cyberspace is, consistent with its treatment of security and infrastructure, more formal, technical, and regulation linked. The EU Cybersecurity Strategy 2020 frames development through the lens of cyber resilience, strategic autonomy, and the promotion of EU values globally. Importantly, this is the first EU document in your dataset to explicitly adopt UN GGE norms, referencing them as part of its effort to advance responsible state behaviour in cyberspace. The strategy outlines a proactive role for the EU and member states in multilateral forums, including a Programme of Action (PoA) proposal at the UN to operationalise norms and promote capacity building. This creates a clear normative link between EU and

[395] International Telecommunication Union (ITU). Resolution 174 (Rev. Busan, 2014): ITU's Role with Regard to International Public Policy Issues Relating to the Risk of Illicit Use of Information and Communication Technologies. Plenipotentiary Conference, Busan, 2014

[396] International Telecommunication Union (ITU). Resolution 130 (Rev. Guadalajara, 2010): Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies. Plenipotentiary Conference, Guadalajara, 2010

[397] United Nations General Assembly. Information and Communications Technologies for Sustainable Development. A/RES/74/197, 10 January 2020

UN instruments, albeit framed within the EU's own institutional and strategic priorities.

Finally, one development-related EU instrument overlaps directly with ASEAN at the bilateral level: the EU–Malaysia Framework Agreement on Partnership and Cooperation (2022). This agreement contains dedicated provisions on ICT and cyber cooperation, with an emphasis on capacity building, marking the only example in the dataset of a formal EU framework agreement with an ASEAN member state in the cyber domain. **This reinforces the point that development-oriented governance in cyberspace often intersects not just across institutions but across governance levels: global, regional, and bilateral, without a single overarching hierarchy to reconcile differences in emphasis, scope, or normative content**.

d. Human rights

In the field of human rights, cyberspace governance presents one of the clearest examples of rule overlap that functions in a complementary rather than a conflicting manner. Each of the three regions (UN, EU, ASEAN) has produced two instruments related to human rights and cyberspace. The only difference lies in the institutional sources: within the UN, one document originates from the Office of the High Commissioner for Human Rights and another from the General Assembly, reflecting a degree of institutional fragmentation. By contrast, the EU instruments are both produced by the European Parliament, while ASEAN's instruments stem from ASEAN TELMIN.

Despite these institutional differences, all three regions converge on the same object of governance: the protection of privacy and personal data. In the EU, this is articulated through Directive (EU) 2016/680, which harmonises rules on the processing of personal data by competent authorities for law-enforcement purposes, and Regulation (EU) 2016/679 (GDPR), a horizontal regulation establishing a binding and comprehensive data protection regime across the Union. These instruments are formal, rigid, and binding in character. The UN approaches the issue through broader human rights framing, as seen in the OHCHR report on The Right to Privacy in the Digital Age (A/HRC/27/37), which addresses privacy in the context of surveillance and mass data collection, and the General Assembly resolution The Right to Privacy

in the Digital Age (A/RES/68/167), which reaffirms privacy as a universal human right, condemns mass surveillance, and urges states to review national procedures and protections. ASEAN, meanwhile, adopts a more flexible and economic-oriented approach through the non-binding ASEAN Framework on Digital Data Governance and the ASEAN Framework on Personal Data Protection. These establish principles and strategies to guide member states in harmonising domestic approaches to data collection, processing, and transfer in support of regional trade and information flows.

At a general level, all three regions acknowledge privacy and personal data protection as best implemented within the domestic legal sphere. The difference is primarily linguistic: ASEAN and the UN instruments tend to use the language of "national frameworks" or "national laws," while the EU stresses harmonisation among member states' "national laws." Substantively, the EU emerges as the most comprehensive and technical regulator, covering issues such as cross-border data transfers, supervisory authorities, and detailed obligations on data controllers and processors. ASEAN's frameworks resemble the EU model but distil it into broader guidelines and strategies, with repeated emphasis on "harmonisation"; a term traditionally associated with EU legal practice.[398] The UN instruments, by contrast, retain a more general human rights framing by focusing on privacy as a universal right, urging states to review surveillance practices in light of international obligations.

The most striking finding, however, is the degree to which the UN instruments explicitly reference and draw upon the European legal experience. The OHCHR report on the right to privacy cites the jurisprudence of the EU Court of Justice and refers no fewer than eight times to European Court of Human Rights cases, such as Weber and Saravia v. Germany[399] on interference with privacy. This demonstrates a normative diffusion in which the EU's detailed regulatory approach to personal data protection significantly informs and shapes the UN's human rights discourse on privacy.

[398] LexisNexis. Harmonisation. Last modified 2024. https://www.lexisnexis.co.uk/legal/guidance/harmonisation-01
[399] Gabriele Weber and Cesar Richard Saravia v. Germany, Application no. 54934/00, decided by the European Court of Human Rights.

e. Economy

In the economic scope of cyberspace governance, ASEAN emerges as the most active and dominant actor compared to the UN and EU. Out of the collected instruments, ASEAN accounts for three, while the UN contributes only one and the EU none. This imbalance, however, must be understood within the methodological limitations of the dataset, which draws on sources such as the UNIDIR Cyber Policy Portal and prioritises documents explicitly cyber-related. Broader economic treaties with major digital implications, such as the EU's Digital Single Market Strategy, or WTO agreements like GATS, GATT, and TRIPS were excluded for scope reasons. If included, such instruments would likely have overshadowed the ASEAN-led initiatives in this area.

Within ASEAN's three economic instruments, notable institutional diversity appears. Two are intergovernmental agreements adopted by ASEAN Heads of State, while the Framework for Negotiating the ASEAN Digital Economy Framework Agreement (DEFA) originates from the ASEAN Coordinating Committee on Electronic Commerce and Digital Economy (ACCED), and the ASEAN ICT Masterplan 2020 was produced by the ASEAN Secretariat. This reflects a degree of institutional overlap at the ASEAN level in governing economic aspects of cyberspace.

The UN's sole contribution, the Roadmap for Digital Cooperation (Report of the Secretary-General), sets out a broad vision of an inclusive digital economy and society. It emphasises global connectivity, digital public goods, and digital inclusion. However, its regional focus is limited: Southeast Asia is treated only in combination with the wider "Asia-Pacific," offering little direct guidance specific to ASEAN's context.[400]

Among ASEAN's instruments, the e-ASEAN Framework Agreement (2000) and the ASEAN Agreement on Electronic Commerce stand out as foundational to ASEAN's digital economy governance. The e-ASEAN Framework Agreement sets liberalisation measures for ICT, e-commerce, and digital infrastructure. Two elements are particularly notable. First, the agreement commits member states to adopt national e-commerce regulatory and legislative frameworks "based on international norms." While it does not specify which norms or organisations, this illustrates ASEAN's recognition of the

[400] United Nations, Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation. A/74/821, May 29, 2020. https://undocs.org/A/74/821.

authority of global governance practices. Second, it explicitly adopts the WTO's definition of "ICT products"[401] under the Information Technology Agreement (ITA1), integrating a global economic framework into its regional policy. Similarly, the ASEAN Agreement on Electronic Commerce refers to WTO norms, specifically GATS, situating ASEAN's economic regulation within established international trade structures.[402]

The other two ASEAN instruments display a more regionally distinct orientation. The Framework for Negotiating the ASEAN Digital Economy Framework Agreement (DEFA) (2025 target) sets principles, scope, and timeline for a legally binding agreement covering digital trade, cross-border e-commerce, payments, data flows, and data protection, while also extending into cybersecurity. Meanwhile, the ASEAN ICT Masterplan 2020 provides a five-year strategy with eight thrusts to propel ASEAN toward a secure, integrated digital economy. Its outlook is general, oriented toward capacity building and regional development, rather than embedding ASEAN firmly within global economic governance frameworks.

Altogether, the documents reveal an interesting duality. ASEAN's economic governance of cyberspace is both inward-looking, seeking to build regional integration through agreements such as DEFA and the ICT Masterplan, and outward referencing, aligning itself with global trade institutions like the WTO. By contrast, the UN offers only a broad, globalist vision, and the EU's absence reflects the scope limitation of the dataset rather than a lack of economic regulation. Overall, ASEAN's role in the economic scope underscores how regional institutions can carve a space for governance by balancing local integration with selective incorporation of international economic norms.

2. Modalities overlap

Across the four modalities, law emerges as the most dominant, with the UN and EU serving as the primary anchors. The UN contributes ten legal instruments, often in the form of resolutions, conventions, and formal reports which, even when formally non-binding, consistently reference higher legal authorities such as the UN Charter or international law.

[401] e-ASEAN Framework Agreement 2000, Article 1 (b)
[402] ASEAN Agreement on Electronic Commerce, Article 1(3), 7 (4)(c), 7(6)(c)

This practice gives UN outputs a quasi-binding character that reinforces its position as the legal reference point in cyberspace governance. The EU follows closely with eight binding instruments, including directives, regulations, and strategies that exert direct force over its member states. In contrast, ASEAN has no regionally binding legal documents, relying instead on consensus-based cooperation. This asymmetry produces a convergence between the UN and EU on law-based governance, while ASEAN remains outside that overlap. As a result, **fragmentation is reinforced vertically: ASEAN member states may participate individually in legal frameworks such as the Budapest Convention, but ASEAN as a bloc avoids legal commitments at the regional level**.

Norms form the second most prominent modality, though distributed unevenly. The UN leads with fifteen instruments that formalize voluntary principles through GGEs, OEWG processes, and General Assembly resolutions. ASEAN follows with six instruments, many of which directly adopt or repurpose UN norms. The ASEAN Checklist for Norm Implementation, the ARF Work Plan, and ministerial statements all reference the 2015 GGE report, demonstrating ASEAN's willingness to align with the UN while retaining its own mechanisms for operationalization. The EU, by contrast, contributes only one clear norm-based instrument, its Cybersecurity Strategy, which merely acknowledges UN norms rather than embedding them into a structured regional framework. Overlaps here are therefore asymmetrical: ASEAN and the UN converge through norm references, while the EU touches norms only rhetorically. These dynamic underlines **the UN's centrality in norm-setting but also highlights ASEAN's distinctive role in filtering and recontextualizing global norms rather than generating new ones.**

Architecture appears less frequently but is strategically significant. The UN, primarily through the ITU, contributes four documents that address standards and technical arrangements, often as a supporting scope within security-related instruments such as those on protecting critical infrastructure. The EU offers one distinct architecture-focused instrument, its 5G risk-mitigation toolbox, which sets strict technical and strategic measures for member states without reference to global standards. ASEAN takes a more hybrid approach, producing five instruments where architecture overlaps with norms. A notable case is the ASEAN Digital Masterplan 2025, which directly cites ITU reporting requirements and broadband standards. Here the overlap structure diverges: **UN–ASEAN linkages are visible**

through ITU references, while the EU operates independently, illustrating fragmentation in standards-setting.

The market modality is the least represented, largely because broader trade instruments such as WTO TRIPS or GATS were excluded from the dataset. Within what remains, ASEAN contributes five instruments overlapping with norms, reflecting its focus on digital economy, e-commerce, and regional integration. The EU adds one significant instrument combining market and norm modalities, notably its Digital Single Market regulations and data governance frameworks. The UN plays almost no role here, aside from occasional references to data and privacy within human rights reports. Overlaps are thus limited to ASEAN and EU activity, but these remain siloed: **the EU looks inward to regulate its own market, while ASEAN frames its digital economy through regional cooperation and partnerships with external factors such as Japan**.

These distributions and overlaps reveal an uneven balance across modalities. Law and norms are concentrated around the UN, with the EU reinforcing the legal dimension and ASEAN selectively adapting normative ones. Architecture is split, with ASEAN aligning to the UN's ITU while the EU regulates autonomously. Market governance, meanwhile, is fragmented, with ASEAN and the EU active in parallel but without coordination. **The overall picture is that law and norms constitute the densest areas of overlap, but architecture and market are marked by disconnection. This imbalance sits at the heart of the cyber regime complex, showing both convergence in legal and normative authority and fragmentation in technical and economic regulation**.

3. Overlap between domestic and global authorities

The overlap between domestic and regional authorities in Southeast Asia reveals a striking degree of vertical alignment in how cyberspace governance is framed and implemented. At the ASEAN level, the Political-Security Community (APSC) pillar dominates, with instruments that emphasize cybercrime, critical infrastructure, voluntary norms, confidence-building measures, and broader regional stability concerns. This framing positions cyberspace primarily as a matter of security, where cooperative pledges, information sharing, and regional mechanisms are designed to reinforce resilience against perceived threats. The ASEAN Economic Community (AEC) plays a secondary role,

reflected in instruments on digital trade facilitation, e-commerce, and data flows, while the ASEAN Socio-Cultural Community (ASCC) is almost entirely absent from cyber-related initiatives, surfacing only indirectly through the ASEAN Digital Masterplan 2025, which itself remains marginal in addressing socio-cultural dimensions.

At the domestic level, ASEAN member states largely mirror this pattern, thereby reinforcing the regional framing. Across the region, national instruments overwhelmingly fall within the APSC pillar, covering cybersecurity laws, cybercrime legislation, personal data protection statutes, and frameworks for critical information infrastructure. **Countries such as the Philippines and Vietnam have national frameworks almost exclusively oriented toward security, embedding cyberspace within broader state security agendas**. In the case of the Philippines, this orientation is notable not only because of its comprehensive domestic framework, but also because it is the sole ASEAN member to have acceded to the Budapest Convention on Cybercrime, directly linking its domestic legal commitments to a global treaty framework that ASEAN itself has not joined.

Other member states demonstrate a more diversified approach. Malaysia, for instance, maintains a wide portfolio, combining security-focused instruments with economic and governance frameworks such as e-commerce legislation,[403] a national Industry 4.0 policy,[404] and public sector transformation initiatives.[405] Singapore similarly blends security and socio-cultural aspects, particularly through cooperative initiatives like the National Cybercrime Action Plan, which emerged from ASEAN-Japan collaboration with Interpol. These examples highlight how some states, through their domestic instruments, both reflect ASEAN's security orientation and expand it by connecting with external actors and frameworks.

Nevertheless, the overall pattern shows that ASEAN's framing of cyberspace governance as primarily a security issue has been internalized by its member states, creating a strong vertical alignment between regional and domestic levels. Economic governance is present but

[403] Malaysia Electronic Commerce Act 2006 (Act 658), https://aseanconsumer.org/file/post_image/Act%20658%20-%20Electronic%20Commerce%20Act%202006.pdf

[404] Malaysia Industry4WRD: National Policy on Industry 4.0, https://www.malaysia.gov.my/stag-portal/content/31224

[405] Malaysia Smart City Framework, Executive Summary, https://www.kpkt.gov.my/kpkt/resources/user_1/GALERI/PDF_PENERBITAN/FRAMEWORK/FRAMEWORK_SMART_CITY_EXECUTIVE_SUMMARY.pdf

fragmented across a handful of states, while socio-cultural governance remains marginal at both levels. This consolidation produces a feedback loop: ASEAN sets the security-first framework, and member states implement it domestically, thereby strengthening ASEAN's authority as a regional reference point. At the same time, capacity gaps among weaker states such as Cambodia or Myanmar reinforce ASEAN's role, as these states rely on regional mechanisms or external guidance to compensate for domestic limitations.

In this way, the **overlap between domestic and ASEAN authorities generates coherence within Southeast Asia but simultaneously accentuates divergence from global authorities such as the UN and EU**, whose approaches are more balanced across legal, normative, and economic modalities. The result is a vertically aligned but globally differentiated governance model that underscores ASEAN's distinctive orientation toward cyberspace governance.

The cross-synthesis between ASEAN/AMS documents and the UN/EU instruments shows both strong parallels and structural divergences in how governance priorities are articulated across levels. The clearest convergence is around the Political–Security pillar (APSC). This mirrors the general governance mapping: both the UN and EU place heavy emphasis on security, cybercrime, and critical infrastructure protection. The UN has 35 instruments aligned with APSC, while the EU has 17, mostly in the form of directives, regulations, and acts. These overlap substantively with ASEAN's own security-centric governance, where both regional (ASEAN-level) and domestic (AMS) documents are overwhelmingly concentrated in the APSC pillar. At the global level, therefore, ASEAN's domestic priorities appear to resonate with the UN and EU emphasis, creating a strong security-driven alignment across institutional levels.

Where divergence begins to emerge is in the treatment of the economic (AEC) and socio-cultural (ASCC) pillars. The UN demonstrates some breadth here: 3 instruments cross into AEC (such as the Roadmap for Digital Cooperation and ICTs for Sustainable Development resolution), while 2 instruments extend into ASCC, notably on privacy and human rights in the digital age. These UN documents provide normative and developmental linkages that go beyond narrow security concerns, reflecting the UN's broad mandate to balance peace, development, and rights. ASEAN, however, reflects only a partial translation of this agenda; AMS states tend to codify security into law while leaving economic and socio-cultural

governance either underdeveloped or embedded in broader digital economy frameworks like ADM 2025.

By contrast, the EU remains heavily skewed toward APSC, with most outputs tied to binding legal measures, directives, acts, and regulations on cybercrime, data protection, and infrastructure resilience. Only a handful of EU instruments touch ASCC themes (e.g., GDPR package, Cybersecurity Strategy, EU–Malaysia cooperation agreements). Notably absent is a strong economic (AEC) track in the EU's cyber governance corpus; despite the EU's Digital Single Market being highly developed, its representation in this dataset is muted, since UNIDIR's portal filters out purely market-oriented regulations. The EU therefore appears as a law-anchored counterpart to ASEAN's largely non-binding approach: both emphasize APSC but differ fundamentally in modality and depth.

When examining document types, further contrasts sharpen. For the UN, APSC and AEC governance is primarily advanced through resolutions and reports, while ASCC elements appear in reports and final acts of conferences, reflecting the UN's normative and agenda-setting character. The EU's governance, by contrast, is operationalized through directives, acts, and regulations, with ASCC-related issues appearing in strategies and cooperation agreements. ASEAN, meanwhile, remains reliant on plans, statements, and cooperation pledges, with binding lawmaking left for AMS states. This asymmetry in governance instruments highlights the layered nature of authority: global institutions Favor broad norm diffusion, regional bodies like the EU legislate, and ASEAN/AMS combine consensus-based pledges with fragmented national implementation.

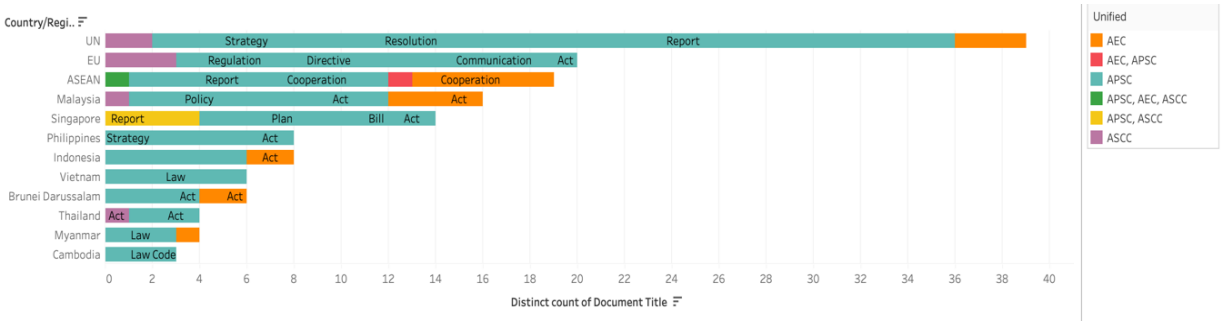


Figure 25 Modalities Overlap - Regional cross section document type and ASEAN Pillar

Overall, the overlap between domestic (AMS) and global (UN/EU) authorities reveals a hierarchical alignment in security governance but also fragmentation in economic and socio-

cultural governance. The UN provides breadth, the EU provides depth, and ASEAN provides political cohesion without binding law. This uneven structure underscores both the opportunities for cross-pillar cooperation (particularly in norm diffusion from the UN) and the persistence of fragmentation when ASEAN states selectively internalize global priorities without regionally binding commitments.

4. Strategic implications: spillovers in the cyber regime complex

The preceding analysis of fragmentation and regime complexity demonstrates not only the multiplicity of actors and institutions governing cyberspace, but also the layered interactions that occur when their respective mandates and outputs overlap. Such interactions rarely remain contained within the boundaries of individual institutions. Instead, they generate spillover effects (both positive and negative) that shape the coherence and legitimacy of global cyberspace governance.[406] As Faude and Große-Kreul argue, international institutions cannot be understood as stand-alone entities pursuing isolated governance objectives; rather, they are embedded within regime complexes characterized by rule overlap and interdependence, where legitimacy depends on how negative spillovers are addressed and justified.[407] In this sense, the strategic implications of fragmentation in cyberspace governance can best be captured through the lens of spillover dynamics.

Positive spillovers are visible in several areas of the mapping. The most notable is the reciprocal recognition between global and regional institutions. The United Nations has repeatedly referenced the Budapest Convention as a touchstone for cybercrime governance, an example of a global institution legitimizing itself by drawing upon a regional framework. Similarly, ASEAN's cyber capacity-building catalogue explicitly aligns with the UN Open-Ended Working Group (OEWG), demonstrating how regional instruments can reinforce the authority and relevance of global ones. In infrastructure and standardization, ASEAN's reliance on ITU norms within its Digital Masterplan 2025 shows how global technical standards provide legitimacy and functional support for regional implementation. These patterns reflect what Faude and Große-Kreul describe as the ability of regime complexes to

[406] Faude and Groβe-Kreul, "Let's Justify! How Regime Complexes Enhance the Normative Legitimacy of Global Governance," June 1, 2020.
[407] *Ibid*

produce inter-institutional justificatory practices that broaden legitimacy by reinforcing rather than duplicating governance objectives.[408]

At the same time, negative spillovers also emerge prominently. The European Union's decision to develop binding cybersecurity and 5G regulations without reference to ITU standards demonstrates how regional autonomy can undermine global cohesion, creating parallel rules and duplication. Within the UN itself, the lack of coordination between ITU and UNODC on child protection issues reflects an intra-institutional spillover that fragments authority and weakens coherence. ASEAN's relative weakness in the socio-cultural and human rights domain, compared to the UN's rights-based approach, similarly creates a legitimacy gap: global institutions press norms of privacy and freedom of expression, while ASEAN's silence or selective engagement forces other actors to question whether its governance approach adequately addresses broader normative expectations. These examples illustrate what Faude and Große-Kreul identify as the "partial orders of justification" produced by stand-alone institutions, which privilege certain governance objectives while marginalizing others, thereby creating pressure within regime complexes to justify such asymmetries.[409]

Spillovers also highlight the dynamics of justification and contestation across levels of governance. In the overlap between domestic and global authorities, ASEAN member states adopt UN and EU norms selectively, embedding them in national legislation in ways that reshape global frameworks. The Philippines' accession to the Budapest Convention integrates a domestic legal system into the global cybercrime framework, a positive spillover that reinforces coherence. Conversely, Malaysia's prioritization of economic and security pillars without significant alignment to socio-cultural norms reflects a divergence that requires justification vis-à-vis global standards. ASEAN as a regional organization further exemplifies this dynamic: by referencing UN GGE norms but insisting on non-duplication, ASEAN effectively "breaks open" the justificatory order imposed by UN institutions, asserting its autonomy while still acknowledging global legitimacy. This is precisely the type of justificatory practice that regime complex theory highlights as a source of normative progress,

[408] *Ibid* 3
[409] *Ibid* 4

since it compels powerful actors to engage with the concerns of weaker or regionally distinct institutions.[410]

These findings suggest that fragmentation in cyberspace governance does not simply produce incoherence but rather sets in motion a cycle of spillovers that can both undermine and reinforce legitimacy. **Positive spillovers**: such as UN referencing Budapest, ASEAN aligning with OEWG and ITU, or bilateral ASEAN–EU cooperation show the integrative potential of regime complexes. **Negative spillovers** such as EU autonomy in cybersecurity, intra-UN duplication, and ASEAN's neglect of rights and socio-cultural issues reveal the risks of rule overlap without coordination. Crucially, these dynamics are not static: regime complexes create a space where institutions are compelled to justify their rules to one another, thereby broadening the discursive field and reducing the dominance of any single actor. In line with Faude and Große-Kreul's account, this indicates that the legitimacy of cyberspace governance is increasingly dependent not on the performance of isolated institutions, but on the justificatory practices that emerge within the broader cyber regime complex.[411]

D. Shifting Frontiers: The Easternization of International Cyberspace Law

This final section advances the core claim of the chapter by identifying and analysing five interrelated indicators through which the easternisation of international cyberspace law becomes empirically visible. Rather than treating easternisation as a singular or uniform shift, the analysis traces how it materializes through changes in where authority is exercised, how norms are produced and applied, and which values underpin governance choices. Specifically, the section demonstrates easternisation through (1) a redistribution of norm-setting influence from universal institutions toward ASEAN as a regional interpreter and, in certain domains, originator of norms; (2) the decentralization of governance away from hierarchical, law-centric models toward plural, non-binding arrangements; (3) the emergence of culturally and philosophically distinct regulatory logics privileging consensus and pragmatism over legal formalism; (4) growing regulatory self-reliance at national and regional levels, marked by selective engagement with global instruments; and (5) a divergence in underlying values and principles that recalibrates

[410] *Ibid*
[411] *Ibid*

what counts as legitimate governance in cyberspace. Taken together, these indicators show that easternisation does not displace existing global frameworks but reshapes their operation and authority, revealing cyberspace as a site where Southeast Asia increasingly asserts influence through adaptation, mediation, and regionally grounded innovation.

