Introduction

TOMOKO ISHIKAWA AND YARIK KRYVOI

1.1 Background: Cybersecurity and the Backlash against Economic Globalisation

The deep integration of internet technologies in our everyday life and business has dramatically impacted the first decades of the twenty-first century. Artificial intelligence, autonomous vehicles, cryptocurrencies, and the Internet of Things have become ubiquitous and continue to expand. The COVID-19 pandemic resulted in individuals and businesses spending more time and money online.[1] These developments increased our dependence on the Internet, and access to an open, stable, and secure cyberspace plays a crucial role not only for businesses but also for the wellbeing and functioning of people's lives.

Simultaneously, the number and sophistication of cybercrimes keeps increasing, indicating that the current cyber regulation has failed to catch up with rapidly emerging cyberthreats. It is reported that in 2021, 80 per cent of businesses experienced ransomware attacks.[2] Reported cases of malicious uses of cyberspace as a way of advancing the interest of states have increased, which includes Russia declaring itself the first state ever to launch a COVID-19 vaccine for public use, following official reports from the United Kingdom that Russian hackers had attempted to steal data relating to its COVID-19 vaccine research. The European Union and the United States attributed a distributed denial of service (DDoS) attack on Ukrainian internet infrastructure to Russian military cyber

[1] UNCTAD, 'COVID-19 Boost to E-commerce Sustained into 2021, New UNCTAD Figures Show', 25 April 2022, available at: https://unctad.org/news/covid-19-boost-e-commerce-sustained-2021-new-unctad-figures-show (accessed 30 September 2022).

[2] Roxanne Libatique, 'Mimecast: 80% of Businesses Experienced Ransomware Attacks in 2021' *Insurance Business Australia*, 25 May 2022, available at: www.insurancebusinessmag.com/au/news/cyber/mimecast-80-of-businesses-experienced-ransomware-attacks-in-2021-407181.aspx (accessed 30 September 2022). See also Derek Reveron and Kathleen A. Mahoney-Norris, *Human and National Security: Understanding Transnational Challenges*, 2nd ed. (New York: Routledge, 2019), 3.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

operators. This attack was reported to be a part of Russia's hybrid warfare strategy for the invasion of Ukraine in February 2022.[3]

This century has also witnessed the intensification of interstate competition for dominance in terms of both technology and normative development in cyberspace. One notable example is the diffusion of 5G technologies, which could form the backbone of national competitiveness and innovation in the future. States compete over who develops technologies, sets standards (relevant for establishing levels of performance and compatibility), and holds the relevant intellectual property.[4] As discussed further in Chapters 2 and 4, the major cyberpowers – the United States and its allies, on the one hand, and China and Russia, on the other – have presented and supported contrasting agendas on cyber norms.[5]

China