1. Shift in norm-setting power[412]

A defining marker of easternization in cyberspace governance is the gradual shift in norm-setting power from universal institutions such as the UN toward regional frameworks like ASEAN. This process does not entail the wholesale replacement of existing institutions, but instead reflects selective uptake, reinterpretation, and regional localization of norms. Together, these dynamics redistribute influence in global governance and highlight the growing role of Southeast Asia as a normative agent.

The first evidence of this shift lies in the increasing visibility of ASEAN initiatives in multilateral negotiations. ASEAN is the only regional institution to have formally committed to implement the UN GGE 2015 norms, reaffirming this pledge at the 32nd ASEAN Summit (2018).[413] This commitment was operationalized through the ASEAN Checklist for Implementation and related ministerial statements, which were subsequently presented by ASEAN states in UN OEWG debates. While UN reports may not always cite ASEAN directly, ASEAN's inputs consistently appear in member state submissions, with Singapore and Indonesia in particular positioning ASEAN as a collective model for norm uptake. This demonstrates that ASEAN does not simply co-exist with global norm-making but actively feeds regional experiences back into global forums, influencing the language and priorities of UN-level discussions.[414]

At the same time, ASEAN's repackaging of global norms into region-specific mechanisms signals a more subtle redistribution of authority. The UN GGE norms remain the global reference point, but ASEAN translated them into the ASEAN Checklist for

[412] François Delerue, Arun Sukumar, and Dennis Broeders, *Responsible Behaviour in Cyberspace: Global Narratives and Practice* (EU Cyber Direct, 2023), https://doi.org/10.2815/643871.
[413] Association of Southeast Asian Nations (ASEAN). "32nd ASEAN Summit." ASEAN, April 25–28, 2018. https://asean.org/32nd-asean-summit/
[414] Cloramidine, Feline & Wibisono, Ali. (2024). Global Cyber Norms Subsidiarity (UN GGE and UN OEWG) within ASEAN's Body. Hasanuddin Journal of Strategic and International Studies (HJSIS). 2. 21-37. 10.20956/hjsis.v2i2.35313.

Implementation; a voluntary, consensus-based tool adapted to Southeast Asia. Regional workshops hosted by Singapore and Malaysia to operationalize the GGE norms further demonstrate ASEAN's causal role: these initiatives facilitated domestic adoption in several AMS, showing that regional mechanisms acted as the pathway through which global norms were internalized nationally.[415] By operationalizing global norms in this way, ASEAN preserves the UN's authorship but asserts control over their application. This partial decentralization illustrates easternization not by rejecting global rules, but by regionalizing their meaning and relevance. As Tan and Ang note, ASEAN does not subscribe wholesale to European or American interpretations of cyberspace governance; rather, it adopts a pragmatic approach that selectively confirms the application of international law while leaving its precise meaning ambiguous.[416]

This assertiveness, however, is uneven**. In infrastructure and standardization, ASEAN remains a norm-taker, adopting ITU benchmarks rather than projecting regional alternatives. Here, authority remains firmly in the hands of global technical institutions, revealing the limits of ASEAN's normative influence**. The absence of regional norm entrepreneurship in this domain tempers the broader easternization narrative, underscoring that its reach varies across issue areas.

By contrast, in the economic dimension, ASEAN demonstrates genuine norm entrepreneurship. The ASEAN Digital Integration Framework and e-Commerce Agreements exemplify region-driven initiatives that exceed both UN and EU outputs. Malaysia and Thailand, for instance, explicitly referenced the ASEAN Digital Integration Framework in their national e-commerce roadmaps, illustrating how ASEAN-originated instruments shape domestic regulatory priorities. Beyond the region, ASEAN's digital trade principles have been cited in discussions around RCEP negotiations, reinforcing ASEAN's role as a broker of digital economy norms.[417] These instruments are not derivative of Western frameworks but emerge directly from regional priorities, positioning ASEAN as a leader in digital economy governance. Crucially, the UN plays only a marginal role in this domain, highlighting a significant reallocation of authority from universal to regional venues. **Here,**

[415] *Ibid*
[416] Tan and Ang, ASEAN Ambiguity on International Law, 138
[417] Feline and Wibisono, Global Cyber Norms, 27

easternization manifests most clearly: the East actively produces new norms rather than merely adapting existing ones.

Looking across modalities, the pattern is consistent: the UN remains the author of abstract global principles, while ASEAN increasingly shapes their practical implementation. Through checklists, toolkits, and ministerial statements, ASEAN ensures that global norms are localized in line with its consensus-driven style. This filtering role has been explicitly acknowledged in OEWG discussions, where ASEAN is presented as bridging Western multi-stakeholder approaches and sovereignty-focused models promoted by China and Russia. In this way, ASEAN acts not only as a regional adapter but as a translator and broker, mediating between competing global visions.[418] For instance, ASEAN has mapped its Charter principles of sovereignty, non-intervention, and human rights directly onto the 2015 UNGGE cyber norms, thereby demonstrating its ability to reinterpret global principles through a regional legal vocabulary.[419]

Finally, the overlap between domestic and global authorities reinforces this dynamic. The UN promotes a multi-pillar governance agenda spanning security, economy, rights, and development, but ASEAN member states have selectively internalized only the security (APSC) pillar. AEC and ASCC pillars remain underdeveloped, reflecting ASEAN's filtering of global priorities. Moreover, ASEAN member states often enact domestic cyber laws that reflect but do not directly adopt global instruments such as the Budapest Convention, thereby confirming alignment with global standards without conceding interpretive control.[420] A good example is Singapore's cybersecurity law,[421] which centres on the protection of critical infrastructure, compared with Vietnam's cyber law,[422] which prioritizes data localization and content control.[423] Both are broadly consistent with international frameworks but framed through divergent domestic priorities, illustrating ASEAN's pluralized, localized approach to norm uptake. These domestic divergences, when justified by reference to ASEAN's

[418] *Ibid* 22
[419] *Ibid*
[420] *Ibid*
[421] Singapore Cybersecurity Act, 2018 Parliament of Singapore, https://sso.agc.gov.sg/Acts-Supp/9-2018/
[422] Vietnam Law on Cybersecurity, 2018, https://www.economica.vn/Content/files/LAW%20%26%20REG/Law%20on%20Cyber%20Security%202018.pdf
[423] Tan and Ang, ASEAN Ambiguity on International Law, 138

collective strategies, further demonstrate that ASEAN functions as the conduit through which global norms are reinterpreted in practice.

In sum, the shift in norm-setting power is layered rather than absolute. The UN continues to produce overarching norms, but ASEAN increasingly defines their meaning in practice, while in domains such as the digital economy it acts as an autonomous norm-setter. By tracing ASEAN's translation of UN norms into regional mechanisms, its spillover into domestic law, and its recognition in UN debates, this section demonstrates causation rather than mere correlation. This selective uptake, regional reinterpretation, and issue-specific entrepreneurship collectively embody easternization in cyberspace governance: a steady redistribution of authority away from Western, law-centric universality toward Southeast Asian, consensus-driven pluralism.

2. Decentralization of governance

Another key marker of easternization lies in the gradual decentralization of cyberspace governance. Instead of consolidating authority within a single hierarchical regime, governance has become increasingly dispersed across bilateral, regional, and multilateral levels, producing a dense regime complex. Within this landscape, ASEAN has emerged as a critical actor (not by centralizing authority in the manner of the European Union) but by cultivating a decentralized governance model that privileges voluntary coordination, political trust, and regional ownership. This divergence is rooted in what Tan and Ang describe as ASEAN's deliberate ambiguity toward international law: it confirms general commitments while avoiding rigid centralization, thereby preserving flexibility in how norms are interpreted and applied.[424]

The contrast with the EU is most visible in the security domain. The EU institutionalizes cybersecurity through binding directives and supranational regulations, which are enforceable across member states. ASEAN, by contrast, operates through non-binding consensus and informal mechanisms. Its partnerships (such as cooperation with Japan on Critical Information Infrastructure Protection) bypass global institutions altogether and instead advance targeted bilateral or regional arrangements. This stands in sharp contrast to the EU's hierarchical approach, where supranational institutions define obligations, monitor

[424] Ibid 143

compliance, and impose penalties. ASEAN's model fragments authority but also reduces dependence on centralized multilateral forums, reflecting a distinctively pluralistic mode of governance.

Infrastructure and standardization follow the same pattern. While the EU uses harmonized legal instruments to enforce technical standards across its internal market, ASEAN develops regionally specific frameworks that coexist alongside ITU global anchors without imposing uniform obligations. This generates overlapping reference points for states, embedding diversity in implementation. Unlike the EU, which aims at legal coherence through supranational enforcement, ASEAN embraces a decentralized approach that tolerates variation and asymmetry as a matter of design.

Development governance similarly illustrates this divergence. The ASEAN Regional Forum's Work Plan explicitly commits to "building on" UN and OEWG outputs without duplicating them. This language signals ASEAN's choice to integrate global norms selectively while retaining control over how they are operationalized. By contrast, EU development governance often prescribes standardized models for implementation, reinforcing hierarchy. The ITU's recognition of regional offices further legitimizes ASEAN's decentralized role, suggesting that fragmentation is not merely tolerated but institutionally validated. The economic domain highlights perhaps the sharpest contrast. In Europe, digital economy governance is tightly bound to the Digital Single Market and enforced through supranational regulations such as the GDPR. Southeast Asia, by contrast, relies on ASEAN-driven instruments like the ASEAN Digital Integration Framework and the ASEAN Agreement on e-Commerce, which are voluntary and adaptable. These frameworks are not Western imports but region-driven innovations reflecting Southeast Asia's priorities. This shift underscores how decentralization allows ASEAN to function as an autonomous rule-maker without replicating the EU's supranationalism.

The law modality deepens this divide. Whereas the EU converges around binding, enforceable legal frameworks, ASEAN relies almost entirely on non-binding commitments, soft-law instruments, and national-level legislation. This is not simply a matter of capacity but a conscious choice: ASEAN's integration proceeds without legal supranationalism, advancing instead through political consensus, pragmatic cooperation, and the preservation

of sovereignty.[425] In place of the EU's rigid, centralized legalism, ASEAN offers an alternative model of regionalism: horizontal, pluralistic, and adaptive.

In sum, **decentralization in cyberspace governance exemplifies easternization by highlighting ASEAN's divergence from Western institutional models. The EU centralizes authority through law; ASEAN disperses it through norms, markets, and voluntary frameworks.** This does not negate the role of global institutions but dilutes their monopoly, embedding governance within a more pluralistic and decentralized order in which Southeast Asia plays an increasingly influential role.

3. Cultural and philosophical shifts

The easternization of cyberspace governance is visible not only in institutional design but also in the cultural and philosophical assumptions that underpin regulatory choices. A comparison between ASEAN, the UN, and the EU reveals a profound divergence in the normative foundations of governance. Whereas Western institutions continue to treat binding law as the apex of regulatory legitimacy, ASEAN privileges consensus-based decision-making, voluntary norms, and developmental pragmatism. This divergence demonstrates that global cyberspace governance is no longer shaped solely by the logic of legal centralization but increasingly by alternative philosophies rooted in Southeast Asian political culture.[426]

The contrast is most apparent in the domain of security. The EU has pursued a distinctly legalistic path, producing directives (such as NIS2), regulations, and enforcement mechanisms that bind its member states to a harmonized cybersecurity regime. This reflects a hierarchical mode of regime complexes, where central institutions are designed to exercise authority over member states and resolve normative conflicts through binding law.[427] ASEAN, by contrast, relies on ministerial declarations, voluntary checklists, and capacity-building initiatives. These lack binding legal force but derive legitimacy from shared political will and mutual restraint. Such reliance on non-binding measures is not merely an institutional weakness; it reflects ASEAN's philosophy of non-interference and gradual consensus.[428] Referencing practices make this divergence clearer: ASEAN and the UN often

[425] *Ibid*
[426] *Ibid*
[427] Henning et al., Hierarchy and Differentiation in International Regime Complexes, 2183
[428] Tan and Ang, ASEAN Ambiguity on International Law, 144

acknowledge one another's instruments, while the EU largely operates within a self-referential legal order. This asymmetry suggests different normative orientations: **ASEAN embraces permeability and adaptation, whereas the EU reinforces the autonomy of its legal system**.[429]

Development governance further illustrates this philosophical divide. While development cooperation might seem a domain conducive to binding commitments, ASEAN resists legalization even here, favouring facilitative frameworks and voluntary coordination. That ASEAN avoids hard law in a low-conflict domain indicates a principled preference rather than mere incapacity. It illustrates how the consensus norm remains embedded across issue-areas, reflecting a cultural attachment to gradualism and flexibility.

Economic governance highlights the divergence even more starkly. The EU regulates the digital economy through binding trade law, competition policy, and market compliance instruments. This embodies the Western tradition of embedding integration within rule-based and legalistic systems of governance, ensuring uniformity through law.[430] ASEAN, in contrast, frames digital integration around connectivity, inclusivity, and small business participation. Its regulatory discourse is not limited to legal ordering but is explicitly tied to regional identity formation; digital economy governance becomes a tool of community-building and solidarity rather than pure market liberalization. This embedding of normative aspirations within economic regulation exemplifies ASEAN's pragmatic but culturally rooted philosophy of governance.

The distribution of regulatory modalities reinforces this interpretation. For the UN and EU, law remains the "gold standard" of legitimacy, with norms and markets as secondary instruments. For ASEAN, law is one tool among many, often outweighed by norms and market mechanisms. To interpret this merely as a capacity deficit would be misleading. Instead, it reflects ASEAN's deliberate subordination of law to consensus and practical cooperation.[431] This modality pluralism represents a philosophical alternative to Western legalism and is itself a key marker of easternization.

[429] Alter and Meunier, The Politics of International Regime Complexity, 17
[430] *Ibid*
[431] Tan and Ang, ASEAN Ambiguity on International Law, 144

Finally, the broader framing of cyberspace governance reflects these cultural divergences. Western models consistently link cyberspace to rights, freedoms, and competitive markets, reinforcing liberal assumptions of governance. ASEAN, however, interprets cyberspace through a security-first, state-centric lens, in which sovereignty and stability form the parameters of legitimacy. Its guiding philosophy of "unity without supranational law" encapsulates this worldview: integration is sought, but without the binding legal centralization characteristic of the EU. Hierarchical regime complexes such as the EU reduce fragmentation through central authority, but at the cost of adaptability.[432] ASEAN deliberately rejects this model, preferring a decentralized, flexible order that privileges harmony, pragmatism, and resilience over formal legalism.

Cultural and philosophical divergences show that easternization is not only about relocating governance venues but also about redefining the substance of governance itself. By privileging consensus, developmental pragmatism, and modality pluralism, ASEAN advances an alternative conception of legitimacy in cyberspace governance. What appears as fragmentation from a Western perspective can thus be read as the institutionalization of a distinct governance philosophy: one that reflects Southeast Asian traditions and gradually reshapes the normative contours of the global order.

4. Regulatory self-reliance

A central indicator of easternization in cyberspace governance lies in the growing trajectory of regulatory self-reliance across ASEAN. Unlike the EU, which embeds member states within a supranational legal order, or the UN, which seeks to universalize binding norms, ASEAN and its member states have opted for a more autonomous, nationally anchored approach. Over time, ASEAN states have multiplied domestic cyber laws; such as Indonesia's Personal Data Protection Act,[433] Singapore's Critical Information Infrastructure

[432] Henning et al., Hierarchy and Differentiation in International Regime Complexes, 2183
[433] Indonesia, Law No. 27 of 2022 concerning Personal Data Protection (Personal Data Protection Act). Enacted October 17, 2022.

regulations,[434] and Malaysia's digital economy acts,[435] while the regional level has advanced cooperative frameworks without legal compulsion. This reflects a deliberate strategy: to engage selectively with global lawmaking processes while retaining sovereignty over implementation. In effect, ASEAN safeguards policy autonomy while still participating in global cyber governance on its own terms, marking a distinct departure from the Western law-centric model.[436]

This tendency is particularly visible in the legal modality. Whereas the UN and EU converge around binding conventions, treaties, and regulations, ASEAN operates almost entirely outside that overlap. Its preference is for non-binding declarations, hybrid architecture–norm initiatives, and market-oriented instruments. The upcoming signing of the UN Cybercrime Convention in October 2025, hosted in Vietnam, illustrates this dynamic.[437] ASEAN states will likely join the 193 parties by signing the instrument, but (as historical precedent suggests) ratification and full domestic incorporation will be delayed or selectively applied. In this way, ASEAN signals participation in the global process without fully conceding legal sovereignty. Hosting the signing in Vietnam further underscores ASEAN's growing procedural visibility in global cyber governance, even as the locus of regulatory authority remains primarily national and regional. More importantly, this moment can be interpreted as a litmus test for ASEAN's regulatory philosophy: whether it will deepen alignment with global legalism or continue privileging selective engagement as a form of easternization.

The same logic extends across other governance domains. In security, the EU's approach reflects a hierarchical regime complex: centralized, binding frameworks that harmonize member states under supranational authority.[438] ASEAN, by contrast, advances its own frameworks for critical information infrastructure protection and regional cybersecurity declarations. Though modest in scope, these instruments demonstrate a form of embryonic

[434] Singapore, Cybersecurity Act, with Cybersecurity (Critical Information Infrastructure) Regulations 2018 (in force August 31, 2018), and the Cybersecurity Code of Practice for Critical Information Infrastructure, Second Edition (CCoP2.0) (effective July 4, 2022)
[435] Malaysia, Digital Signature Act 1997 (Act 562); Computer Crimes Act 1997 (Act 563); Communications and Multimedia Act 1998 (Act 588). Also, Malaysia Digital Economy Blueprint (MyDIGITAL). Putrajaya: Economic Planning Unit, Prime Minister's Department, 2021 (launched 2021)
[436] Tan and Ang, ASEAN Ambiguity on International Law, 144
[437] United Nations. Proposed United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. To be signed in October 2025, Vietnam (forthcoming).
[438] Henning et al., Hierarchy and Differentiation in International Regime Complexes, 2183

legal and technical self-reliance, privileging regional ownership over supranational imposition. In infrastructure, **ASEAN continues to rely heavily on ITU standards, suggesting dependency. Yet this reliance can be read not as weakness but as a sector-selective strategy: adopting global anchors where necessary, while innovating regionally in domains where autonomy is more feasible**.

The development domain further illustrates this selective engagement. ASEAN documents consistently reference UN frameworks, but their implementation rests on ASEAN-specific procedures that allow member states to retain control. The absence of structured ASEAN–EU engagement in development (apart from ad hoc bilateral agreements such as the EU–Malaysia Framework Agreement) highlights ASEAN's preference for intra-regional and bilateral governance over cross-regional, hierarchical coordination.[439] Similarly, in the economic domain, ASEAN has produced independent instruments such as the ASEAN Agreement on e-Commerce and the ASEAN Digital Integration Framework. These do not replicate WTO, GATS, or TRIPS templates but instead reflect region-driven priorities, positioning ASEAN as an emerging hub for digital economy governance.

Equally important is the modalities mix ASEAN employs. Unlike the UN and EU, which privilege law as the central mode of regulation, ASEAN experiments with flexible combinations such as architecture × norms or market × norms. The ASEAN Digital Masterplan 2025, for instance, references ITU standards but embeds them within a broader framework that emphasizes inclusivity, economic growth, and capacity-building. This hybrid approach demonstrates that ASEAN is not attempting to replace global anchors wholesale but is instead constructing adaptive, region-specific regulatory instruments.

Taken together, these patterns reveal a trajectory of regulatory self-reliance in Southeast Asia. At the national level, member states rely on domestic legal instruments as the backbone of cyber governance. **At the regional level, ASEAN produces cooperative frameworks that reinforce autonomy without binding supranational authority. At the global level, ASEAN engages selectively, signing and referencing instruments when politically advantageous but resisting full legal integration**. This constellation of practices illustrates easternization: the consolidation of a third regulatory pole within the cyber regime complex, one that blends national sovereignty, regional pragmatism, and selective engagement with

[439] Alter and Meunier, The Politics of International Regime Complexity, 17

global law.[440] In this way, ASEAN is not only a participant in global cyberspace governance but increasingly a trend-setter, demonstrating how non-Western approaches can redefine the normative and institutional contours of international law itself.

5. Values and principles divergence

The final dimension of easternization in cyberspace governance emerges in the divergence of values and principles underpinning institutional practices across regions. Whereas the UN and EU continue to anchor their frameworks in formal legality, enforceability, and universalist normative claims, ASEAN embeds its governance philosophy in consensus, developmental pragmatism, and flexibility. This divergence is not simply procedural but reflects deeper cultural and political traditions that shape each region's regulatory ethos. It also explains why cyberspace governance is fragmenting into distinct normative pathways.[441]

In the security domain, the contrasts are particularly sharp. UN General Assembly resolutions and OEWG processes frame cybercrime primarily through criminal law enforcement, emphasizing state responsibility, international cooperation, and capacity-building assistance. The EU, by contrast, constructs its security governance around technical resilience and regulatory compliance, as seen in instruments such as the NIS2 Directive and the EU Cybersecurity Act. Here, security is tied not only to law but also to the binding alignment of markets, infrastructures, and private actors with enforceable standards. ASEAN adopts yet another philosophy: cooperative capacity-building. Its initiatives stress shared resources, regional coordination, and non-binding commitments rather than enforceable legal regimes. In this sense, ASEAN reflects a governance culture where legitimacy derives from consensus and inclusivity, rather than legal compulsion.[442]

In infrastructure governance, divergence is less pronounced. All three regions broadly converge on ITU-driven standards and global development metrics, suggesting that easternization is uneven across thematic scopes. Where global harmonization is technically indispensable, ASEAN aligns itself with international anchors. Yet even here, ASEAN

[440] *See* Alter and Meunier. and Henning et al., "Hierarchy and Differentiation in International Regime Complexes: A Theoretical Framework for Comparative Research"
[441] *Ibid*
[442] Tan and Ang, ASEAN Ambiguity on International Law, 144

emphasizes adaptation and accessibility, situating infrastructure development within a broader narrative of digital inclusivity and regional integration rather than strict compliance with uniform technical benchmarks.[443]

The divergence is more striking in the economic domain. ASEAN's economic instruments (such as the ASEAN Digital Integration Framework and the ASEAN Agreement on e-Commerce) prioritize regional development, inclusivity, and pragmatic cooperation. By contrast, the EU and UN embed economic governance within broader commitments to rights, enforceability, and legal compliance. The EU, in particular, advances a rule-based economic model grounded in competition law, consumer protection, and rights safeguards. ASEAN, however, frames the digital economy as a vehicle for regional cohesion and empowerment, focusing on MSMEs, digital connectivity, and equitable growth. This divergence reflects an east–west philosophical split: legal formalism in the West versus developmental pragmatism in Southeast Asia.[444]

The distribution of regulatory modalities further reinforces this values divergence. UN and EU documents converge around a law–norm overlap, projecting stability, security, and binding order as the preferred governance template. ASEAN, by contrast, Favors norm–market and norm–architecture overlaps, emphasizing flexibility, inclusivity, and developmental outcomes. This points to easternization at the level of values: ASEAN consciously resists the primacy of binding law and instead institutionalizes a governance philosophy rooted in voluntary consensus, collective development, and adaptive cooperation.

Taken together, these divergences reveal that easternization is not only about the relocation of governance venues or the balance of modalities but also about the normative underpinnings of governance itself. ASEAN's emphasis on inclusivity, pragmatism, and consensus reflects a governance philosophy that is qualitatively distinct from the legalism of the UN and EU. This cultural and normative divergence, embedded in ASEAN's institutional practice, represents a critical dimension of *easternization in cyberspace governance: the emergence of alternative philosophies of order that recalibrate what counts as "legitimate governance" in the global digital domain.*

[443] Laura, The Global War, 784

[444] Laura Gómez-Mera, "International Regime Complexity," in *Oxford Research Encyclopedia of International Studies* (Oxford University Press, 2021), https://doi.org/10.1093/acrefore/9780190846626.013.648.

E. Broader implications for international law

The preceding analysis has shown how the rise of Southeast Asia's cyberspace governance frameworks contributes to what can be described as the **easternisation of international law**. This argument rested on a systematic mapping of cyberspace governance using Lessig's theory of regulability, which provided a conceptual lens to evaluate the interplay of law, norms, market, and architecture across institutional and regional levels. On this basis, fragmentation and regime complexity in cyberspace were identified, revealing not only overlapping and contested institutional claims but also distinctive regional approaches. The comparison between the UN, EU, and ASEAN underscored how ASEAN states, while engaging global and Western frameworks, increasingly develop their own regimes, referencing external models selectively rather than adopting them wholesale. Viewed through the regime complex framework, **ASEAN's governance philosophy emerged as distinct: pragmatic, non-binding, consensus-driven, and anchored in regional developmental priorities.**

Such findings cannot be confined to cyberspace alone. They carry broader implications for the structure and trajectory of international law as a whole, particularly in rapidly developing and technologically sensitive domains such as artificial intelligence and outer space. Cyberspace thus becomes a prism through which wider transformations in the authority, legitimacy, and normative underpinnings of international law can be observed.

One implication concerns the shifting authority structure of international law. The Asia-Pacific region, long underrepresented in the making of international legal norms, is increasingly shaping the field. Despite being home to a significant share of the world's population and economy, Asian states historically remained peripheral to international law's development. This imbalance is now being redressed, driven by both threats (climate change, human rights violations, and cyber insecurity) and opportunities such as regional economic integration and the proliferation of legal mechanisms.[445] Since the end of the Cold War, this has manifested in the creation of institutions such as the ASEAN Regional Forum (ARF), designed in part to accommodate regional hegemons and in part to allow smaller states to shape their environment. Meanwhile, larger actors such as China and India have advanced evolving norms on climate

[445] *See* Chesterman Simon, Owada Hisashi, and Saul Be, *The Oxford Handbook of International Law in Asia and the Pacific* .

change, cyber governance, energy security, trade, and outer space (Sidhu, in Chesterman). In the cyberspace domain, ASEAN's frameworks demonstrate this broader dispersion of authority: rather than binding supranational regimes, governance authority is dispersed horizontally across national and regional levels, creating a multipolar legal landscape. **Authority is no longer exercised solely through universal treaties but is negotiated among plural institutional venues.**

A second implication relates to legitimacy. The author argues that international law's inherently global nature ensures that overlapping claims are inevitable: states and regions continuously seek to shape law to advance their own positions, often in opposition to its supposed universalist origins. "Contributionism" has thus become a justificatory tool for Third World states to assert their role in law's creation. Yet the legitimacy of international law is now increasingly pluralized. Great power ambitions and geopolitical contestation have made existing legal frameworks inadequate, even to the point of requiring a "restart."[446] Cyberspace governance illustrates this tension: the UN relies on universalist resolutions, the EU on binding regulatory compliance, and ASEAN on consensus-based declarations. Each claims legitimacy, but on different grounds; formal legality, enforceability, or inclusivity. This suggests that **international law's legitimacy now derives not only from binding instruments but also from justificatory practices across overlapping institution**s, where consensus and ownership can confer as much legitimacy as formal law.

Third, easternisation in cyberspace governance demonstrates how international law itself is being recalibrated. Traditional international law, based on states as primary subjects and sources confined to treaties, custom, precedents, and general principles, often proves too rigid to address contemporary challenges. Climate change, artificial intelligence, and other global technological transformations reveal the limitations of this model. Posthuman theory has further exposed the Eurocentric underpinnings of international law, built on the universalized image of "Man" as rational, sovereign, and progressive; an image deeply tied to colonial expansion and Western modernity. In cyberspace, these assumptions persist in Western approaches privileging enforceability and formal legality. By contrast, **ASEAN's consensus-driven, pragmatically developmental, and hybrid modality frameworks recalibrate the field.** They reveal an alternative regulatory philosophy that resists the universalism of law-

[446] Tikk-Ringas, International Cyber Norms Dialogue as an Exercise of Normative Power, 3

centric models and foregrounds flexibility, inclusivity, and regionally grounded pragmatism. This reconstitution of international law through easternisation does not signify rejection but rather adaptation; an assertion of plural visions of order that weaken the hegemony of Eurocentric legalism.

Finally, the findings carry implications for the discipline of international law itself. Cyberspace demonstrates that international law can no longer be conceptualized as a single, coherent system cantered on treaties and customary rules. Instead, it functions as a regime complex in which binding and non-binding instruments, universalist norms, and regional practices coexist. This raises critical questions: whose values underpin legitimacy? Can coherence be maintained when authority is so fragmented? How should universality be reconciled with plural, even divergent, governance philosophies? Rather than pathologizing fragmentation, scholars may need to reconceptualize it as the institutionalization of regulatory pluralism. From this perspective, **easternisation represents more than a regional phenomenon: it is a structural transformation of international law itself, normalizing the coexistence of alternative philosophies of order and recalibrating what counts as legitimate governance in the global domain.**

In this sense, cyberspace governance is an early test site. The easternisation visible in ASEAN's approaches foreshadows similar transformations in other domains shaped by technological disruption and rapid development, from AI to space governance. International law will increasingly need to operate in a multipolar, plural, and contested environment: an order where legitimacy stems as much from inclusivity, pragmatism, and adaptability as from enforceable legal form.

CHAPTER V
CONCLUSION

A. Summary of findings

The mapping exercise establishes that international cyberspace governance remains fragmented, soft-law heavy, and regionally pluralized. Across 148 instruments, the global order is shaped less by binding treaties than by strategies, declarations, and cooperative frameworks. Binding law exists but is unevenly distributed: the EU leads in enforceable regulation, the UN functions primarily as a forum for global norms, and ASEAN advances consensus-driven but non-binding frameworks. Governance activity surged after 2015, peaking in 2021, reflecting the securitization of cyberspace in response to major cyber incidents and accelerated digital transformation during the COVID-19 pandemic. Once peripheral to international law, cyberspace has now become central to global governance debates. ASEAN's output is notable: collectively, the region and its member states have produced more instruments than the UN and EU combined, indicating the emergence of a regionally distinctive normative presence. While the UN and EU continue to hold formal authority, ASEAN's thematic focus and procedural distinctiveness demonstrate that cyberspace governance is no longer exclusively Western-led. Nearly two-thirds of instruments originate domestically, confirming that national legal systems remain the backbone of cyber regulation, while thematic emphasis highlights security as dominant, complemented by ASEAN's economic frameworks linking digital governance with regional integration and developmental goals.

The analysis shows that international cyberspace governance is modality-diverse rather than law-centric. Norms dominate at global and regional levels, particularly through UN-led principles and ASEAN's consensus-based mechanisms, while binding law is concentrated at the domestic level or within the EU's supranational system. Regional divergence is evident: the EU anchors governance in binding law, the UN primarily produces norms, and ASEAN favours non-binding instruments and hybrid technical-market approaches. This variation reflects different regulatory philosophies, explaining both fragmentation and regime complexity. Hybrid instruments further illustrate practical governance adaptation, though they also increase overlap and potential inconsistency. Collectively, these findings confirm the relevance of Lessig's framework for mapping international cyberspace governance and show

how ASEAN's approach contributes to easternisation—not by overturning Western models, but by establishing regionally distinctive ways of interpreting, operationalizing, and selectively complementing global norms.

Fragmentation manifests horizontally across institutions and vertically across authority levels. Thematic fragmentation privileges security while other domains such as human rights, economy, socio-cultural issues remain peripheral. Institutional divergence shows the UN emphasizing norm diffusion, the EU enforcing binding regulation, and ASEAN promoting non-binding declarations and cooperative frameworks. Vertical fragmentation arises from the uneven translation of global norms into regional or national law: ASEAN member states adopt domestic cyber laws that often diverge in scope and implementation, and regional frameworks lack harmonizing authority. This confirms that cyberspace governance proliferates through overlapping and partially inconsistent logics rather than converging into a single legal order.

These dynamics collectively generate a regime complex: overlapping institutions pursue similar objectives without hierarchical coordination. Security, infrastructure, and developmental domains are characterized by parallel frameworks, some referencing each other, others operating independently. Economic initiatives further illustrate region-driven norm entrepreneurship, particularly ASEAN's digital economy agreements, which exist alongside global frameworks. This non-hierarchical coexistence produces both positive spillovers, such as operationalizing UN norms regionally, and challenges, such as duplication and legal uncertainty.

Finally, the analysis demonstrates that ASEAN's governance trajectory exemplifies easternisation in cyberspace law. ASEAN selectively interprets and implements global norms, redistributes normative influence within the region, and develops autonomous instruments in domains like the digital economy. Governance is increasingly decentralized, favouring regional and bilateral arrangements that complement rather than replicate Western-centric institutions. Cultural and philosophical divergences such as consensus, pragmatism, and voluntary cooperation further distinguish ASEAN's approach from EU legalism or UN universalism. Regulatory self-reliance is evident as ASEAN and its members engage selectively with global treaties while preserving sovereignty and shaping domestic and regional frameworks according to local priorities. Together, these patterns illustrate easternisation not as a wholesale transformation of international law, but as the emergence of regionally

distinctive practices that coexist with, adapt, and selectively diverge from Western-dominated models, signalling Southeast Asia's growing role as a normative actor in global cyberspace governance.

B. Challenges and Limitations

While this dissertation offers a systematic and empirically grounded account of international cyberspace governance, it is not without challenges and limitations. These reflect both the nature of the research design and the inherent complexity of the subject matter.

1. Data collection and availability

The first limitation concerns the scope and availability of the dataset. Although the study systematically collected 148 instruments across the UN, EU, ASEAN, and ASEAN member states, it does not represent an exhaustive corpus of all potentially relevant documents. Notably, the dataset excludes instruments that are not inherently cyber-related but nonetheless shape the digital domain, such as EU regulations governing the internal market or the Digital Single Market. These omissions were deliberate, aimed at maintaining analytical focus, but they narrow the lens of governance mapping. Similarly, court judgments and case law (which exert significant influence in some regions) particularly within the EU, were excluded to preserve comparability across regions. While these decisions ensured consistency, they inevitably limit the generalizability of findings and mean that certain normative or jurisprudential developments fall outside the scope of the analysis.

A further limitation concerns uneven coverage across regions. While UN and EU repositories provide comprehensive and centralized access to official instruments, ASEAN and several of its member states have less systematic publication practices, with many documents available only in national languages or scattered across government portals. Although multiple repositories were consulted to mitigate this gap, the possibility remains that some instruments were missed or under-represented. This coverage asymmetry may bias east–west comparisons by overstating the density of Western legal instruments relative to Southeast Asia, even where governance activity exists but is less formally documented.

2. Methodological suitability, quality, and feasibility

A second set of challenges arises from the methodological approach itself. Computational legal studies offer powerful advantages, particularly their ability to process large volumes of documents and reveal macroscopic patterns that would be invisible through close doctrinal reading. As Lie and Langford emphasize, these approaches provide "distant reading" tools that can complement doctrinal interpretation by uncovering broader networks and hidden regularities. Yet, their strength is also their limitation: computational methods are less suited to answering causal questions or capturing fine-grained interpretive nuance. For example, coding overlap between regimes can identify cross-references, but it cannot on its own explain why such overlaps occurred or how actors understood them. This interpretive gap requires supplementation by qualitative reasoning, which introduces an additional layer of subjectivity.

Quality concerns also extend to both data and method. Computational approaches depend heavily on the completeness and reliability of the underlying corpus, and any omission, misclassification, or processing error risks distorting results. Although validation checks and triangulation were employed, some uncertainty inevitably remains. Likewise, computational tools operate probabilistically, and small coding errors or mis-specified algorithms can generate unexpected outcomes. This raises a broader feasibility challenge: most international lawyers, including the author of this dissertation, are trained in doctrinal methods rather than computational ones. Engaging with such methods requires either moderation of ambition, collaboration, or careful adaptation of computational tools into a legal framework. This study pursued the first of these strategies, using accessible classification and visualization methods (e.g., Tableau) to complement qualitative interpretation, while recognizing that deeper machine learning applications would exceed its technical and disciplinary scope.

3. Applicability of Lessig's modalities

Another limitation stems from the analytical framework itself. Lessig's theory of regulability was originally formulated in the context of national and domestic regulation of cyberspace. Its adaptation to the international domain requires conceptual stretching. While the modalities of law, norms, architecture, and market remain useful heuristics, their meanings become less precise when applied to fragmented international regimes. For example, "law" at the international level often takes the form of non-binding resolutions or

regional directives, which lack the same enforceability as domestic legislation. The dissertation addresses this challenge by refining the operational definitions of each modality for international governance, but this remains an interpretive choice that could be contested by other scholars.

4. **Intent vs resource limitations**

The study also faces difficulty in disentangling intent from capacity. ASEAN's reliance on non-binding, consensus-based instruments can be interpreted both as a principled governance philosophy and as a pragmatic response to resource disparities among member states. Similarly, the absence of binding ASEAN-wide legal frameworks may reflect a deliberate preference for soft-law coordination, but it may equally result from limited institutional infrastructure. The findings cannot conclusively determine which of these explanations is primary. Instead, the dissertation treats both as analytically relevant but acknowledges that the ambiguity complicates causal claims about why fragmentation and divergence occur.

5. **Threshold of easternization**

Finally, the greatest limitation lies in the novelty of the easternization concept itself. The research presents easternization as an interpretive framework for identifying normative and institutional divergence in international law, rather than as an established theory with clear benchmarks. As such, the evidentiary threshold for demonstrating easternization is necessarily fluid. The dissertation does not claim that Southeast Asia has fundamentally transformed the global legal order, but that it provides recurring, empirical indicators of alternative pathways. These findings remain provisional, and further evidence will be needed to determine whether the trends identified here consolidate into a more durable structural shift.

Taken together, these challenges do not undermine the dissertation's findings but contextualize them. They highlight the balance between breadth and depth, between computational scalability and interpretive nuance, and between theoretical innovation and empirical caution. By acknowledging these limitations, the study aims to situate its claims within the evolving methodological debates of international law and to provide a transparent basis for future research to refine, expand, or contest its conclusions.

C. Directions for future research

The limitations of this study also open up promising avenues for further inquiry. Four in particular stand out.

1. Toward a more holistic mapping of cyberspace governance

This dissertation has primarily mapped governance through instruments issued by states and international organizations, with a focus on treaties, conventions, declarations, and national legislation. However, as noted in the limitations, the sources of international law remain broader than the categories covered here. Future research could integrate judicial decisions, arbitral awards, and customary law practices to provide a fuller picture of how cyberspace is regulated under the international law framework. Including jurisprudence, particularly from the EU and regional human rights courts, would help to capture the interpretive authority of courts and tribunals, and offer a more balanced comparison between regions where adjudication plays a stronger role. Similarly, incorporating customary practice could clarify whether repeated state behaviour in cyberspace is crystallizing into general rules of international law.

2. Extending comparative mapping beyond ASEAN

The scope of this project was deliberately limited to ASEAN and its member states, compared against the UN and EU, in order to examine the dynamics of easternization in a manageable framework. Future research could broaden this comparison to include other regional actors, such as the African Union, the Organization of American States, or sub-regional initiatives in Latin America or Africa. Such comparative work would allow researchers to test whether the trends observed in Southeast Asia (consensus-driven norm-making, selective integration with global law, and reliance on hybrid modalities) are unique to ASEAN or part of a broader rebalancing in international law. This would also address the limitation of regional focus and contribute to a more global understanding of regime complexity in cyberspace.

3. Substantive testing of Lessig's modalities

In this dissertation, Lessig's modalities were operationalized in a formal and structural way, identifying whether documents carried features of law, norms, architecture, or market.

While this approach captured patterns of modality dominance and hybridization, it did not conduct a deep content analysis of how each modality substantively functions in practice. Future studies could, for instance, analyse how specific legal texts frame enforcement mechanisms, how norms evolve through diplomatic discourse, how architecture constrains behaviour through technical standards, or how markets regulate through trade and competition law. Such a substantive analysis would not only validate the suitability of Lessig's framework for international law but also enrich our understanding of how modalities interact in concrete regulatory settings.

4. Developing easternization as a grounded analytical framework

The concept of easternization has been introduced here as a lens for interpreting regional divergence in cyberspace governance, but it remains a novel and relatively underdeveloped framework in international law scholarship. Future research could test the robustness of this concept through a more grounded, qualitative content analysis of national and regional instruments. This would involve examining not only the form of instruments but also their substantive language (values, principles, and enforcement philosophies) to trace how far they depart from Western legalist traditions. In addition, further empirical work could expand beyond cyberspace to adjacent domains such as artificial intelligence governance or outer space law, testing whether similar patterns of regional norm entrepreneurship, selective integration, and alternative modality balances can be observed.

In sum, these directions underscore that the present research should be seen as an initial mapping exercise rather than a definitive account. By combining broader sources of international law, extending comparative scope, deepening modality analysis, and grounding the concept of easternization more fully, future research can build on this study's foundation to develop a richer and more comprehensive understanding of how global governance in technology-sensitive domains is evolving.

ANNEX A

MASTER DATASET

Link to the full dataset on sheets: https://bit.ly/Masterdataset-HaekalsThesis

UN Documents

ID	Document Title	Source/Link	Year	Country/Region	Level	Institution	Legal Subject	Governance Function	Document Type	Source of IL	Lessig Modality	Main Scope of Regulation	Supporting Scope	Governance Type	Keywords/Indicators	Summary/Notes
1	A/72/327: Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security	https://docs.un.org/en/A/72/327	2017	UN	International	UN General Assembly	IO	Cooperation	Report	General Principles	Norms	Infrastructure and standardization	Security	Algorithmic	Voluntary norms, state behavior, responsible use	Non-binding policy report from a multilateral expert group discussing international cyber threats, application of international law to ICTs, and norms of state behavior. No consensus was reached. Serves as a key reference for evolving norms in cyber governance.
3	Roadmap for **Digital Cooperation** (Report of the Secretary-General)	https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf	2020	UN	International	UN Secretary General	IO	Cooperation	Roadmap	General Principles	Norms	Economy	Development	Institutional	Digital economy, human rights, security, digital cooperation	Role of stakeholders in advancing a safety and more equitable digital world
4	Report of the Office of the United Nations High Commissioner for Human Rights: **The right to privacy in the digital age** (A/HRC/27/37)	https://docs.un.org/en/A/HRC/39/29	2018	UN	International	United Nations High Commissioner for Human Rights	IO	Policy	Report	General Principles	Norms	Human Rights	Human Rights	Institutional	Human rights, privacy, surveillance, personal data	promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council
5	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of **International Security** (A/72/327)	https://docs.un.org/en/A/72/327	2017	UN	International	UN General Assembly	IO	Cooperation	Report	General Principles	Norms	Infrastructure and standardization	Security	Algorithmic	Information security	International law applies to the use of information and communication technologies, confidence building measures
6	Report of the Secretary-General: Strengthening the United Nations **Crime Prevention and Criminal Justice Programme**, in particular its technical cooperation capacity	https://www.unodc.org/documents/treaties/a_res_57/153e.pdf	2002	UN	International	UN Secretary General	IO	Policy	Report	General Principles	Law	Security	Infrastructure and standardization	Institutional	Cyber crime, computerrelated crime	Effective measures to prevent and control computer-related crime
7	Comprehensive Study on Cybercrime UNODC	https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf	2013	UN	International	UNODC	IO	Policy	Strategy Document	General Principles	Law	Security	Security	Institutional	Cybercrime, harmonization, international cooperation, capacity-building, electronic evidence, human rights, jurisdiction, legal frameworks	This UNODC study provides a global review of legal frameworks for addressing cybercrime. It synthesizes national practices and legal models to support harmonization. Key references to general principles of law include: – Jurisdiction doctrines like territoriality and universality, p.183
8	Report of the Secretary-General: Effective measures to prevent and control computer-related crime UNSG	https://digitallibrary.un.org/record/465763?ln=en&v=pdf	2002	UN	International	UN Commission on Crime Prevention and Criminal Justice (CCPCJ)	IO	Policy	Report	General Principles	Law	Security	Infrastructure and standardization	Institutional	Cybercrime, legislation, cooperation, international instruments, harmonization, jurisdiction, encryption, technical capacity, critical infrastructure	This UN Secretary-General report surveys national and international legal developments in countering computer-related crime. It emphasizes legislative modernization, the implementation of model laws, and jurisdictional doctrines (pp. 2–6). It also addresses the tension between law
9	Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children UNODC	https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf	2014	UN	International	UNODC	IO	Policy	Report	General Principles	Law	Security	Security	Institutional	Child abuse, ICT exploitation, digital crime, international instruments, criminal justice	Investigates how new technologies are used in child abuse/exploitation; includes legal analysis, offender profiles, and policy responses.
10	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)	https://docs.un.org/en/A/70/174	2015	UN	International	UN Group of Governmental Experts (GGE)	IO	Policy	Report	General Principles	Norms	Infrastructure and standardization	Security	Algorithmic	Norms of behavior, critical infrastructure, due diligence, state responsibility, human rights	Recommends non-binding norms, emphasizes protection of critical infrastructure and responsible state behavior in cyberspace.
11	Report of the Open-ended working group on developments in the Field of Information and Telecommunications in the Context of International Security A/AC.290/2021/CRP.2	https://dig.watch/wp-content/uploads/2022/08/OEWG-Report.pdf	2021	UN	International	UNGA	IO	Policy	Report	General Principles	Norms	Security	Development	Institutional	Responsible State behavior, critical infrastructure, digital divide, multistakeholderism, trust-building	Reaffirms voluntary norms of State behavior in cyberspace; promotes trust, capacity-building, and multilateral dialogue under UN auspices.
12	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)	https://dig.watch/wp-content/uploads/A_68_98_E.pdf	2013	UN	International	UN GGE	IO	Policy	Report	General Principles	Norms	Security	Development	Institutional	International peace and security, responsible behavior, UN Charter, norms, capacity-building, institutional dialogue	Affirms applicability of international law to ICTs; recommends voluntary norms, cooperative measures, and future dialogues under UN frameworks.
13	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)	https://docs.un.org/en/A/65/201	2010	UN	International	UN Group of Governmental Experts (GGE)	IO	Policy	Report	General Principles	Norms	Infrastructure and standardization	Security	Institutional	International peace, ICT misuse, voluntary cooperation, multistakeholder engagement	Introduces concerns about attribution and misuse of ICTs; stresses confidence-building, trust, and the applicability of international norms.
14	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/60/202)	https://docs.un.org/en/A/60/202	2005	UN	International	UN Group of Governmental Experts (GGE)	IO	Policy	Report	General Principles	Norms	Security	Development	Institutional	Information security, cooperative frameworks, preliminary international discussions	Early GGE report highlighting challenges in consensus-building on ICT security; exploratory in nature.
15	Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (A/76/135)	https://docs.un.org/en/A/76/135	2021	UN	International	UN Group of Governmental Experts (GGE)	IO	Policy	Report	General Principles	Norms	Security	Development	Institutional	Responsible State behaviour, international peace and security, cyber norms, international cooperation, human rights, capacity-building	Expands prior GGE consensus by reaffirming norms, elaborating on confidence-building, international law, and cyber capacity-building; reflects growing normative layering in cyberspace governance.
16	Mapping of International Internet Public Policy Issues	https://unctad.org/system/files/official-document/ecn162015crp2add1_en.pdf	2014	UN	International	Commission on Science and Technology for Development (CSTD), ECOSOC	IO	Cooperation	Report	General Principles	Law, Architecture, Norms	Infrastructure and standardization	Security	Institutional	Internet governance, public policy, intersectoral clusters, ECOSOC, WGEC, enhanced cooperation	Maps 643 mechanisms across 40 thematic issues in Internet public policy. Highlights institutional gaps, coordination challenges, and governance clusters from legal to human rights to economic aspects. Prepared under ECOSOC for WSIS review.
17	Compilation of Preliminary Conclusions and Recommendations from the UNODC Expert Group on Cybercrime	https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/CRP/V2101012.pdf	2021	UN	International	UNODC / CCPCJ	IO	Cooperation	Strategy	General Principles	Law, Architecture, Norms	Security	Security	Legal	cybercrime, criminalization, electronic evidence, capacity-building, Budapest Convention, mutual legal assistance	Consolidates recommendations from global expert meetings on cybercrime covering legislation, enforcement, sovereignty, evidence handling, and cooperation models.
18	Countering the Use of the Internet for Terrorist Purposes - Legal and Technical Aspects, Working Group Compendium	https://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf	2011	UN	International	United Nations Counter-Terrorism Implementation Task Force (CTITF)	IO	Policy	Strategy Document	General Principles	Law	Security	Security	Legal	Terrorism, cybercrime, legal frameworks, human rights, harmonization, jurisdiction, encryption, procedural law, internet governance	This CTITF compendium explores the legal and technical challenges of terrorist use of the internet. It surveys national, regional, and international legal responses and highlights general legal doctrines such as jurisdiction, proportionality, and fundamental rights (pp. 1–9, 186). It emphasizes using existing
19	General Assembly Resolution 75/282 Countering the Use of ICTs for Criminal Purposes	https://digitallibrary.un.org/record/3928637?ln=en&v=pdf	2024	UN	International	UN General Assembly	IO	Legislation	Resolution	General Principles	Law	Security	Security	Legal	Cybercrime, international cooperation, criminal justice, countering criminal use of ICTs	Addresses the global threat of ICT-related crime; supports capacity-building, legal harmonization, and finalization of the new cybercrime convention under UN auspices.
20	Draft UN Convention on Cybercrime	https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf	2023	UN	International	Ad Hoc Committee on Cybercrime	State	Legislation	Convention	Treaties/Convention	Law	Security	Security	Legal	Cybercrime convention, procedural law, international legal cooperation, harmonization	Draft convention text covering substantive and procedural cybercrime law, jurisdiction, enforcement, and international cooperation frameworks. NOT YET IN FORCE. in accordance with article 65(1) which reads as follows: "This Convention shall enter into force on the ninetieth day after the date of
21	General Assembly Resolution 79/243 Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in	https://documents.un.org/doc/undoc/gen/n21/133/51/pdf/n2113351.pdf	2021	UN	International	UN General Assembly	State	Structure	Resolution	General Principles	Law	Security	Security	Institutional	Cybercrime treaty process, Ad Hoc Committee, intergovernmental negotiations	Mandates the establishment of an Ad Hoc Committee to elaborate a comprehensive international convention on cybercrime, marking a structural shift in international legal negotiations.
22	Plenipotentiary Resolution 130 – Strengthening ITU Role in Building Confidence and Security in the Use of ICTs	https://ccdcoe.org/uploads/2018/10/ITU-061124-PPConfSecICT.pdf	2014	UN	International	ITU	IO	Policy	Resolution	General Principles	Law, Architecture	Development	Security	Institutional	trust in ICTs, capacity building, cross-border security cooperation	Expands ITU's mandate to support technical assistance, capacity building, and confidence-building initiatives.
23	Plenipotentiary Resolution 174 (Busan, 2014) – ITU Role in Building Confidence and Security in the Use of ICTs	https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20174.pdf	2014	UN	International	ITU	IO	Policy	Resolution	General Principles	Law, Norms	Development	Security	Institutional	cybersecurity confidence, international cooperation, trust-building, ICT policy	Urges global collaboration and standards alignment on cybersecurity policies and technical capabilities.
24	Global Cybersecurity Agenda – Chairman's Report	https://www.itu.int/en/action/cybersecurity/documents/gca-chairman-report.pdf	2007	UN	International	ITU	IO	Structure	Strategy	Judicial Decisions/Writing	Architecture, Norms	Security	Development	Institutional	focal point, cybersecurity harmonization, multi-stakeholder coordination	Outlines ITU's structural proposals for centralizing cyber coordination efforts under the Global Cybersecurity Agenda framework.
25	International Telecommunication Regulations (Melbourne 1988)	https://www.itu.int/osg/csd/wtpf/wtpf2009/documents/ITU_ITRs_88.pdf	1988	UN	International	ITU	IO	Legislation	Convention	Treaties/Convention	Law, Architecture	Infrastructure and standardization	Infrastructure and standardization	Legal	international regulations, telecom services, accounting, priority telecommunication	A binding international agreement governing telecommunication standards, charges, and principles of cooperation.
26	Cybersecurity Strategy Guide – Second Edition	https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf	2021	UN	International	ITU	IO	Policy	Cooperation	General Principles	Law, Architecture, Norms	Security	Infrastructure and standardization	Institutional	national cybersecurity strategy, lifecycle, governance, risk assessment, policy coordination	Guide for national governments to design and implement cybersecurity strategies, covering legal, technical, and organizational components.
27	Child Online Protection (COP) Policy Brief	https://www.itu.int/en/cop/documents/guidelines-policy%20makers-e.pdf	2020	UN	International	ITU	IO	Policy	Policy Brief	Judicial Decisions/Writing	Norms	Security	Human Rights	Institutional	child protection, online safety, digital rights, capacity building, awareness	Offers policy guidance to governments for implementing child online protection strategies; emphasizes education, legal frameworks, and public awareness.
28	Final Acts of the Plenipotentiary Conference (Bucharest, 2022)	https://www.itu.int/hub/publication/s-conf-actf-2022/	2022	UN	International	ITU	IO	Structure	Conference Final Acts	General Principles	Architecture	Development	Socio-Cultural	Legal	governance structure, strategic planning, ITU mandates, multilingualism, ICT development	Compilation of final decisions, resolutions, and mandates adopted during the ITU Plenipotentiary Conference 2022. Covers budgeting, institutional structure, strategic plans, gender policy, digital inclusion, and language equity.
29	UNIDIR Report A/79/240: Work of the Advisory Board on Disarmament Matters	https://unidir.org/wp-content/uploads/2024/09/UNIDIR_2024_ABDM_Report.pdf	2024	UN	International	UNIDIR / Advisory Board on Disarmament Matters	IO	Structure	Report	General Principles	Architecture	Security	Security	Institutional	Emerging tech, military AI, disarmament, dual-use technologies, foresight	Strategic foresight report assessing peace and security implications of emerging technologies (AI, space, biotech). Covers governance gaps, future risks, and disarmament policy strategies.
30	Resolution A/RES/74/197: ICTs for Sustainable Development	https://docs.un.org/en/A/RES/74/197	2019	UN	International	UN General Assembly	State	Policy	Resolution	General Principles	Norms	Development	Economy	Institutional	ICTs, sustainable development, SDGs, WSIS, gender digital divide, broadband access, e-commerce	GA resolution reaffirming the role of ICTs in advancing sustainable development. Emphasizes digital cooperation, closing digital divides, and promoting inclusive access to technology.
31	Resolution on The right to privacy in the digital age (A/RES/68/167)	https://digitallibrary.un.org/record/764407/files/A_RES_68_167-EN.pdf	2013	UN	International	UN General Assembly	State	Legislation	Resolution	General Principles	Norms	Human Rights	Economy	Institutional	Privacy, digital surveillance, human rights, freedom of expression, accountability, international oversight	Reaffirms privacy as a universal human right; condemns mass surveillance; calls for national reviews and protections of data privacy in line with international human rights law.
32	Resolution on Combating the criminal misuse of information technologies (A/RES/56/121)	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf	2001	UN	International	UN General Assembly	State	Legislation	Resolution	General Principles	Law	Security	Security	Institutional	Cybercrime, high-technology crime, legal frameworks, international and regional cooperation	Reaffirms the approach in Resolution 55/63, emphasizes regional cooperation, calls for national legal reforms, and recognizes ongoing developments like the Budapest Convention.
33	Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)	International peace, ICT misuse, voluntary cooperation, multistakeholder engagement	Introduces concerns about attribution and misuse	UN	International	UN General Assembly	State	Legislation	Resolution	General Principles	Law	Security	Development	Institutional	Computer crime, criminal misuse of ICTs, legal reform, international cooperation, law enforcement, capacity-building	Encourages harmonization of legal frameworks and enhanced law enforcement cooperation to combat cybercrime; urges Member States to address legal and technical challenges posed by digital misuse.
34	Resolution on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures (A/RES/58/199)	https://docs.un.org/en/A/RES/58/199	2003	UN	International	UN General Assembly	State	Policy	Resolution	General Principles	Architecture	Infrastructure and standardization	Infrastructure and standardization	Institutional	Critical infrastructure, cybersecurity, information sharing, international cooperation, threat response	Outlines foundational elements for global cybersecurity culture; emphasizes cross-sectoral partnerships and protection of critical infrastructure.
35	Resolution on the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (A/RES/64/211)	https://docs.un.org/en/A/RES/64/211	2009	UN	International	UN General Assembly	State	Structure	Resolution	General Principles	Architecture	Infrastructure and standardization	Security	Algorithmic	Critical infrastructure protection, public-private cooperation, cybersecurity strategy, capacity-building, assessment tool	Encourages national and international cooperation for critical infrastructure protection; provides a self-assessment tool to evaluate national cybersecurity systems.
36	Resolution on the Creation of a global culture of cybersecurity (A/RES/57/239)	https://docs.un.org/en/A/RES/57/239	2002	UN	International	UN General Assembly	State	Policy	Resolution	General Principles	Norms	Security	Socio-Cultural	Institutional	Cybersecurity culture, societal awareness, international cooperation, best practices, education	Proposes a global culture of cybersecurity built on awareness, ethics, risk assessment, and cooperation among all stakeholders; encourages integration into national efforts and global summits.
37	Kyoto Declaration on Advancing Crime Prevention, Criminal Justice and the Rule of Law	https://www.unodc.org/documents/commissions/Congress/21-02815_Kyoto_Declaration_ebook_rev_cover.pdf	2021	UN	International	UNODC / UN Congress on Crime Prevention and Criminal Justice	State	Policy	Declaration	General Principles	Law, Norms	Security	Development	Institutional	crime prevention, cybercrime, access to justice, digital technologies, international cooperation	Political declaration adopted at the 14th UN Crime Congress emphasizing digital-era crime prevention, international cooperation, and justice system strengthening, including cybercrime.
38	The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation	https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf	2019	UN	International	UN Secretary-General's High-Level Panel on Digital Cooperation	IO	Cooperation	Report	General Principles	Norms, Architecture	Infrastructure and standardization	Human Rights	Institutional	digital governance, cooperation models, human rights, multistakeholderism, digital inclusion	Outlines recommendations for inclusive digital governance, proposing a new cooperation architecture and affirming digital human rights principles.
39	Private Sector Engagement in Responding to the Use of ICT for Terrorist Purposes	https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/private-sector-engagement-in-responding-to-the-use-of-the-internet-and-ict-for-	2021	UN	International	UN Counter-Terrorism Executive Directorate (CTED)	IO	Cooperation	Working Paper	General Principles	Market, Architecture	Security	Socio-Cultural	Institutional	terrorism, ICTs, private sector, multi-stakeholder, content regulation, data exchange	Explores how private technology companies cooperate with governments to prevent terrorist use of ICTs. Emphasizes multistakeholder roles in governance.
40	UN Security Council Resolution 70/237 on Developments in the field of information and telecommunications in the context of international security	https://docs.un.org/en/A/RES/70/237	2015	UN	International	UN Security Council	IO	Cooperation	Resolution	General Principles	Norms	Infrastructure and standardization	Security	Institutional	ICTs, Norms, International Law, GGE, Coopration, Security, International Peace	International law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and
41	UN Security Council Resolution 2341 (2017): Protection of Critical Infrastructure Against Terrorist Attacks	https://digitallibrary.un.org/record/859472?ln=en	2017	UN	International	UN Security Council	State	Legislation	Security Council Resolution	General Principles	Law, Architecture	Infrastructure and standardization	Security	Institutional	critical infrastructure, counterterrorism, international security, ICT vulnerabilities	Encourages states to enhance resilience of critical infrastructure, including digital networks, against terrorist threats. Affirms international cooperation obligations.

EU Documents

42	EU Cybersecurity Strategy 2020	https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0	2020	EU	Regional	European Commission	IO	Policy	Strategy	General Principles	Law, Market, Norms	Development	Legal	Institutional	resilience, digital sovereignty, EU values, trust	Strategic policy framework for building cyber resilience in the EU and globally promoting its values. References regulation, public-private cooperation, and strategic autonomy.
43	EU Data Governance Act	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868	2022	EU	Regional	European Parliament & Council	IO	Legislation	Act	Treaties/Convention	Architecture	Infrastructure and standardization	Infrastructure and standardization	Legal	Interoperability, data infrastructure	Legal framework on data sharing architecture and standards.
44	Budapest Convention on Cybercrime	https://rm.coe.int/1680081561	2001	EU	International	Council of Europe (adopted globally)	State	Legislation	Convention	Treaties/Convention	Law	Security	Security	Legal	treaty, harmonization, cybercrime, legal obligation	Binding treaty that harmonizes national laws on cybercrime and facilitates international cooperation. First and most widely adopted legal instrument in this field.
45	ENISA Mandate (Regulation (EU) 2019/881)	https://eur-lex.europa.eu/eli/reg/2019/881/oj	2019	EU	Regional	European Union	IO	Structure	Regulation	Treaties/Convention	Law, Architecture	Security	Infrastructure and standardization	Legal	cyber agency, operational structure, EU regulation, NIS	Legal framework establishing the role and responsibilities of ENISA, the EU's cybersecurity agency. Defines structure and authority within the European cybersecurity landscape.
46	EU Cyber Defence Policy Framework	https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en	2014	EU	Regional	European Commission & High Representative	IO	Policy	Policy Brief	General Principles	Architecture, Norms	Security	Security	Institutional	EUCDCC, MICNET, strategic compass, cyber rapid response, civilian-military cooperation	Sets ambitious plan to boost EU cyber defence capabilities post-Ukraine war; emphasises detection, deterrence, industry, skills, and NATO cooperation.
47	Cybersecurity Strategy of the European Union	https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391	2013	EU	Regional	European Commission & High Representative	IO	Policy	Communication	General Principles	Architecture, Norms	Security	Infrastructure and standardization	Institutional	resilience, crime, defence, industry, diplomacy	First EU cybersecurity strategy; five priorities incl. resilience & international cyber policy.
48	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures	https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures	2020	EU	Regional (EU)	European Commission & NIS Cooperation Group	IO	Policy	Cooperation	General Principles	Architecture, Norms	Infrastructure and standardization	Infrastructure and standardization	Institutional	supplier risk, 5G, certification, multi-vendor, MANO	Lists strategic & technical measures (supplier vetting, multi-vendor, certification, resilience) for Member States' 5G roll-outs; foundation for national plans & NIS CG monitoring.
49	Coordinated Response to Large Scale Cybersecurity Incidents and Crises (Recommendation)	https://eur-lex.europa.eu/eli/reco/2017/1584/oj/eng	2017	EU	Regional	European Commission	IO	Cooperation	Cooperation	General Principles	Architecture, Norms	Security	Security	Institutional		
50	Resilience, Deterrence and Defence: Building strong cybersecurity for the EU	https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN	2017	EU	Regional	European Commission & High Representative	IO	Cooperation	Communication	General Principles	Architecture, Norms	Security	Infrastructure and standardization	Institutional	resilience, cyber defence, ENISA reform, certification framework, skills	2017 cybersecurity package communication proposing ENISA mandate renewal, EU certification framework & Joint Cyber Unit.
51	CIIP Communication – Protecting Europe from Large-Scale Cyber-Attacks (2009)	On Critical Information Infrastructure Protection- Protecting Europe from large scale cyber-attacks and disruptions- enhancing preparedness, security	2009	EU	Regional	European Commission	IO	Cooperation	Communication	General Principles	Architecture, Norms	Security	Infrastructure and standardization	Institutional	CIIP, preparedness, resilience, ENISA, EPCIP action plan	Sets EU action plan to strengthen security & resilience of critical information infrastructures; precursor to NIS policy.
52	2010 EU Internal Security Strategy in Action: Five Steps towards a more secure Europe	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0673	2010	EU	Regional (EU)	European Commission; EP & Council	IO	Policy	Communication	General Principles	Law, Norms	Security	Infrastructure and standardization	Institutional	cyber-crime, EUROPOL, CERT, enforcement, 2011-14 timeline	Sets 5-year action plan; Objective 3 builds EU cyber-crime capacity incl. EC3 & CERT network.
53	Joint Framework on countering hybrid threats, a European Union response	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016JC0018	2016	EU	Regional	European Commission & High Representative	IO	Policy	Communication	General Principles	Market, Norms	Security	Development	Institutional	hybrid threats, strategic communication, resilience, solidarity clause, NATO cooperation	Provides EU-wide approach to improve awareness, resilience, crisis response against hybrid threats; proposes Hybrid Fusion Cell & EU-NATO coordination.
54	NIS2 Directive	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555	2022	EU	Regional	European Parliament & Council	IO	Legislation	Directive	Treaties/Convention	Law	Security	Infrastructure and standardization	Institutional	risk-management, incident reporting, essential & important entities, CSIRTs network	Repeals NIS Directive; broadens scope; sets stricter cyber risk & reporting duties; supervision & sanctions framework.
55	Directive 2019/ 713 on Combating fraud and counterfeiting of electronic payments	https://eur-lex.europa.eu/eli/dir/2019/713/oj/eng	2019	EU	Regional	European Parliament & Council	IO	Legislation	Directive	Treaties/Convention	Law	Security	Economy	Institutional	non-cash fraud, virtual currencies, payment instruments, penalties	Updates EU rules to combat fraud/counterfeiting of non-cash payments, incl. digital & virtual currency aspects.
56	Directive (EU) 2016/680 (Personal Data)	https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng	2016	EU	Regional (EU)	European Parliament & Council	IO	Legislation	Directive	Treaties/Convention	Law	Human Rights	Security	Legal	personal data, competent authorities, processing, fundamental rights	Harmonises protection of personal data processed by competent authorities for law-enforcement purposes.
57	Directive 2013/40/EU (Attacks against information system)	https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng	2013	EU	Regional (EU)	European Commission	IO	Legislation	Report	Treaties/Convention	Law	Security	Infrastructure and standardization	Legal	attacks on information systems, transposition gaps, penalties	Reviews MS transposition; highlights divergences, penalty levels, operational POCs & statistics.
58	Regulation (EU) 2016/679 (GDPR Package)	https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng	2016	EU	Regional (EU)	European Parliament & Council	IO	Legislation	Regulation	Treaties/Convention	Law	Human Rights	Human Rights	Legal	personal data, fundamental rights, processing, consent, enforcement	Horizontal data-protection regulation harmonising rules across the EU; repeals Directive 95/46/EC.
59	Regulation (EU) 2019/881 – Cybersecurity Act	https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng	2019	EU	Regional (EU)	European Parliament & Council	IO	Legislation	Regulation	Treaties/Convention	Law	Security	Infrastructure and standardization	Legal	ENISA, certification framework	Creates EU cybersecurity certification framework & permanent ENISA mandate.
60	Regulation (EU, Euratom) 2023/2841 – Cybersecurity for EU Institutions	https://eur-lex.europa.eu/eli/reg/2023/2841/oj/eng	2023	EU	Regional (EU)	European Parliament & Council	IO	Legislation	Regulation	Treaties/Convention	Law	Security	Infrastructure and standardization	Legal	CERT-EU, governance board, risk management	Common cyber measures for EU institutions; establishes Inter-institutional Cybersecurity Board.
61	EU-Malaysia Framework Agreement on Partnership and Cooperation (2022)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4646003	2022	EU	Bilateral	EU & Malaysia	IO	Cooperation	Cooperation	Treaties/Convention	Norms	Development	Development	Legal	cyber capacity building, information society	Broad PCA; articles on ICT & cyber cooperation emphasise capacity building.

ASEAN Documents

62	2015 ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies		2015	ASEAN	Regional	ASEAN	State	Cooperation	Work Plan	General Principles	Architecture, Norms	**Development**	Security	Institutional	confidence-building, capacity building, CBMs, incident response	Implements 2012 ARF ministers' statement with practical CBMs and capacity-building activities.	APSC
63	ASEAN ICT Masterplan 2020		2020	ASEAN	Regional	ASEAN	State	Policy	Strategy	General Principles	Architecture, Norms	Economy	Infrastructure and standardization	Institutional	digital economy, infrastructure, information security, strategic thrusts	Five-year masterplan with eight strategic thrusts to propel ASEAN towards a secure, integrated digital economy.	AEC
64	ASEAN Framework on Personal Data Protection		2016	ASE	Regional	ASEAN TELMIN	State	Policy	Cooperation	General Principles	Market, Norms	Human Rights	Economy	Institutional	personal data protection principles, privacy, free flow of information	Sets common principles for personal data protection to support regional trade and information flow.	AEC
65	CIIP Guidelines, 9th ASEAN-Japan Information Security Policy Meeting		2016	ASEAN	Regional	ASEAN -Japan	State	Policy	Cooperation	General Principles	Architecture, Norms	Security	Development	Institutional	CIIP, governance, risk assessment, cyber exercises	Provides checklist and best-practice framework for ASEAN regulators to craft CIIP policies, including information-sharing and cyber-exercise models.	APSC
66	ASEAN Framework on Digital Data Governance		2018	ASEAN	Regional	ASEAN TELMIN	State	Policy	Cooperation	General Principles	Market, Norms	Human Rights	Economy	Algorithmic	digital data governance, cross-border data flows, classification	Non-binding framework guiding member states on data governance to boost digital economy and harmonise regulations.	AEC
67	ASEAN Declaration to Prevent and Combat Cybercrime		2017	ASEAN	Regional	ASEAN Heads of State/Government	State	Cooperation	Cooperation	General Principles	Norms	Security	Development	Institutional	cybercrime, harmonisation, capacity building, cooperation	High-level pledge to harmonise cybercrime laws, strengthen capacity and cooperate regionally.	APSC
68	ARF Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security		2012	ASEAN	Regional	ASEAN Regional Forum	State	Cooperation	Statement	General Principles	Norms	Security	Infrastructure and standardization	Institutional	cooperation pledge, CBMs, stability, risk reduction	Ministerial commitment to intensify regional cooperation and develop a work plan on ICT security.	APSC
69	ASEAN Leaders' Statement on Cybersecurity Cooperation		2018	ASEAN	Regional	ASEAN Leaders' Summit	State	Cooperation	Cooperation	General Principles	Norms	**Development**	Security	Institutional	voluntary norms, capacity building, confidence-building measures	High-level political commitment to implement voluntary cyber norms and strengthen regional cooperation and capacity building.	APSC
70	Japan-ASEAN Cybersecurity Policy Meeting		2024	ASEAN	Regional	ASEAN & Japan (NISC, MIC, METI)	State	Cooperation	Cooperation	General Principles	Norms	**Development**	Security	Institutional	joint capacity building, information sharing, cyber exercise roadmap	Press communiqué confirming enhanced ASEAN-Japan collaboration on cyber exercises, CIIP workshops, awareness drives and capacity building.	APSC
71	ASEAN Ministerial Conference on Cybersecurity, Third Edition	https://asean.org/chairmans-statement-of-the-3rd-asean-ministerial-conference-on-cybersecurity/	2018	ASEAN	Regional	ASEAN Ministerial Conference on Cybersecurity (AMCC)	State	Policy	Cooperation	General Principles	Norms	**Development**	Security	Institutional	cyber norms, UN GGE 11 norms adoption, cybersecurity mechanism, directory of PoCs	Ministers agree in-principle to adopt UN 2015 GGE norms and propose ASEAN cyber mechanism.	APSC
72	ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace		2023	ASEAN	Regional	ASEAN Member States / UNODA-UNIDIR	State	Policy	Cooperation	General Principles	Architecture, Norms	**Development**	Security	Institutional	UN cyber norms, implementation pillars, capacity building	Toolkit offering actionable steps for ASEAN states to operationalise the 11 UN voluntary cyber norms.	APSC
73	ASEAN Security Outlook 2021		2021	ASEAN	Regional	ASEAN Secretariat	State	Policy	Report	General Principles	Norms	Security	Security	Institutional	regional security concerns, COVID-19 impact, cybersecurity threats	Biennial report cataloguing member-state perspectives on traditional and non-traditional security issues, highlighting rising cyber risks.	APSC
74	ASEAN Working Paper on Needs-Based Cyber Capacity-Building Catalog		2024	ASEAN	Regional	ASEAN Member States (Working Paper to UN OEWG)	State	Cooperation	white paper	General Principles	Architecture, Norms	Security	Development	Institutional	capacity-building catalog, partnership principle, OEWG 2024	Proposes a needs-based catalog matching ASEAN states' cyber capacity gaps with international providers under UN OEWG framework.	APSC
75	ASEAN Digital Integration Index (ADII) – First Report		2021	ASEAN	Regional	ASEAN Coordinating Committee on Electronic Commerce (ACCEC)	State	Policy	Report	General Principles	Market, Norms	Infrastructure and standardization	Development	Institutional	digital integration, index pillars, measurement, recommendations	First baseline measurement of ASEAN Digital Integration Index across six pillars.	APSC
76	ASEAN Digital Masterplan 2025 (ADM 2025)		2021	ASEAN	Regional	ASEAN Digital Ministers' Meeting (ADGMIN)	State	Policy	Cooperation	General Principles	Market, Architecture, Norms	Infrastructure and standardization	Development	Algorithmic	broadband, digital services, e-government, inclusion, 8 desired outcomes	Guides ASEAN digital transformation 2021-2025 with eight desired outcomes and enabling actions.	APSC, AEC, ASCC
77	Framework for Negotiating the ASEAN Digital Economy Framework Agreement (DEFA)		2023	ASEAN	Regional	ASEAN Economic Community Council / ACCED	State	Policy	Cooperation	General Principles	Law, Market, Norms	Economy	Economy	Institutional	DEFA, digital trade, cross-border data, digital ID, interoperability	Sets principles, scope and timeline (2025) for negotiating legally binding DEFA.	AEC
79	e-ASEAN Framework Agreement	https://agreement.asean.org/media/download/20140119121135.pdf	2000	ASEAN	Regional	ASEAN Heads of State/Government	State	Legislation	Agreement	Treaties/Convention	Market, Norms	Economy	Infrastructure and standardization	Legal	ICT products & services, e-commerce, liberalisation, digital divide	Treaty establishing objectives and liberalisation measures for ASEAN ICT sector, e-commerce, and digital infrastructure.	AEC
80	ASEAN Agreement on Electronic Commerce	https://agreement.asean.org/media/download/20190306035048.pdf	2019	ASEAN	Regional	ASEAN Economic Ministers / ASEAN Heads of State	State	Legislation	Agreement	Treaties/Convention	Market, Norms	Economy	Economy	Legal	e-commerce liberalisation, cross-border data, digital trade facilitation	First ASEAN legally binding instrument to promote secure e-commerce and reduce barriers to digital trade.	AEC
81	ASEAN Digital Masterplan 2025 (ADM 2025)		2021	ASEAN	Regional	ASEAN Digital Ministers' Meeting (ADGMIN) / ASEAN Secretariat	State	Policy	Work Plan	General Principles	Market, Architecture, Norms	Infrastructure and standardization	Economy	Algorithmic	broadband, digital inclusion, e-gov, trusted services, eight desired outcomes	Guides ASEAN digital transformation 2021-2025 via 8 desired outcomes & enabling actions to build a secure, inclusive digital economy.	AEC, APSC

AMS Documents

82	Computer Misuse Act 1993 (2020 Revised Edition)		2021	Singapore	National	Parliament of Singapore / Law Revision Commission	State	Legislation	Act	National Law	Law	Security	Security	Legal	cybercrime, unauthorized access, digital identity, legal penalties	Defines and penalizes offenses related to unauthorized access, modification, use, and disclosure of computer systems and data; includes clauses on national digital identity and protected systems.	APSC
83	Cybersecurity Code of Practice for Critical Information Infrastructure – Second Edition Revision One		2022	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Structure	Code	General Principles	Architecture	Infrastructure and standardization	Security	Algorithmic	critical infrastructure, CII, cybersecurity controls, CSA, security-by-design	Mandatory code under Cybersecurity Act; sets technical and organizational requirements for operators of Critical Information Infrastructure (CII), including governance, risk management, detection, and recovery.	APSC
84	Be Safe Online Handbook		2023	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Policy	Handbook	General Principles	Norms	Socio-Cultural	Human Rights	Institutional	public awareness, online safety, cyber hygiene, digital resilience	Educational and awareness tool aimed at the general public; promotes digital hygiene practices and responsible online behavior to increase cybersecurity awareness and resilience.	APSC, ASCC
85	Singapore's Operational Technology Cybersecurity Masterplan 2019		2019	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Policy	Strategic Documents	General Principles	Norms	Security	Development	Institutional	OT systems, industrial control systems, CII, cybersecurity training, OT-ISAC, threat sharing, policy framework	Sets national vision and strategy for protecting Operational Technology and Critical Information Infrastructure; outlines four key thrusts: training, information sharing, policy strengthening, and resilience tech development.	APSC
86	Cybersecurity Certification Guide		2021	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Structure	Guide	General Principles	Market	Infrastructure and standardization	Economy	Institutional	certification schemes, CLS, Common Criteria, NITES, IoT security, market assurance	Describes Singapore's cybersecurity certification schemes to assure product security through standardised evaluation; promotes consumer confidence and market-based regulatory mechanisms.	APSC
87	Cybersecurity Act 2018		2018	Singapore	National	Parliament of Singapore	State	Legislation	Act	National Law	Law	Security	Security	Legal	critical information infrastructure, regulation, licensing, incident reporting, risk assessment	Establishes regulatory framework for CII protection, incident reporting, licensing of cybersecurity providers, and powers of the Cybersecurity Commissioner.	APSC
88	Cybersecurity (Critical Information Infrastructure) Regulations 2018		2018	Singapore	National	Prime Minister's Office / CSA	State	Legislation	Regulation	National Law	Law	Security	Infrastructure and standardization	Legal	CII designation, information provision, incident response, appeal process, cybersecurity risk assessment	Implements detailed procedures under the Cybersecurity Act for designating CII, conducting risk assessments, incident reporting, and managing appeals and compliance.	APSC
89	The Singapore Cybersecurity Strategy 2021		2021	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Policy	Strategy	General Principles	Norms	Security	Development	Institutional	resilience, CIIs, international cooperation, certification, talent, cybercrime, standards, AI governance	Outlines national cyber priorities post-2016: building resilient infrastructure, enabling safer cyberspace, enhancing global cooperation, and growing talent. Emphasizes zero-trust architecture, public-private initiatives, international norm advocacy, and market confidence through certification.	APSC
90	Singapore Cyber Landscape 2022		2023	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Structure	Report	General Principles	Architecture	Security	Infrastructure and standardization	Institutional	incident trends, ransomware, phishing, APTs, CIIs, sectoral exposure, cybercrime, public-private trust, threat response	Annual threat landscape report detailing attacks on CIIs, emerging threats, and response strategies. Reinforces institutional mechanisms for threat sharing and sectoral coordination.	APSC, ASCC
91	Safer Cyberspace Masterplan 2020		2020	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Policy	Masterplan	General Principles	Norms	Security	Infrastructure and standardization	Institutional	digital hygiene, ISP-level defense, IoT security labeling, cyber outreach, SMEs, public sector integration	Outlines whole-of-nation plan to raise national cybersecurity baseline. Promotes basic digital hygiene, ISP-level protection, cyber labels for consumer tech, and outreach for businesses and individuals.	APSC, ASCC
92	Cybersecurity (Amendment) Bill 2024		2024	Singapore	National	Parliament of Singapore	State	Legislation	Bill	National Law	Law	Security	Infrastructure and standardization	Legal	third-party infrastructure, foundational digital infrastructure, international designation, audit, cloud computing, critical information infrastructure	Substantial amendment to Cybersecurity Act 2018; expands regulatory reach to include third-party-owned CII, virtual systems, foundational digital infrastructure, and cloud systems; defines new compliance mechanisms and extends powers of the Commissioner.	APSC
93	IoT Security Landscape Report		2022	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Structure	Report	General Principles	Architecture	Security	Infrastructure and standardization	Institutional	IoT security, device vulnerabilities, security baseline, consumer protection, architecture security	Outlines security landscape for IoT devices in Singapore; provides threat overview, sectoral vulnerabilities, and recommendations for design-based safeguards to support architecture-based cybersecurity regulation.	APSC, ASCC
94	National Cybercrime Action Plan (NCAP)	https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf	2015	Singapore	National	Ministry of Home Affairs / Inter-Ministry Committee on Cybercrime	State	Policy	Plan	General Principles	Law	Security	Development	Institutional	cybercrime, law enforcement, public-private cooperation, INTERPOL, Budapest Convention	Strategic framework to combat cybercrime; focuses on international cooperation, domestic capability, legal frameworks, and public awareness; aligns with Budapest Convention principles without being a party.	APSC
95	Operational Technology Cybersecurity Competency Framework		2023	Singapore	National	Cyber Security Agency of Singapore (CSA)	State	Structure	Framework	General Principles	Market	Security	Development	Institutional	workforce development, cybersecurity competencies, OT systems, national skills framework	Defines role-based competency standards for OT cybersecurity professionals; supports workforce upskilling and alignment with national digital infrastructure needs.	APSC
96	Electronic Commerce Act 2006 (Act 658)		2006	Malaysia	National	Parliament of Malaysia	State	Legislation	Act	National Law	Law	Security	Economy	Legal	electronic message, contract formation, electronic signature, commercial transactions	Provides legal recognition for electronic messages in commercial transactions; defines contract formation, signature, retention, and delivery via digital means. Supports digital trade facilitation.	AEC
97	Digital Signature Act 1997 (Act 562)		1997	Malaysia	National	Parliament of Malaysia	State	Legislation	Act	National Law	Law	Security	Security	Legal	digital signature, certification authority, secure communication, electronic authentication	Regulates the use of digital signatures and licensing of certification authorities; includes duties, rights, legal presumptions, and criminal offenses tied to digital identity verification in Malaysia.	AEC
98	Computer Crimes Act 1997 (Act 563)		1997	Malaysia	National	Parliament of Malaysia	State	Legislation	Act	National Law	Law	Security	Infrastructure and standardization	Legal	unauthorized access, modification, computer data, cybersecurity offences	Establishes criminal offences for unauthorized access, modification, and communication involving computer systems; defines legal scope for computer-related crimes and procedural powers for enforcement.	APSC
99	National Security Council Act 2016 (Act 776)		2016	Malaysia	National	Parliament of Malaysia	State	Structure	Act	National Law	Law	Security	Security	Legal	national security, NSC powers, security area, emergency powers, coordination	Establishes Malaysia's National Security Council and grants broad powers to designate security areas, coordinate operations, and issue directives during national threats; includes legal immunities and centralized crisis management.	APSC
100	National Security Policy (NSP)		2021	Malaysia	National	National Security Council (NSC)	State	Policy	Policy	General Principles	Norms	Security	Infrastructure and standardization	Institutional	sovereignty, cyber threats, people's security, territorial integrity, critical infrastructure	Defines national core values and security strategies. Highlights cyber threats as key non-physical risk to critical information infrastructure and public mindsets. Builds on NSC Act 2016 to integrate cyber with broader national security frameworks.	APSC
101	Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS)		2002	Malaysia	National	MAMPU (Jabatan Perdana Menteri)	State	Structure	Guideline	General Principles	Architecture	Security	Infrastructure and standardization	Institutional	ICT security, public sector, compliance, MAMPU, incident response, risk management	Establishes ICT security responsibilities for Malaysian government agencies, including risk assessment, compliance monitoring, and reporting mechanisms. Core document under the national ICT security framework (MyMIS).	APSC
102	Communications and Multimedia Act 1998 (Act 588)		1998	Malaysia	National	Parliament of Malaysia	State	Legislation	Act	National Law	Law	Infrastructure and standardization	Security	Legal	licensing, digital infrastructure, security obligations, interception powers, regulatory framework	Regulates communications and multimedia industries in Malaysia; includes licensing, regulatory powers, infrastructure obligations, and provisions for lawful network interception and emergency powers.	APSC
103	Industry4WRD: National Policy on Industry 4.0		2018	Malaysia	National	Ministry of International Trade and Industry (MITI)	State	Policy	National Policy	General Principles	Market	Economy	Security	Institutional	Industry 4.0, smart manufacturing, SMEs, automation, digitalization, productivity, AI, IoT, cybersecurity	Outlines Malaysia's national policy to transition manufacturing sector toward Industry 4.0 technologies. Emphasizes ecosystem-building, SME digital adoption, productivity growth, and cybersecurity infrastructure.	AEC
104	Joint Statement: Trilateral Meeting on Security Among the Philippines, Indonesia, and Malaysia		2017	Malaysia	Trilateral	Foreign Ministries and National Security Councils	State	Cooperation	Joint Statement	General Principles	Norms	Security	Security	Institutional	terrorism, counter-extremism, intelligence sharing, regional security, cyber threats	Establishes trilateral cooperation on counter-terrorism and cybersecurity, including cyber threat containment, ICT abuse prevention, intelligence sharing, and counter-narratives across Southeast Asia.	APSC
105	Malaysia Smart City Framework (Executive Summary)		2018	Malaysia	National	PLANMalaysia (Federal Department of Town and Country Planning)	State	Policy	Framework	General Principles	Architecture	Security	Socio-Cultural	Institutional	smart cities, digital infrastructure, IoT, urban planning, cybersecurity	Outlines strategic vision and governance framework for smart cities in Malaysia; emphasizes digital infrastructure, data-driven planning, and embedded cybersecurity across city systems.	AEC
106	Kertas Putih Penyampaian Perkhidmatan Awam (KPP2)		2023	Malaysia	National	Jabatan Perkhidmatan Awam (JPA)	State	Policy	White Paper	General Principles	Norms	Security	Socio-Cultural	Institutional	digital government, public service reform, cybersecurity standards, digital trust	Government white paper proposing transformation of Malaysia's public service delivery, including adoption of cybersecurity standards and digital trust principles as core architecture of future administration.	ASCC
107	Malaysia Cyber Security Strategy 2020–2024		2020	Malaysia	National	National Cyber Security Agency (NACSA)	State	Policy	Strategy	General Principles	Architecture	Security	Security	Institutional	cybersecurity strategy, national resilience, cybercrime, critical infrastructure, digital trust, incident response	Outlines Malaysia's national strategy for cyber resilience, including legal reforms, public-private cooperation, cyber hygiene awareness, and CII protection from 2020–2024.	APSC
108	National Defence Policy		2010	Malaysia	National	Ministry of Defence (MINDEF)	State	Policy	Policy	General Principles	Norms	Security	Security	Institutional	sovereignty, cyber-warfare, regional cooperation, UN peacekeeping, Total Defence (HANRUH), ICT infrastructure	Sets out Malaysia's defence posture including cyber capabilities, ICT infrastructure, multilateral diplomacy, and modernisation of the Malaysian Armed Forces.	APSC
109	Pelan Strategik MINDEF 2021–2025		2021	Malaysia	National	Ministry of Defence (MINDEF)	State	Structure	Strategic Plan	General Principles	Law	Security	Security	Institutional	civil-military cooperation, defence technology, veteran welfare, Total Defence, capability development	Strategic blueprint aligned with Defence White Paper to enhance national defence readiness and civil-military synergy, with emphasis on cyber threats and digital preparedness.	APSC
110	Penal Code (Act 574)		1997	Malaysia	National	Parliament of Malaysia	State	Legislation	Act	National Law	Law	Security	Security	Legal	cybercrime, unauthorized access, data breaches, digital evidence, criminal law	General criminal code which includes legal provisions on unauthorized computer access, cyber fraud, and digital criminal liability.	APSC
111	Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)		2016	Malaysia	National	Chief Government Security Office (CGSO)	State	Structure	Framework	General Principles	Architecture	Security	Socio-Cultural	Institutional	public sector cybersecurity, governance, resilience, cyber risk, framework, audit, enforcement	National framework for cybersecurity risk governance in Malaysia's public sector, including identification, response, audit, recovery, and legal compliance procedures.	APSC
112	Indonesia Defence White Paper 2015		2015	Indonesia	National	Ministry of Defence (Kemhan)	State	Policy	White Paper	General Principles	Norms	Security	Security	Institutional	total defence, national resilience, sovereignty, cyber threats, ICT infrastructure	Establishes Indonesia's defence doctrine and strategic outlook; includes cyber threats as part of total defence strategy; outlines defence industrial base and ICT-based sovereignty concerns.	APSC
113	Cybersecurity and Resilience Bill (Draft) 2019		2019	Indonesia	National	House of Representatives (DPR) / BSSN (proposed)	State	Legislation	Draft Bill	National Law	Law	Security	Infrastructure and standardization	Legal	cyber threats, BSSN authority, data protection, critical infrastructure, cybersecurity governance	Draft legislation to establish national cybersecurity governance, define cyber threats, and empower BSSN. Includes provisions for cyber resilience, regulatory oversight, and protection of digital sovereignty.	APSC
114	Electronic Information and Transactions Law (UU ITE)		2008	Indonesia	National	Parliament of Indonesia	State	Legislation	Act	National Law	Law	Economy	Security	Legal	electronic transactions, digital contract, content regulation, cross-border data, jurisdiction	Establishes legal basis for digital and electronic transactions, content liabilities, and jurisdictional application across borders; foundational cyber law in Indonesia with several amendments.	AEC X APSC
116	Law No. 27/2022 on Personal Data Protection		2022	Indonesia	National	Parliament of Indonesia	State	Legislation	Act	National Law	Law	Security	Economy	Legal	data protection, personal data, privacy rights, digital economy, enforcement	First comprehensive data protection law in Indonesia; establishes legal obligations for data controllers and processors; framed as part of digital rights and economic transformation.	AEC X APSC
117	BSSN Regulation No. 3/2021 on Cybersecurity and Media Literacy		2021	Indonesia	National	Badan Siber dan Sandi Negara (BSSN)	State	Structure	Regulation	National Law	Norms	Security	Socio-Cultural	Legal	cyber literacy, public awareness, cyber hygiene, BSSN, media education	Regulation mandates national literacy programs on cybersecurity and media usage; includes public awareness training on hoaxes, cyberbullying, data protection, and incident response. Led by BSSN with stakeholder collaboration.	APSC
118	MoD Regulation No. 82/2014 on Cyber Defence		2014	Indonesia	National	Ministry of Defence (Kementerian Pertahanan)	State	Structure	Ministerial Regulation	National Law	Architecture	Security	Security	Legal	cyber defence, strategic assets, CII, coordination, sovereignty	Defines roles and responsibilities for cyber defence within the military and defence sector; includes threat response coordination, asset protection, and technical architecture planning.	APSC
119	Presidential Regulation No. 47/2023 on National Cybersecurity Strategy and Cyber Crisis Management		2023	Indonesia	National	Office of the President / BSSN	State	Policy	Presidential Regulation	National Law	Architecture	Security	Infrastructure and standardization	Legal	cybersecurity strategy, crisis management, national interest, CII protection, BSSN coordination	Establishes Indonesia's national cybersecurity strategy, mandates incident response protocols, and details the management of cyber crises including risk mitigation, CII defence, and inter-agency coordination.	APSC
120	Government Regulation No. 71/2019 on Electronic Systems and Transactions		2019	Indonesia	National	Government of Indonesia	State	Legislation	Government Regulation	National Law	Law	Economy	Security	Legal	data management, PSE, cross-border flow, accountability, compliance	Regulates electronic systems and digital transactions, including private and public PSE compliance, cross-border data handling, and minimum cybersecurity standards for system operators.	AEC
121	Convention on Cybercrime (Budapest Convention)		2001	Philippines	International	Council of Europe	State	Legislation	Convention	National Law	Law	Security	Security	Legal	cybercrime, criminalisation, jurisdiction, procedural law, cooperation	International treaty setting global standards for combating cybercrime through harmonized criminal laws, investigative powers, and international cooperation. Serves as a legal foundation for many national cybercrime laws.	APSC
122	AFP Cyberspace Strategic Plan (in progress)		2017	Philippines	National	Armed Forces of the Philippines (AFP)	State	Structure	Strategic Documents	General Principles	Architecture	Security	Security	Institutional	cyber defence, strategic plan, cyber force, military networks, digital resilience	Outlines AFP efforts to establish a cyberspace-capable force through strategic planning, institutional partnerships, and integration of cyber defence into military operations. Still under development as of 2017.	APSC
123	National Security Strategy (NSS) 2018		2018	Philippines	National	Office of the President / National Security Council	State	Policy	Strategy	General Principles	Norms	Security	Infrastructure and standardization	Institutional	national security, cyber threats, digital infrastructure, governance, ICT security	Comprehensive national security vision incorporating cyber threats, infrastructure protection, and information dominance. Supports civilian-military collaboration in digital security.	APSC
124	Department of Information and Communications Technology Act of 2015 (RA 10844)		2015	Philippines	National	Congress of the Philippines	State	Structure	Act	National Law	Law	Security	Infrastructure and standardization	Legal	DICT, ICT development, cybersecurity mandate, digital infrastructure, government tech	Establishes DICT as the primary national body for ICT governance. Includes oversight for cybersecurity, national digital infrastructure, digital literacy, and strategic planning responsibilities.	APSC
125	National Cybersecurity Plan 2022		2017	Philippines	National	Department of Information and Communications Technology (DICT)	State	Policy	Strategy	General Principles	Architecture	Infrastructure and standardization	Security	Institutional	critical infrastructure, threat response, incident management, awareness, digital protection	Outlines strategic framework for protecting critical ICT infrastructure, enabling cyber resilience, and strengthening governance coordination. Highlights institutional roles and public-private cooperation.	APSC
126	National Security Policy 2017–2022		2017	Philippines	National	National Security Council	State	Policy	Policy	General Principles	Norms	Infrastructure and standardization	Security	Institutional	cybersecurity, hybrid threats, national sovereignty, whole-of-nation, strategic threats	Presents a strategic vision integrating cyber and digital security into national sovereignty priorities. Emphasizes hybrid warfare and multi-sectoral preparedness.	APSC
127	Cybercrime Prevention Act of 2012 (RA 10175)		2012	Philippines	National	Congress of the Philippines	State	Legislation	Act	National Law	Law	Security	Security	Legal	cybercrime, hacking, CICC, digital evidence, jurisdiction, cyber libel, real-time traffic	Defines cybercrime offenses, establishes penalties and procedures for investigation and enforcement, and creates Cybercrime Investigation and Coordinating Center (CICC) under the Office of the President.	APSC
128	Rules on Electronic Evidence (A.M. No. 01-7-01-SC)		2001	Philippines	National	Supreme Court of the Philippines	State	Legislation	Rules of Court	Judicial Decisions/Writing	Law	Security	Legal	Legal	electronic document, digital signature, authentication, evidentiary rules, electronic testimony	Establishes legal standards for electronic documents in judicial proceedings. Covers digital signatures, admissibility, evidentiary weight, and authentication procedures.	APSC
129	Act on Computer Crime B.E. 2550 (2007)		2007	Thailand	National	Royal Thai Government	State	Legislation	Act	National Law	Law	Security	Security	Legal	computer crime, hacking, digital evidence, content-related offenses	Thailand's foundational cybercrime legislation. Covers offenses related to unauthorized access, data modification, spamming, malware, and content crimes such as defamation and national security threats.	APSC
130	Cybersecurity Act B.E. 2562 (2019)		2019	Thailand	National	Ministry of Digital Economy and Society	State	Legislation	Act	National Law	Law	Security	Security	Legal	national cybersecurity committee, CII, response coordination, risk assessment	Establishes frameworks for protecting critical infrastructure, with oversight by the National Cybersecurity Committee. Focus on preventive measures, incident reporting, and cyber resilience.	APSC
131	Cyber Security Policy and Action Plan 2022–2027		2022	Thailand	National	National Cyber Security Agency (NCSA)	State	Policy	Strategy	General Principles	Architecture	Security	Economy	Institutional	strategic objectives, cyber threat response, public-private partnership, digital economy	Provides a roadmap for strengthening national cybersecurity capacities. Includes training, monitoring, public-private coordination, and technical capability development through a five-year plan.	APSC
132	Personal Data Protection Act B.E. 2562 (2019)		2019	Thailand	National	Royal Thai Government / Ministry of Digital Economy and Society	State	Legislation	Act	General Principles	Law	Security	Legal	Legal	data controller, data processor, consent, data transfer, enforcement, penalties	Comprehensive data protection law modeled on GDPR. Defines personal data rights, cross-border flow regulation, duties of data controllers/processors, and enforcement structures under a dedicated authority.	ASCC
134	2001 Decree No. 55/2001/ND-CP on Internet Services		2001	Vietnam	National	Government of Vietnam	State	Legislation	Decree	National Law	Law	Infrastructure and standardization	Security	Legal	internet services, regulation, use policy	Defines the management, provision, and use of internet services; includes obligations of providers and users.	APSC
135	2016 Law on Network Information Security		2016	Vietnam	National	National Assembly	State	Legislation	Law	National Law	Law	Security	Infrastructure and standardization	Legal	information security, network systems, protection obligations	Comprehensive law defining information security requirements, responsibilities, and state management functions.	APSC
136	2016 Cyber Information Security		2016	Vietnam	National	Government of Vietnam	State	Policy	Policy Document	General Principles	Norms	Security	Infrastructure and standardization	Institutional	cybersecurity framework, policy orientation, institutional responsibilities	Outlines general government policy directions and principles for managing cyber information security.	APSC
137	2017 Workshop on Cybersecurity Policy for CLMV		2017	Vietnam	Multilateral	Vietnam Ministry of Foreign Affairs & ASEAN Partners	State	Cooperation	Workshop Summary	General Principles	Norms	Development	Security	Institutional	capacity building, regional diplomacy, ASEAN	Focuses on international cooperation, capacity development, and policy sharing among CLMV countries.	APSC
138	2018 Law on Cybersecurity		2018	Vietnam	National	National Assembly	State	Legislation	Law	National Law	Law	Security	Security	Legal	national cybersecurity, enforcement, infrastructure, social order	Legal framework for protecting national security and social order in cyberspace, including obligations for businesses and individuals.	APSC
139	2016 Decision 898/QD-TTg on Cyber Information Security		2016	Vietnam	National	Prime Minister	State	Policy	Decision	Judicial Decisions/Writing	Norms	Security	Development	Institutional	information security, national resilience, strategy 2016–2020	Sets orientations, goals, and duties for ensuring cyber information security, emphasizing capacity building and public-private cooperation.	APSC
140	Cambodian ICT Masterplan 2020		2014	Cambodia	National	Ministry of Posts and Telecommunications	State	Policy	Strategy	General Principles	Architecture	Infrastructure and standardization	Development	Institutional	digital infrastructure, public-private partnerships, e-government, cybersecurity vision	Outlines Cambodia's vision for ICT development, including infrastructure growth, government digitization, and cybersecurity priorities up to 2020.	APSC
141	Criminal Code of Cambodia (Unofficial English Translation)		2009	Cambodia	National	Royal Government of Cambodia	State	Legislation	Code	National Law	Law	Security	Security	Legal	criminal offenses, fraud, illegal access, defamation, content restrictions	Provides general criminal law applicable to ICT-related offenses such as fraud, data interference, and illegal content.	APSC
142	Law on Telecommunications		2015	Cambodia	National	Ministry of Posts and Telecommunications	State	Legislation	Law	National Law	Law	Infrastructure and standardization	Security	Legal	telecom regulation, infrastructure, interception, national security	Covers telecom operator obligations, licensing, user rights, and includes provisions allowing surveillance in the name of national security.	APSC
143	Computer Misuse Act (Chapter 194)		2007	Brunei Darussalam	National	Government of Brunei	State	Legislation	Act	National Law	Law	Security	Security	Legal	unauthorized access, hacking, cybercrime	Defines and penalizes computer-related offenses such as hacking, unauthorized access, and misuse of computer systems.	APSC
144	Electronic Transactions Act (Chapter 196)		2008	Brunei Darussalam	National	Government of Brunei	State	Legislation	Act	National Law	Law	Economy	Economy	Legal	e-commerce, digital signature, online contracts	Facilitates electronic transactions and recognition of digital signatures; supports the legal validity of online commercial activities.	AEC
145	National Broadband Policy 2014–2017		2014	Brunei Darussalam	National	Ministry of Communications	State	Policy	Policy Document	General Principles	Architecture	Infrastructure and standardization	Infrastructure and standardization	Institutional	broadband infrastructure, ICT access, economic growth	Lays out infrastructure and policy targets for increasing broadband access and connectivity across Brunei.	AEC
146	Digital Government Strategy 2015–2020		2015	Brunei Darussalam	National	Prime Minister's Office	State	Policy	Strategy	General Principles	Architecture	Security	Development	Institutional	e-government, digital services, cybersecurity framework	Outlines the strategic vision and programs for transforming Brunei into a digital government aligned with Wawasan 2035.	APSC
147	Brunei Defence White Paper 2011		2011	Brunei Darussalam	National	Ministry of Defence	State	Policy	White Paper	General Principles	Norms	Security	Security	Institutional	cyber warfare, military strategy, national security	Identifies cyber threats as part of Brunei's broader security strategy, emphasizing regional cooperation and preparedness.	APSC
148	Commonwealth Model Law on Computer and Computer-Related Crimes		2017	Brunei Darussalam	International	Commonwealth Secretariat	IO	Legislation	Model Law	General Principles	Law	Security	Security	Legal	model legislation, cybercrime, procedural powers, digital evidence	A model legal framework intended to guide Commonwealth countries, including Brunei, in drafting cybercrime laws.	APSC
149	Electronic Transactions Law		2004	Myanmar	National	State Peace and Development Council	State	Legislation	Law	National Law	Law	Security	Security	Legal	electronic record, data message, signature, certification authority, cybersecurity offences	Provides legal basis for electronic transactions, data authenticity, and digital signature validation. Establishes regulatory bodies for implementation and enforcement.	APSC
150	Telecommunications Law		2013	Myanmar	National	Pyidaungsu Hluttaw	State	Legislation	Law	National Law	Law	Infrastructure and standardization	Security	Legal	telecommunications, licensing, technical standards, consumer protection, offences	Governs telecom service providers and equipment, network standards, and licensing. Includes consumer protection and cybersecurity-related offences.	APSC
151	Computer Science Development Law		1996	Myanmar	National	State Law and Order Restoration Council	State	Legislation	Law	General Principles	Law	Security	Infrastructure and standardization	Legal	computer licensing, information control, state security, software regulation	Sets institutional structures for computer regulation, licensing, software export/import. Emphasizes state control and national security in ICT.	APSC
152	e-Governance Master Plan 2016–2020		2016	Myanmar	National	Ministry of Communications and Information Technology	State	Policy	Strategic Documents	General Principles	Architecture	Infrastructure and standardization	Socio-Cultural	Institutional	e-government, ICT infrastructure, digital transformation, interoperability	Outlines national e-governance strategy to modernize public service delivery. Focus on interoperability, citizen platforms, and ICT infrastructure.	AEC

CLASSIFICATION CODEBOOK

1. Document Title
   Official or commonly used title of the document. Use the full name as listed on the issuing institution's website or official publication.

2. Source / Link
   URL or citation where the document is publicly accessible. Use direct PDF links or official repositories.

3. Year
   Year the document was published or adopted. Format: YYYY (e.g., 2020).

4. Country / Region
   Jurisdiction or regional body responsible for issuing the document. E.g., UN, EU, ASEAN, or individual ASEAN states.

5. Level
   Governance level of the document: International, Regional, National, or Bilateral/Multilateral.

6. Institution
   Primary issuing body or author of the document. E.g., UNGA, ITU, European Commission, ASEAN Secretariat, etc.

7. Legal Subject
   Type of legal actor represented. Values: States, International Organizations (IOs), or NGOs.

8. Governance Type (UNIDIR)
   Function performed by the document:
   - Policy: Strategies, visions
   - Structure: Institutional setups
   - Legislation: Binding rules
   - Cooperation: Agreements, partnerships
   -

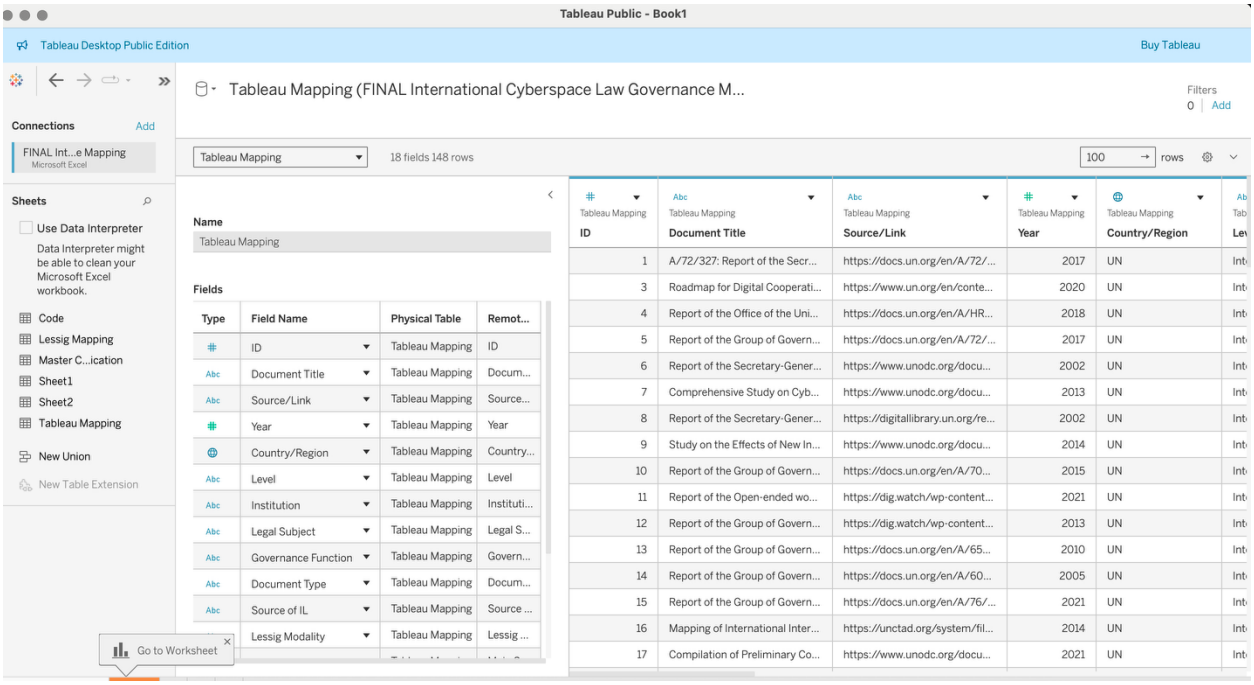
9. Document Type
   Formal classification of the document. E.g., Strategy, White Paper, Law, Regulation, Convention, MoU, Agreement, etc.

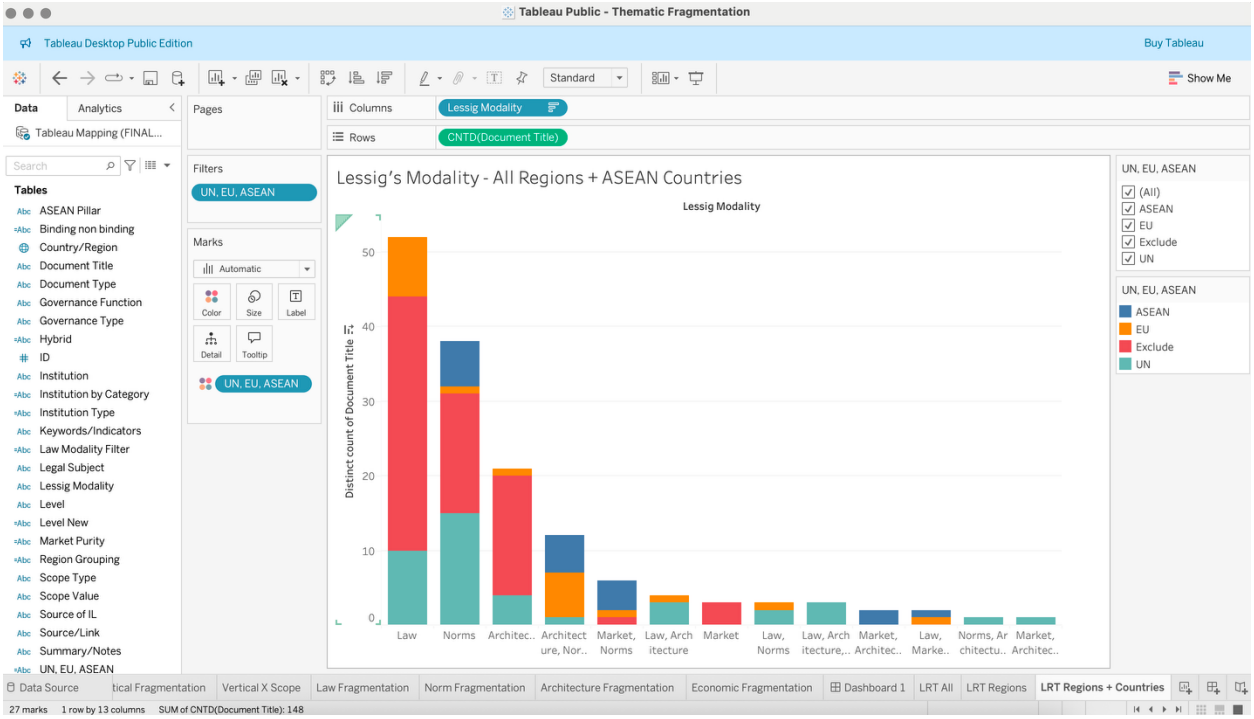
10. Source of International Law
    Relation to ICJ Art. 38(1):
    - Treaties
    - Customs
    - General Principles
    - Judicial Decisions / Writings

11. Lessig's Modality
    Regulatory approach of the document
    - Law: Binding mechanisms
    - Norms: Informal standards
    - Market: Economic forces
    - Architecture: Technical design
    - Multiple may apply
    -
12. Keywords / Indicators
    Topical focus or themes in the document. E.g., Cybersecurity, Privacy, Encryption, Norms, etc

13. Summary / Notes
    Brief summary of the document's content, scope, or significance for quick reference.

ANNEX C
TABLEAU MAPPING





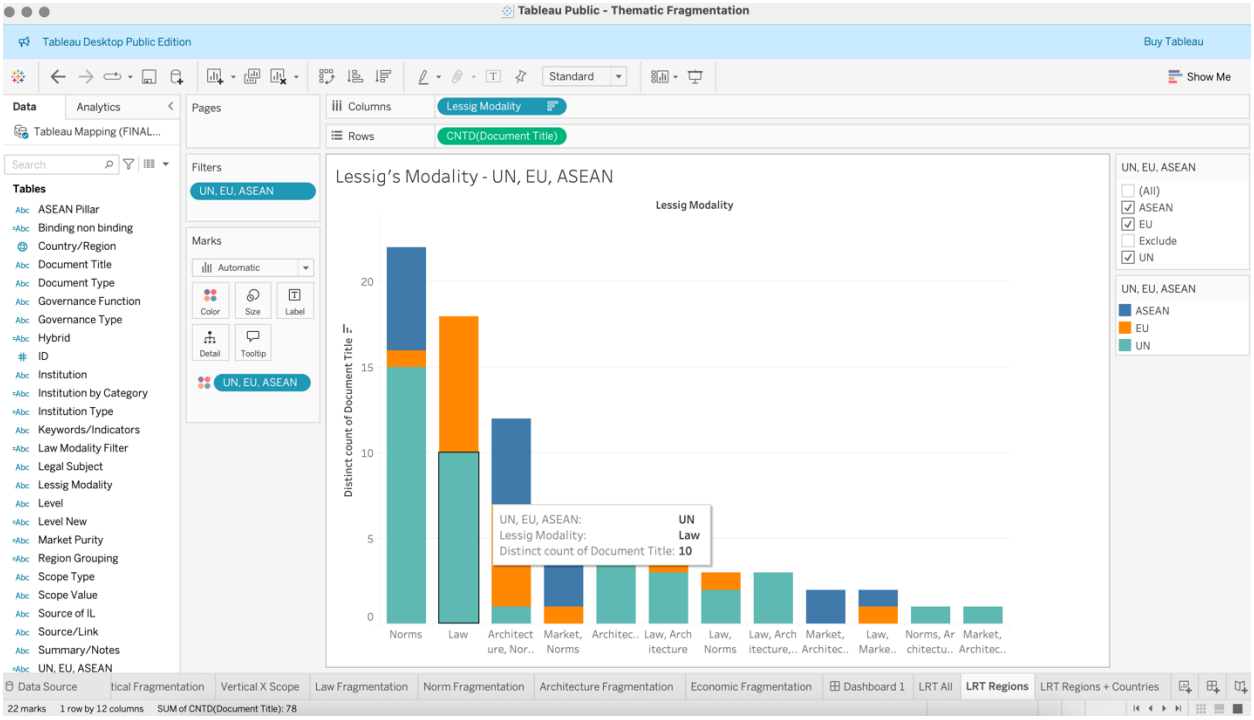


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Pages
Columns
Lessig Modality
Rows
CNTD(Document Title)
Filters
UN, EU, ASEAN
Marks
Automatic
Color
Size
Label
Detail
Tooltip
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Lessig's Modality - UN, EU, ASEAN
Lessig Modality
Distinct count of Document Title
UN, EU, ASEAN:
Lessig Modality:
Distinct count of Document Title:
UN
Law
10
Norms
Law
Architect ure, Nor..
Market, Norms
Architec..
Law, Arch itecture
Law, Norms
Law, Arch itecture,..
Market, Architec..
Law, Marke..
Norms, Ar chitectu..
Market, Architec..
(All)
ASEAN
EU
Exclude
UN
Data Source
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmentation
Economic Fragmentation
Dashboard 1
LRT All
LRT Regions
LRT Regions + Countries
22 marks
1 row by 12 columns
SUM of CNTD(Document Title): 78

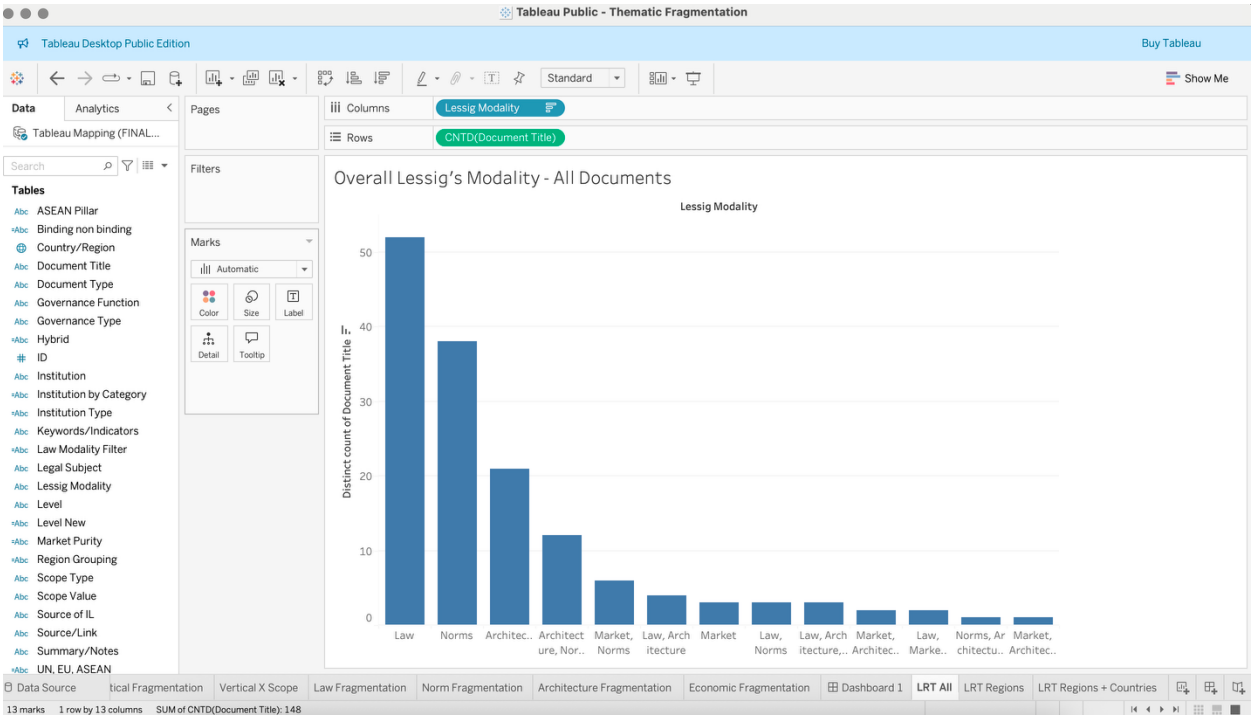


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Pages
Columns
Lessig Modality
Rows
CNTD(Document Title)
Filters
Marks
Automatic
Color
Size
Label
Detail
Tooltip
Tables
Overall Lessig's Modality - All Documents
Lessig Modality
Distinct count of Document Title
Law
Norms
Architec..
Architect ure, Nor..
Market, Norms
Law, Arch itecture
Market
Law, Norms
Law, Arch itecture,..
Market, Architec..
Law, Marke..
Norms, Ar chitectu..
Market, Architec..
Data Source
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmentation
Economic Fragmentation
Dashboard 1
LRT All
LRT Regions
LRT Regions + Countries
13 marks
1 row by 13 columns
SUM of CNTD(Document Title): 148

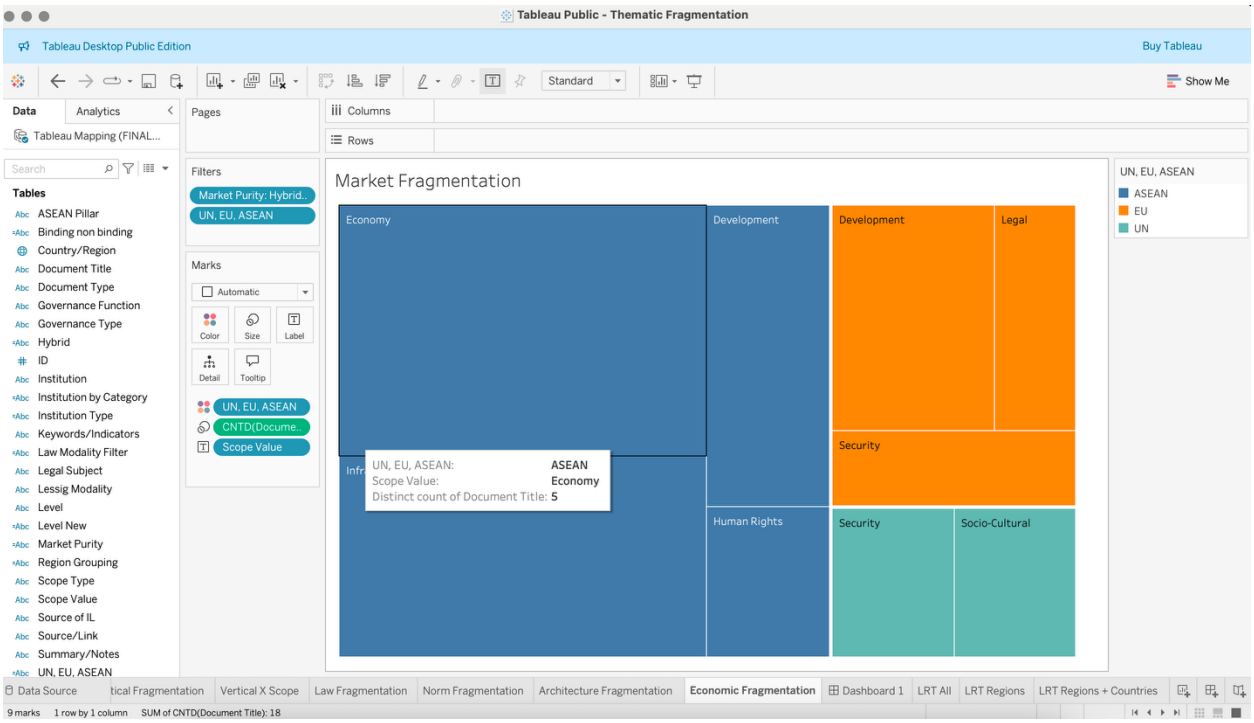


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Pages
Columns
Rows
Filters
Market Purity: Hybrid..
UN, EU, ASEAN
Marks
Automatic
Color
Size
Label
Detail
Tooltip
UN, EU, ASEAN
CNTD(Docume..
Scope Value
Market Fragmentation
Economy
Development
Development
Legal
Security
Human Rights
Security
Socio-Cultural
UN, EU, ASEAN:
ASEAN
Scope Value:
Economy
Distinct count of Document Title: 5
UN, EU, ASEAN
ASEAN
EU
UN
Data Source
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmentation
Economic Fragmentation
Dashboard 1
LRT All
LRT Regions
LRT Regions + Countries
9 marks
1 row by 1 column
SUM of CNTD(Document Title): 18

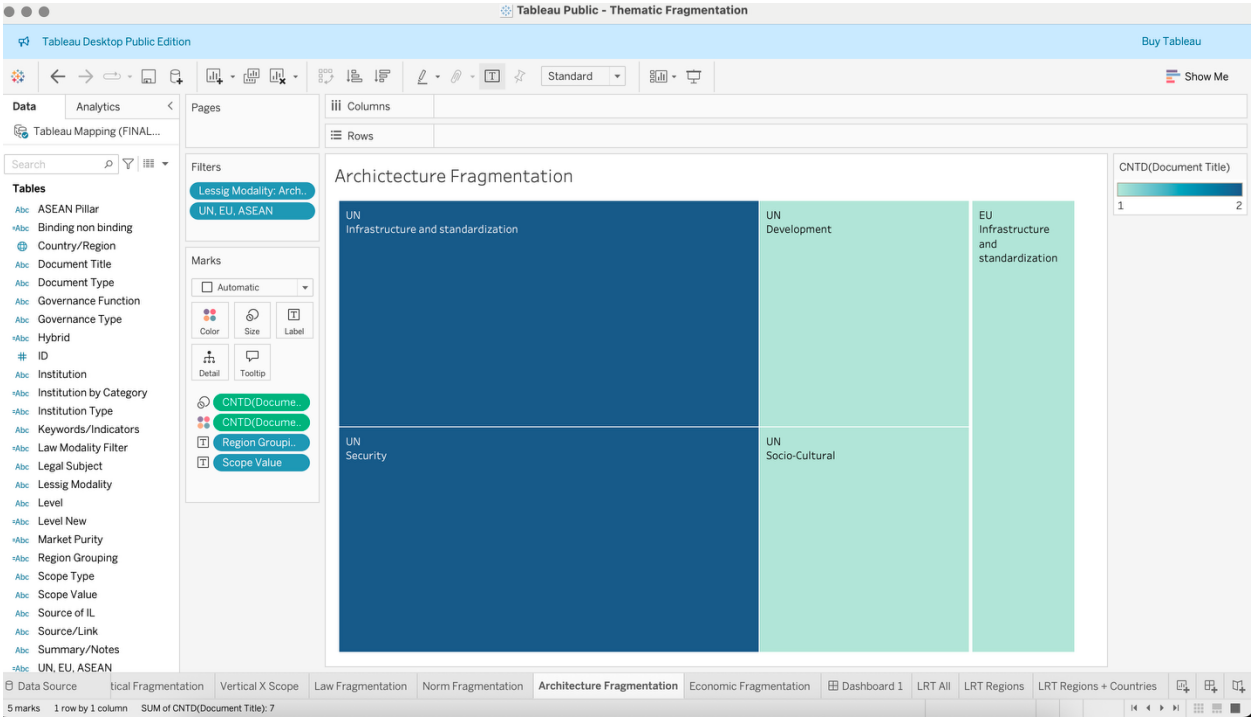


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Pages
Columns
Rows
Filters
Lessig Modality: Arch..
UN, EU, ASEAN
Marks
Automatic
Color
Size
Label
Detail
Tooltip
CNTD(Docume..
CNTD(Docume..
Region Groupi..
Scope Value
Architecture Fragmentation
UN
Infrastructure and standardization
UN
Development
EU
Infrastructure and standardization
UN
Security
UN
Socio-Cultural
CNTD(Document Title)
1
2
Data Source
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmentation
Economic Fragmentation
Dashboard 1
LRT All
LRT Regions
LRT Regions + Countries
5 marks
1 row by 1 column
SUM of CNTD(Document Title): 7

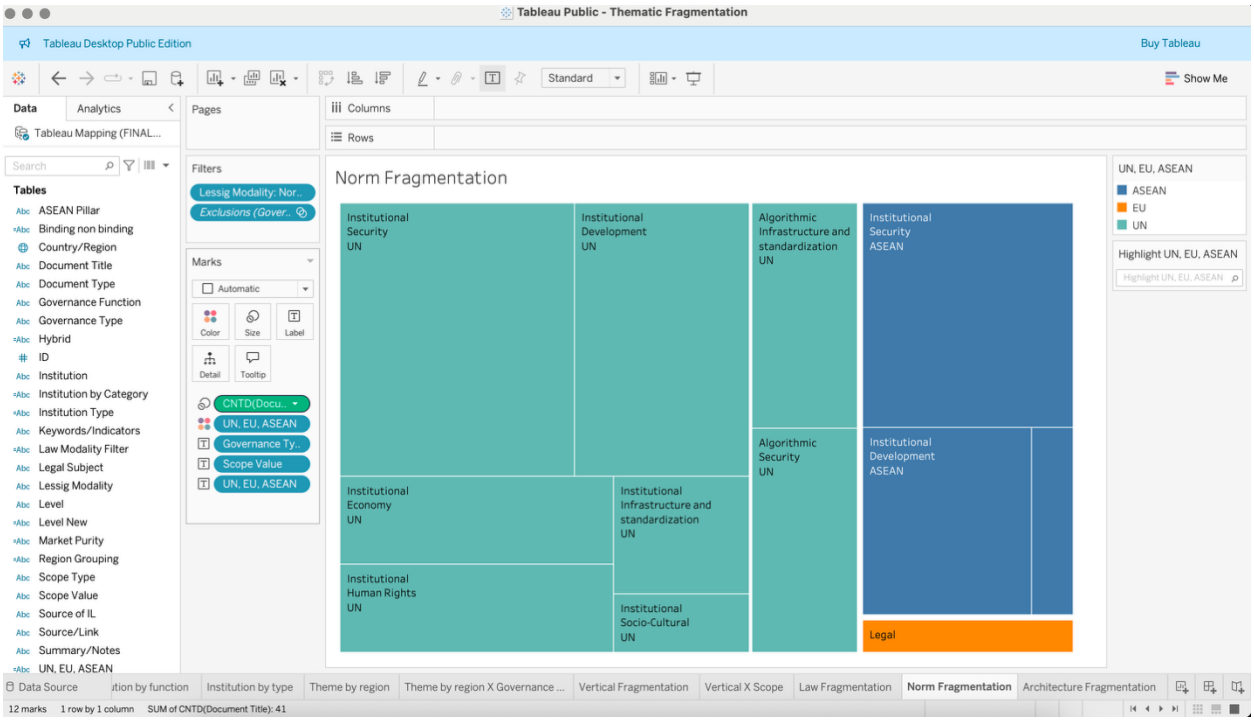


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Pages
Columns
Rows
Filters
Lessig Modality: Nor..
Exclusions (Gover..
Marks
Automatic
Color
Size
Label
Detail
Tooltip
CNTD(Docu..
UN, EU, ASEAN
Governance Ty..
Scope Value
UN, EU, ASEAN
Norm Fragmentation
Institutional Security UN
Institutional Development UN
Algorithmic Infrastructure and standardization UN
Institutional Security ASEAN
Algorithmic Security UN
Institutional Development ASEAN
Institutional Economy UN
Institutional Infrastructure and standardization UN
Institutional Human Rights UN
Institutional Socio-Cultural UN
Legal
UN, EU, ASEAN
ASEAN
EU
UN
Highlight UN, EU, ASEAN
Data Source
Institution by function
Institution by type
Theme by region
Theme by region X Governance ...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmentation
12 marks
1 row by 1 column
SUM of CNTD(Document Title): 41

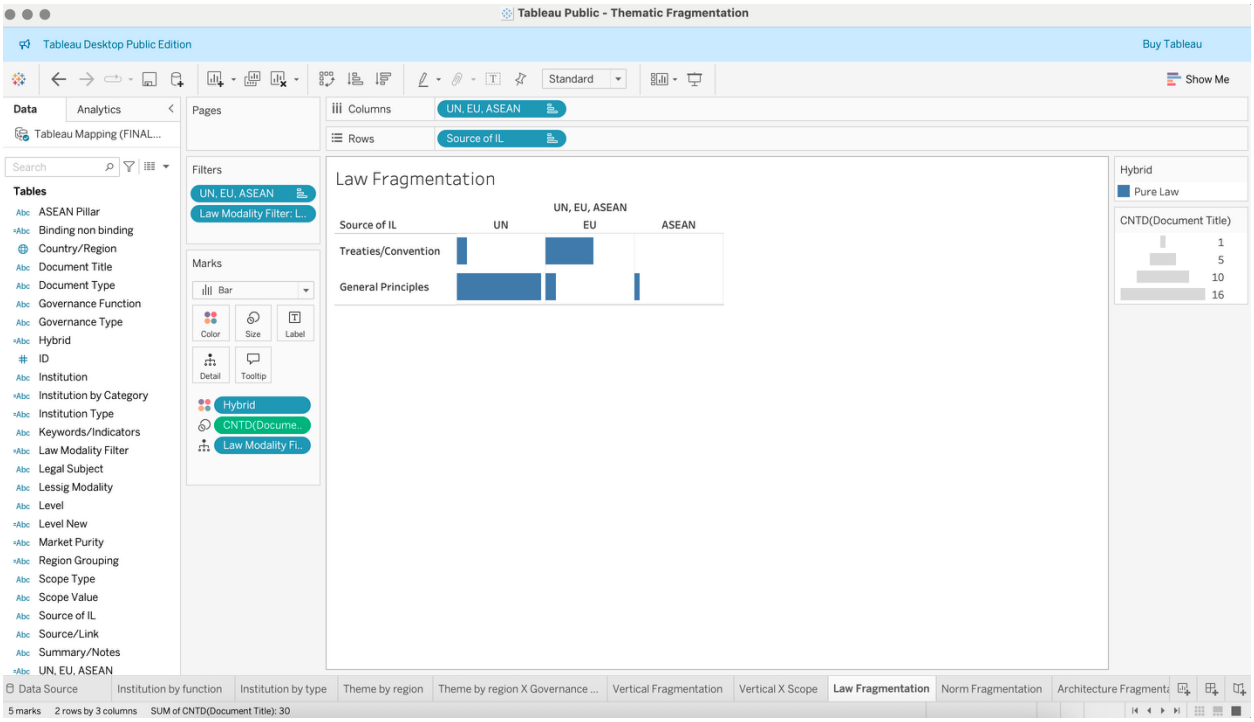


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Pages
Columns
UN, EU, ASEAN
Rows
Source of IL
Filters
UN, EU, ASEAN
Law Modality Filter: L...
Marks
Bar
Color
Size
Label
Detail
Tooltip
Hybrid
CNTD(Docume..
Law Modality Fi..
Law Fragmentation
UN, EU, ASEAN
Source of IL
UN
EU
ASEAN
Treaties/Convention
General Principles
Hybrid
Pure Law
CNTD(Document Title)
1
5
10
16
Data Source
Institution by function
Institution by type
Theme by region
Theme by region X Governance ...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmenta
5 marks
2 rows by 3 columns
SUM of CNTD(Document Title): 30

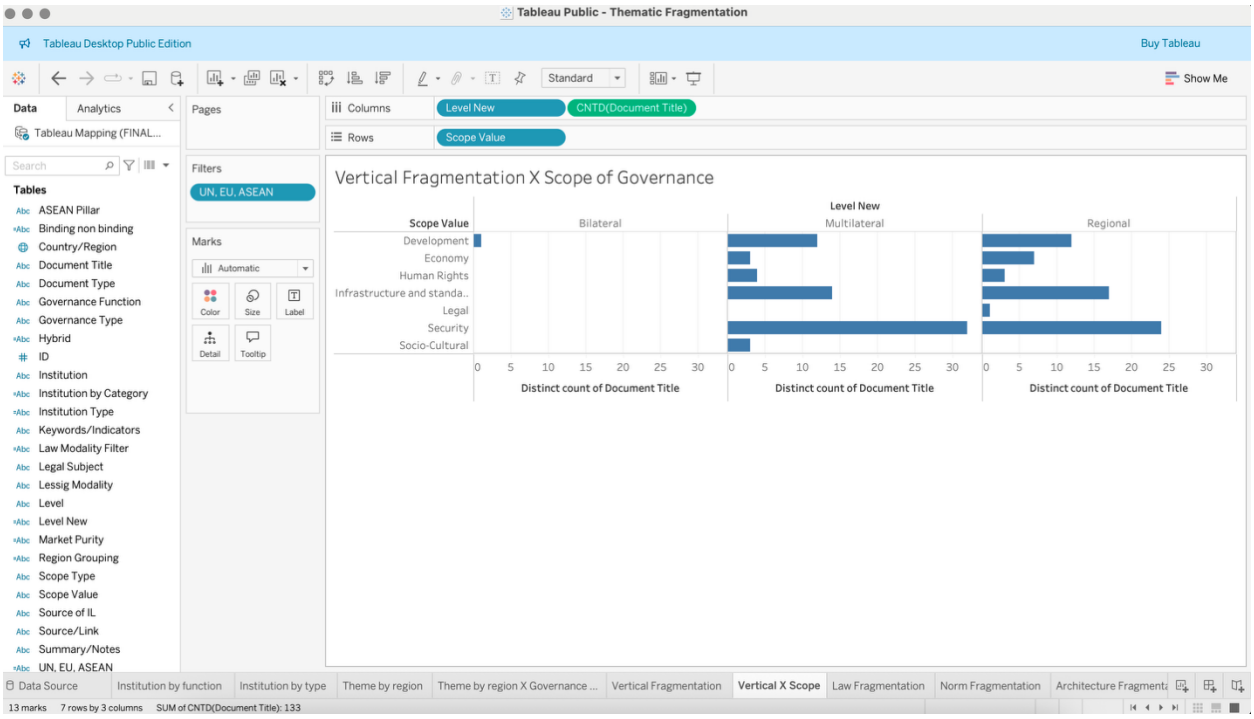


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Pages
Columns
Level New
CNTD(Document Title)
Rows
Scope Value
Filters
UN, EU, ASEAN
Marks
Automatic
Color
Size
Label
Detail
Tooltip
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Vertical Fragmentation X Scope of Governance
Level New
Scope Value
Bilateral
Multilateral
Regional
Development
Economy
Human Rights
Infrastructure and standa..
Legal
Security
Socio-Cultural
0 5 10 15 20 25 30
Distinct count of Document Title
Data Source
Institution by function
Institution by type
Theme by region
Theme by region X Governance ...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmenta
13 marks
7 rows by 3 columns
SUM of CNTD(Document Title): 133

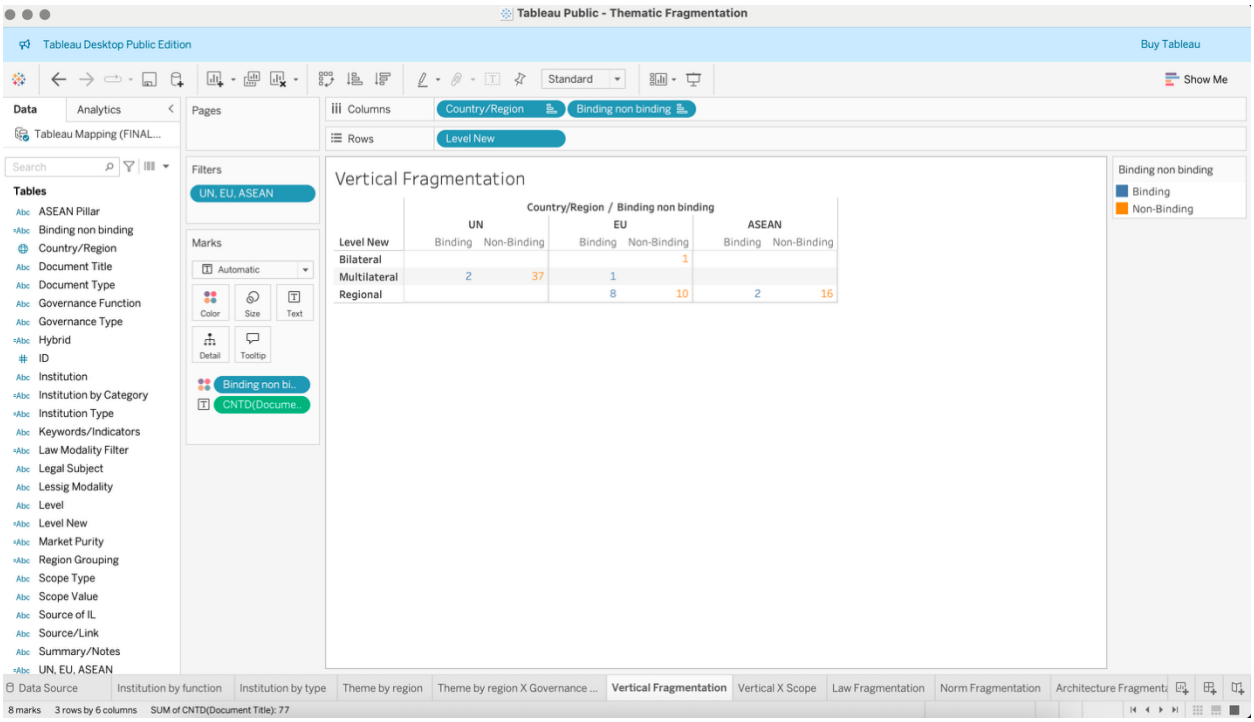


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Data
Analytics
Tableau Mapping (FINAL...
Pages
Columns
Country/Region
Binding non binding
Rows
Level New
Filters
UN, EU, ASEAN
Marks
Automatic
Color
Size
Text
Detail
Tooltip
Binding non bi..
CNTD(Docume..
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Vertical Fragmentation
Country/Region / Binding non binding
UN
EU
ASEAN
Level New
Binding
Non-Binding
Bilateral
1
Multilateral
2
37
1
Regional
8
10
2
16
Binding non binding
Binding
Non-Binding
Data Source
Institution by function
Institution by type
Theme by region
Theme by region X Governance ...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
Architecture Fragmenta
8 marks
3 rows by 6 columns
SUM of CNTD(Document Title): 77

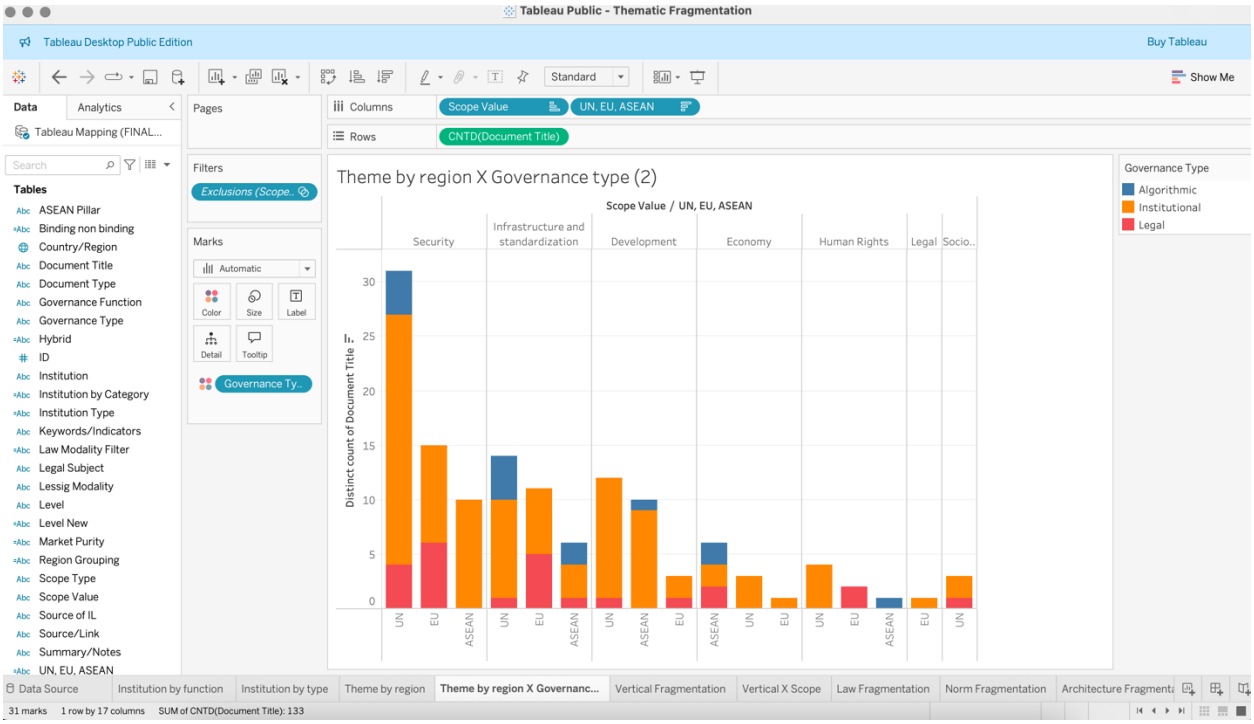


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Columns
Scope Value
UN, EU, ASEAN
Rows
CNTD(Document Title)
Theme by region X Governance type (2)
Scope Value / UN, EU, ASEAN
Security
Infrastructure and standardization
Development
Economy
Human Rights
Legal
Socio..
Distinct count of Document Title
Governance Type
Algorithmic
Institutional
Legal
Tables
ASEAN Pillar
Binding non binding
Country/Region
Document Title
Document Type
Governance Function
Governance Type
Hybrid
ID
Institution
Institution by Category
Institution Type
Keywords/Indicators
Law Modality Filter
Legal Subject
Lessig Modality
Level
Level New
Market Purity
Region Grouping
Scope Type
Scope Value
Source of IL
Source/Link
Summary/Notes
UN, EU, ASEAN
Data Source
Institution by function
Institution by type
Theme by region
Theme by region X Governanc...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
31 marks
1 row by 17 columns
SUM of CNTD(Document Title): 133

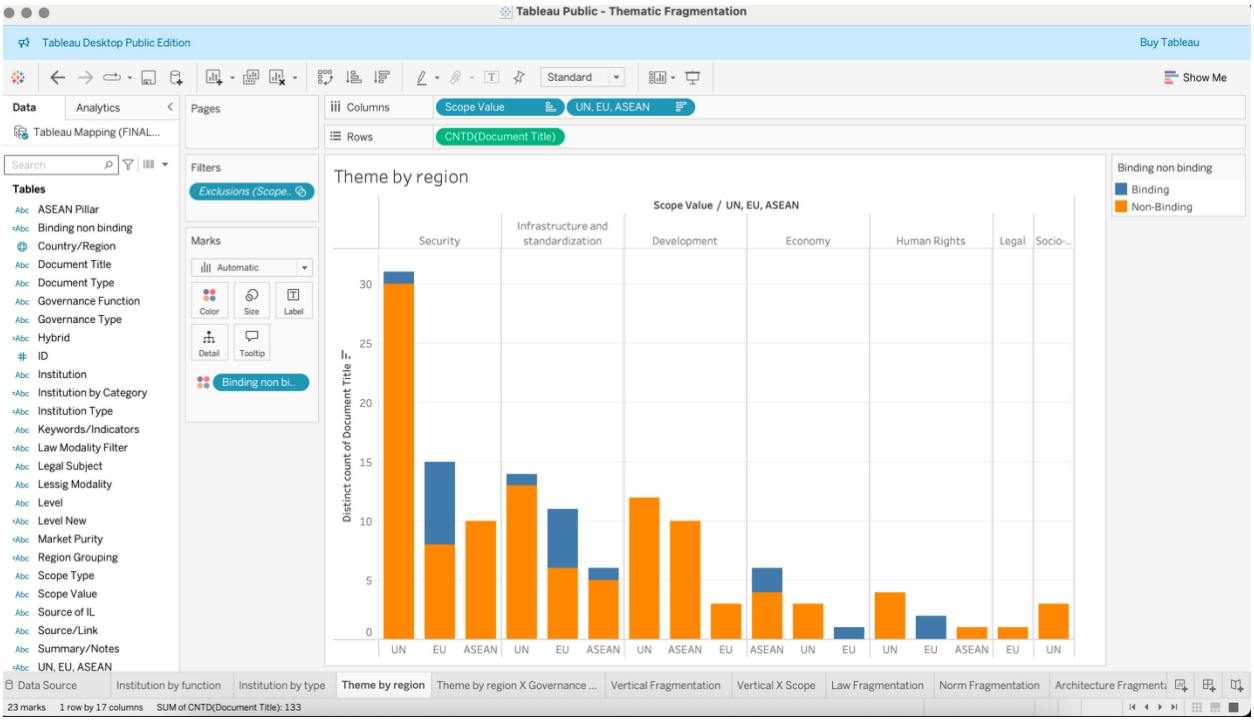


Tableau Public - Thematic Fragmentation
Tableau Desktop Public Edition
Buy Tableau
Show Me
Columns
Scope Value
UN, EU, ASEAN
Rows
CNTD(Document Title)
Theme by region
Scope Value / UN, EU, ASEAN
Security
Infrastructure and standardization
Development
Economy
Human Rights
Legal
Socio-..
Distinct count of Document Title
Binding non binding
Binding
Non-Binding
Tables
Theme by region
Theme by region X Governance ...
Vertical Fragmentation
Vertical X Scope
Law Fragmentation
Norm Fragmentation
23 marks
1 row by 17 columns
SUM of CNTD(Document Title): 133

REFERENCES

Books

Alschner Wolfgang. *Research Methods in International Law*. Edited by Rossana Deplano and Nicholas Tsagourias. Edward Elgar Publishing, 2021

Alvarez, José E. *International Organizations as Law Makers*. Edited by José E Alvarez. Oxford University PressOxford, 2006. https://doi.org/10.1093/acprof:oso/9780198765639.003.0001.

Arvidsson, Matilda, and Emily Jones. *International Law and Posthuman Theory*. London: Routledge, 202

Baldwin, Robert, Martin Cave, and Martin Lodge. *The Oxford Handbook of Regulation*. *The Oxford Handbook of Regulation*. Oxford University Press, 2010

Barnett, Michael, and Raymond Duvall. "Power in Global Governance." In *Power in Global Governance*, Cambridge University Press, 2004.

Benkler, Yochai. *The Wealth of Networks How Social Production Transforms Markets and Freedom*. Yale University Press, 2006.

Castells Manuel. *The Internet Galaxy*. Oxford University Press, 2002

Chesterman Simon, Owada Hisashi, and Saul Be. *The Oxford Handbook of International Law in Asia and the Pacific,* Oxford , 2019

Drahos Peter, *Regulatory Theory: Foundations and Applications*, ANU Press, 2017

Delerue François, Sukumar Arun, Broeders Dennis. "RESPONSIBLE BEHAVIOUR IN CYBERSPACE Global Narratives and Practice Edited By," n.d.

Fang, Binxing. *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Springer Singapore, 2018

Gillespie, Tarleton. *Custodians of the Internet*. Yale University Press, 2019

Heidbreder, Eva G., and Gijs Jan Brandsma, *The Palgrave Handbook of Public Administration and Management in Europe*, London: Palgrave Macmillan UK, 2018

Huddleston R, Jamieson Thomas, James Patrick, *Handbook of Research Methods in International Relations*, Edward Elgar Publishing, 2022

Kenney, Martin. *Understanding Sillicon Valley*. Edited by Martin Kenney. Stanford Business Books, 2000

Krasner, Stephen D. *International Regimes*, Cornell University Press, 1983

Lessig, Lawrence. *Code*. Basic Books, 2008.

Lessig, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. Cambridge: Basic Books, 2006.

Malick Tafsir Ndiaye, Wolfrum Rüdiger, *Law of the Sea, Environmental Law and Settlement of Disputes*, Martinus Nijhoff Publishers, 2007

Padirac Bruno, *The International Dimensions of Cyberspace Law*, 1st ed, Routledge, 2000

Portnoy, Michael, and Seymour Goodman. *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. New York: Springer, 2009

Rachman, Gideon. *Easternization: Asia's Rise and America's Decline from Obama to Trump and Beyond*. Other Press, 2016

Samuel Cherian, Sharma Munish, *Securing Cyberspace: International and Asian Perspectives*, Pentagon Press, 2016

Stokke, Olav Schram. *Governing High Seas Fisheries*. Edited by Olav Schram Stokke. Oxford University Press, 2001

Takashi Shiraishi, Tetsushi Sonobe, *Emerging States and Economies: Their Origins, Drivers, and Chalenges Ahead*, Springer, 2019

Thomas, Pradip Ninan. *Platform Regulation, Exemplars, Approaches, and Solutions*. Oxford University Press, 2023

Tsagourias Nicholas, Buchan Russel, *Research Handbook on International Law in Cyberspace*, Edward Elgar Publishing, 2021

Yee Fen Lim. *Law and Regulation in Cyberspace*. 2nd ed. Oxford University Press, 2007.

Zittrain, Jonathan L. *The Future of the Internet and How to Stop It*. Yale University Press & Penguin UK, 2008.

Journal Articles

Alter, Karen J., and Sophie Meunier. "The Politics of International Regime Complexity." *Perspectives on Politics* 7, no. 1 (March 2009): 13–24. https://doi.org/10.1017/S1537592709090033.

Al-Mahrouqi, Aadil & Cianain, Cormac & Kechadi, Tahar. (2015). Cyberspace Challenges and Law Limitations. International Journal of Advanced Computer Science and Applications. 6. 10.14569/IJACSA.2015.060837

Asyari, Haekal Al. “Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law.” *AUC IURIDICA* 69, no. 4 (December 4, 2023): 211–28. https://doi.org/10.14712/23366478.2023.56.

Austin, Greg, Kai Lin Tay, and Munish Sharma. “China’s Cyber Influencingand Interference.” *International Institute for Strategic Studies*, 2022. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/02/great-power-offensive-cyber-campaigns_04-china.pdf.

Barrinha, André, and Rebecca Turner. “Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India.” *Contemporary Security Policy* 45, no. 1 (January 2, 2024): 72–109. https://doi.org/10.1080/13523260.2023.2266906.

Benvenisti, Eyal, and George W Downs. “The Empire’s New Clothes: Political Economy and the Fragmentation of International Law.” *Stanford Law Review* 60, no. 2 (2007): 595–631.

Burley, Anne-Marie Slaughter. “International Law and International Relations Theory: A Dual Agenda.” *American Journal of International Law* 87, no. 2 (April 10, 1993): 205–39. https://doi.org/10.2307/2203817.

Cai, Cuihong, and Ruoyang Zhang. “Fragmentation of Global Cybersecurity Governance: Quasi-Public Goods and Multi-Level Conflicts.” *Global Political Economy* 4, no. 1 (March 2025): 32–50. https://doi.org/10.1332/26352257Y2024D000000016.

Chen, Xuechen, and Yifan Yang. “Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance.” *International Spectator* 57, no. 3 (2022): 48–65. https://doi.org/10.1080/03932729.2022.2066841.

Chesterman, Simon. “Asia’s Ambivalence about International Law and Institutions: Past, Present and Futures.” *European Journal of International Law* 27, no. 4 (November 29, 2016): 945–78. https://doi.org/10.1093/ejil/chw051.

Csonka, Peter. “The Council of Europe’s Convention on Cyber-Crime and Other European Initiatives.” *Revue Internationale de Droit Pénal* Vol. 77, no. 3 (September 17, 2007): 473–501. https://doi.org/10.3917/ridp.773.0473.

Delerue, François, Arun Sukumar, and Dennis Broeders. *Responsible Behaviour in Cyberspace: Global Narratives and Practice* . EU Cyber Direct, 2023. https://doi.org/10.2815/643871.

Dyson, Matthew. “The Idea of Public Law by Martin Loughlin.” *The Cambridge Law Journal*

64, no. 2 (July 23, 2005): 503–4. https://doi.org/10.1017/S0008197305226946.

Esade, Fundación, Athanasios Kouliopoulos, Marie Vandendriessche, and Angel Saz-Carranza. "Case Study of Cyber Governance," 2020.

Fattedad, Sarah Collins, Michael DeVito, Yasmin Góes, Mariam Khorenyan, and Leila Milgrim. "Towards A Global Digital Governance Architecture: Mapping Pathways for Cooperation and Inclusion 2," n.d.

Faude, Benjamin, and Felix Groβe-Kreul. "Let's Justify! How Regime Complexes Enhance the Normative Legitimacy of Global Governance." *International Studies Quarterly* 64, no. 2 (June 1, 2020): 431–39. https://doi.org/10.1093/isq/sqaa024.

Faude Benjamin, Groβe-Kreul, Felix "Let's Justify! How Regime Complexes Enhance the Normative Legitimacy of Global Governance." *International Studies Quarterly* 64, no. 2 (June 1, 2020): 431–39. https://doi.org/10.1093/isq/sqaa024.

Feraru, Atena S. "ASEAN Decision-Making Process: Before and after the ASEAN Charter." *Asian Development Policy Review* 4, no. 1 (2016): 26–41. https://doi.org/10.18488/journal.107/2016.4.1/107.1.26.41.

Christoph Engel and Kenneth H. Keller, *Governance of Global Networks in the Light of Differing Local Values*, edited by. Law and Economics of International Telecommunications – Wirtschaftsrecht der internationalen Telekommunikation, 2001.

Goldsmith J, "Unilateral Regulation of the Internet: A Modest Defence." *European Journal of International Law* 11, no. 1 (January 1, 2000): 135–48. https://doi.org/10.1093/ejil/11.1.135.

González Fuster, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Vol. 16. Cham: Springer International Publishing, 2014. https://doi.org/10.1007/978-3-319-05023-2.

Greenstein, Shane. "Commercialization of the Internet: The Interaction of Public Policy and Private Choices or Why Introducing the Market Worked so Well." *Innovation Policy and the Economy* 1 (January 2000): 151–86. https://doi.org/10.1086/ipe.1.25056144.

Habermas, Jürgen. *Theorie Des Kommunikativen Handelns*. Vol. 1. Suhrkamp, 1995.

Heinl, Caitríona. "Asia Pacific Contributions to International Cyber Stability," n.d. https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace,.

Henning, C Randall, Tyler Pratt, Robert Keohane, Axel Marx, Jean-Frédéric Morin, Julia Morse,

Christina Davis, et al. “Hierarchy and Differentiation in International Regime Complexes: A Theoretical Framework for Comparative Research,” 2020.

Hofmann, Stephanie C., and Patryk Pawlak. “Governing Cyberspace: Policy Boundary Politics across Organizations.” *Review of International Political Economy* 30, no. 6 (November 2, 2023): 2122–49. https://doi.org/10.1080/09692290.2023.2249002.

Hutchison, C. “Ecological Sensitivity and Global Legal Pluralism: Rethinking the Trade and Environment Conflict.” *Journal of Environmental Law* 18, no. 1 (December 2, 2005): 172–76. https://doi.org/10.1093/jel/eqi043.

Jain, Sushil. “Easternization of the West: An Essay in Reverse Colonization.” *SSRN Electronic Journal*, September 1, 1988. https://doi.org/10.2139/SSRN.1851868.

Kittichaisaree, Kriangsak. *Public International Law of Cyberspace*. Vol. 32. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-54657-5.

Kokott, J., and C. Sobotta. “The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR.” *International Data Privacy Law* 3, no. 4 (November 1, 2013): 222–28. https://doi.org/10.1093/idpl/ipt017.

Koskenniemi, Martti. “The Fate of Public International Law: Between Technique and Politics.” *The Modern Law Review* 70, no. 1 (January 4, 2007): 1–30. https://doi.org/10.1111/j.1468-2230.2006.00624.x.

Kuerbis, Brenden, and Farzaneh Badiei. “Mapping the Cybersecurity Institutional Landscape.” *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 466–92. https://doi.org/10.1108/DPRG-05-2017-0024/FULL/XML.

Lewis, James. “Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia,” n.d. https://www.interpol.int/Public/ICPO/PressReleases/PR2010/PR052.asp.

Li, Yuchong, and Qinghui Liu. “A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments.” *Energy Reports* 7 (November 2021): 8176–86. https://doi.org/10.1016/j.egyr.2021.08.126.

Lie, Runar Hilleren, and Malcolm Langford. “The Computational Turn in International Law.” *Nordic Journal of International Law* 93, no. 1 (2024): 38–67. https://doi.org/10.1163/15718107-bja10081.

Mačák, Kubo, Talita Dias, and Ágnes Kasper. *Handbook on Developing a National Position on International Law and Cyber Activities A Practical Guide for States*, 2025.

Maisaia, V., Guchua, A., & Zedelashvili, T. (2020). The cybersecurity of Georgia and threats from Russia. Eastern Review, 9, 105–119. https://doi.org/10.18778/1427-9657.09.07

Mendez, Fernando. "The European Union and Cybercrime: Insights from Comparative Federalism." *Journal of European Public Policy* 12, no. 3 (June 20, 2005): 509–27. https://doi.org/10.1080/13501760500091737.

Missiroli, Antonio. *Geopolitics and Strategies in Cyberspace: Actors, Actions, Structures and Responses Hybrid CoE Paper 7*, n.d. www.hybridcoe.fi.

Mostert, Menno, Annelien L. Bredenoord, Bart Van Der Slootb, and Johannes J.M. Van Delden. "From Privacy to Data Protection in the EU: Implications for Big Data Health Research." *European Journal of Health Law*. Brill Nijhoff, 2017. https://doi.org/10.1163/15718093-12460346.

Murata, Kiyoshi, Andrew A. Adams, and Ana María Lara Palma. "Following Snowden: A Cross-Cultural Study on the Social Impact of Snowden's Revelations." *Journal of Information, Communication and Ethics in Society* 15, no. 3 (August 14, 2017): 183–96. https://doi.org/10.1108/JICES-12-2016-0047.

Noor, Elina. "Positioning ASEAN in Cyberspace." *Asia Policy* 15, no. 2 (April 1, 2020): 107–14. https://doi.org/10.1353/ASP.2020.0033.

Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." *Global Commission on Internet Governance*, no. Paper Series No.1 (May 2014).

Öberg, Marko Divac. "The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ." *European Journal of International Law* 16, no. 5 (November 1, 2005): 879–906. https://doi.org/10.1093/ejil/chi151.

Orellana, M.A. "The Swordfish Dispute between the EU and Chile at the ITLOS and the WTO." *Nordic Journal of International Law* 71, no. 1 (2002): 55–81. https://doi.org/10.1163/157181002400497867.

Paasi, Anssi. "The Resurgence of the 'Region' and 'Regional Identity': Theoretical Perspectives and Empirical Observations on Regional Dynamics in Europe." *Review of International Studies* 35, no. S1 (February 1, 2009): 121–46. https://doi.org/10.1017/S0260210509008456.

Paulus, Andreas L. "Legitimacy of International Law and the Role of the State Legitimacy of International Law and the Role of the State THE LEGITIMACY OF INTERNATIONAL

LAW AND THE ROLE OF THE STATE INTRODUCTION: FRAGMENTATION AND THE ROLE OF THE STATE." *Michigan Journal of International Law*. Vol. 25, 2004. https://repository.law.umich.edu/mjilhttps://repository.law.umich.edu/mjil/vol25/iss4/13.

Perritt, Henry H, and Henry H Perriti. "The Internet Is Changing International Law, 73 Chi." *L. Rev*. Vol. 73, 1998. https://scholarship.kentlaw.iit.edu/cklawreviewAvailableat:https://scholarship.kentlaw.iit.edu/cklawreview/vol73/iss4/4.

Ratai, Balazs. "Understanding Lessig - Implications for EU Cyberspace Policy." *International Review of Law, Computers & Technology*, 2005, 277–86. https://papers.ssrn.com/abstract=905866.

Raustiala, Kal, and David G. Victor. "The Regime Complex for Plant Genetic Resources." *International Organization*, March 2004. https://doi.org/10.1017/S0020818304582036.

Mark Raymond, "Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot,"

Raymond, Mark, and Justin Sherman. "Authoritarian Multilateralism in the Global Cyber Regime Complex: The Double Transformation of an International Diplomatic Practice." *Contemporary Security Policy* 45, no. 1 (2024): 110–40. https://doi.org/10.1080/13523260.2023.2269809.

Ross, Andrew R. N., Cristian Vaccari, and Andrew Chadwick. "Russian Meddling in U.S. Elections: How News of Disinformation's Impact Can Affect Trust in Electoral Outcomes and Satisfaction with Democracy." *Mass Communication and Society* 25, no. 6 (November 2, 2022): 786–811. https://doi.org/10.1080/15205436.2022.2119871.

Ruismäki, Arttu. "Applying Lessig's Pathetic Dot Theory on Regulation of Digital Video Game Distribution Platforms." Hanken School of Economics, 2022.

Sari, Monica Nila. "ASEAN Regional Effort on Cybersecurity and Its Effectiveness," n.d. https://docs.broadcom.com/doc/istr-22-2017-en.

Shakarian, Paulo. "The 2008 Russian Cyber-Campaign Against Georgia." *Military Review*, 2011, 63–68.

Haataja, S, The 2007 cyber-attacks against Estonia and international law on the use of force: an informational approach. Law, Innovation and Technology, 9(2), 2017

Sidhu, Waheguru Pal Sing. "Regional Peace and Security." In *Chesterman Simon, Owada*

Hisashi, and Saul Be, The Oxford Handbook of International Law in Asia and the Pacific, edited by Simon, Chesterman, Hisashi Owada, and Ben Saul. Oxford University Press, 2019.

Sieber, U. "The Emergence of Information Law: Object and Characteristics of a New Legal Area." In *Law, Information and Information Technology*, edited by Eli Lederman and Ron Shapira. Kluwer Law International, 2001.

Sliwinski, Krzysztof Feliks. "Moving beyond the European Union's Weakness as a Cyber-Security Agent." *Contemporary Security Policy* 35, no. 3 (September 2, 2014): 468–86. https://doi.org/10.1080/13523260.2014.959261.

Sloot, Bart Van Der. "Privacy as Human Flourishing Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?," 2014. http://nbn-resolving.

Stadnik, Ilona. "What Is an International Cybersecurity Regime and How We Can Achieve It?" *Masaryk University Journal of Law and Technology* 11, no. 1 (June 30, 2017): 129–54. https://doi.org/10.5817/MUJLT2017-1-7.

Stockmann, Daniela. "Tech Companies and the Public Interest: The Role of the State in Governing Social Media Platforms." *Information, Communication & Society* 26, no. 1 (January 2, 2023): 1–15. https://doi.org/10.1080/1369118X.2022.2032796.

Sukumar, Arun, Dennis Broeders, and Monica Kello. "The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy." *Contemporary Security Policy* 45, no. 1 (January 2, 2024): 7–44. https://doi.org/10.1080/13523260.2023.2296739.

Tan, Eugene E.G., and Benjamin Ang. "ASEAN Ambiguity on International Law and Norms for Cyberspace." *Baltic Yearbook of International Law*, 20:133–62. Brill Nijhoff, 2022. https://doi.org/10.1163/22115897_02001_008.

Tekunan, Susy. "The Asean Way: The Way To Regional Peace?" *Jurnal Hubungan Internasional* 3, no. 2 (2014): 142–47. https://doi.org/10.18196/hi.2014.0056.142-147.

Tiirmaa-Klaar, Heli. "The Evolution of the UN Group of Governmental Experts on Cyber Issues From a Marginal Group to a Major International Security Norm-Setting Body Cyberstability Paper Series New Conditions and Constellations in Cyber," 2021.

Tikk-Ringas, Eneken. "International Cyber Norms Dialogue as an Exercise of Normative Power." *Georgetown Journal of International Affairs* 17, no. 3 (2016): 47–59.

https://doi.org/10.1353/gia.2016.0036.

Trigueño, Eslava L. “International Law: On (Most of) the World Being (Always, Somehow) Out of Place.” In *Out of Place: Fieldwork and Positionality in Law and Society*, edited by LJ Chua and MF Massoud, 160–87. Cambridge Studies in Law and Society, Cambridge University Press, n.d.

Urgessa, Worku Gedefa. “Multilateral Cybersecurity Governance: Divergent Conceptualizations and Its Origin.” *Computer Law & Security Review* 36 (April 2020): 105368. https://doi.org/10.1016/j.clsr.2019.105368.

Weggener, Henning. “Cyber Peace.” In *The Quest for Cyber Peace*, 77–86. International Telecommunications Union, 2011.

Wessel, Ramses A. “European Law and Cyberspace.” In *Research Handbook on International Law and Cyberspace*, edited by Nicholas Tsagourias and Russell Buchan, 491–408. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.

Whittaker, Jason. *The Cyberspace Handbook*. Routledge, 2004. https://doi.org/10.4324/9780203486023.

Whittle, Devon. “The Limits of Legality and the United Nations Security Council: Applying the Extra-Legal Measures Model to Chapter VII Action.” *European Journal of International Law* 26, no. 3 (August 1, 2015): 671–98. https://doi.org/10.1093/ejil/chv042.

Young, Margaret A. “Introduction: The Productive Friction between Regimes.” In *Regime Interaction in International Law*, edited by Margaret A Young. Cambridge University Press, 2012.

Reports

Appellate Body Report, United States – Import Prohibition of Certain Shrimp and Shrimp Products, WT/DS58/AB/R (circulated 12 October 1998) (DSR 1998:VII, 2755)

Committee, Counter Terrorism. “Concept Note Special Meeting of the Counter-Terrorism Committee with Member States and Relevant International and Regional Organisations, Civil Society and the Private Sector on ‘Preventing the Exploitation of Information and Communications Technologies for Terrorist Purposes, While Respecting Human Rights and Fundamental Freedoms,2016.

Counter-Terrorism Committee Executive Directorate. “Technical Meeting of the Counter-

Terrorism Committee Executive Directorate on 'Preventing Terrorists from Exploiting the Internet and Social Media to Recruit Terrorists and Incite Terrorist Acts, While Respecting Human Rights and Fundamental Freedoms' Final Agenda Opening Session," 2015

Counter Terrorism Implementation Task Force. "COUNTER-TERRORISM IMPLEMENTATION TASK FORCE CTITF,"

CTITF Working Group on Use of the Internet for Terrorist Purposes Riyadh Conference on Use of the Internet to Counter the Appeal of Extremist Violence' (January 2011) http:// www .un .org/ en/ terrorism/ ctitf/ pdfs/ ctitf _riyadh _conference _summary _recommendations .pdf.

ECOSOC General segment briefing on "Cyber security: emerging threats and challenges", 'Special Event on Cybersecurity and Development – Informal summary' (9 December 2011) http://www.un.org/en/ecosoc/cybersecurity/summary.pdf.

Falco, Marco De. "Stuxnet Facts Report: A Technical and Strategic Analysis." Tallin, 2012

Final Report, World Telecommunication Development Conference, Buenos Aires (9-20 October 2017) https:// www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

Labs, Fireeye. "APT30 and The Mechanics of a Long-Running Cyber Espionage Operation," 2015.

Kouliopoulos, Athanasios, Marie Vandendriessche, and Angel Saz-Carranza. "Report: Case Study of Cyber Governance," 2020

Intersessional Panel of the Commission on Science and Technology for Development. "The Mapping of International Internet Public Policy Issues Database," 2015.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Cooperative Cyber Defence Centre of Excellence, 2007.

Panel Report, EC – Measures Affecting the Approval and Marketing of Biotech Products Panel Report WT/DS291/R, WT/DS292/R, WT/DS293/R (circulated 29 September 2006) (DSR 2006:III, 847).

Security Council Report, 'In Hindsight: The Security Council and Cyber Threats' (23 December 2019) https:// www.securitycouncilreport.org/monthly-forecast/2020 -01/the-security-council-and-cyber-threats.php.

UN Counter-terrorism Implementation Task Force, 'Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes' (February 2009) http:// www .un .org/ en/

terrorism/ ctitf/ pdfs/ wg6 -internet _rev1 .pdf.
UN Counter-terrorism Implementation Task Force, 'Countering the Use of the Internet for Terrorist Purposes: Legal and Technical Aspects' (May 2011) http:// www .un .org/ en/ terrorism/ ctitf/ pdfs/ WG _Compendium -Legal _and _Technical _Aspects _2011 .pdf.
Use of Nuclear Weapons in Armed Conflict (1999) (I) ICJ Rep 66.

Laws

Agreement on the Application of Sanitary and Phytosanitary Measures (signed 15 April 1994) in WTO, The Legal Texts (Cambridge University Press, 1999)
Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks (1995) 34 ILM 1547 (in force 11 December 2001
Agreement Establishing the World Trade Organization (signed 15 April 1994) in WTO
Charter of the Association of Southeast Asian Nations, Nov. 20, 2007, 2624 UNTS 223
Statute of the International Court of Justice, art. 38(1), 59 Stat. 1055, 33 UNTS 993 (1945)
International Telecommunication Regulations, Dec. 9, 1988, 1589 UNTS 3.
ASEAN Agreement on Electronic Commerce, Jan. 22, 2019
e-ASEAN Framework Agreement, Nov. 24, 2000, 2216 UNTS 233
United Nations Convention on the Law of the Sea (1982) 21 ILM 1261 (1982) (in force 16 November 1994).

Case Law

CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238
CJEU, Case C-139/01, Österreichischer Rundfunk and Others, ECLI:EU:C:2003:294
ECtHR Gabriele Weber and Cesar Richard Saravia v. Germany, App no. 54934/00
ECtHR, Gaskin v. United Kingdom, App no. 10454/83 (7 July 1989)
ECtHR, Khelili v. Switzerland, App no. 16188/07 (18 October 2011)

Internet Sources

Australia's Position on the Application of Internatioanl Law to State Conduct in Cyberspace,

https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf,

Council of the European Union, Declaration on a Common Understanding of International Law in Cyberspace, 2024, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

Drake J, William. *The Working Group on Internet Governance*. https://www.apc.org/sites/default/files/IG_10_Final_0.pdf.

Statista, Estimated Cost of Cybercrime Worldwide, https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Global Cybersecurity Agenda (GCA)' (ITU) http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report .pdf

Grant Gross, "Cyber Attack on Georgia Outages Websites," Wall Street Journal, August 12, 2008, https://www.wsj.com/articles/SB121850756472932159.

National position of the United States of America (2021) https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021)

LexisNexis. Harmonisation. Last modified 2024. https://www.lexisnexis.co.uk/legal/guidance/harmonisation-01

OECD (2020), Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement, OECD, Paris, accessed on 27 May 2021 from www.oecd.org/digital/digital-economy-outlook-covid.pdf.

Viebeck, Elise. "Cyberattacks Followed Malaysia Airlines Flight Disappearance." The Hill, 2015.

World Health Organization (2020), Novel Coronavirus(2019- NCoV) Situation Report - 13, accessed on 27 May 2021 from https://www.who.int/docs/defaultsource/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

The Federal Government of Germany, On the Application of International Law in Cyberspace, Position Paper, 2021, https://www.auswaertiges-amt.de/resource/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-

of-international-law-in-cyberspace-data.pdf

The use of the internet for terrorist purposes' (UN, 2012) http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes .pdf.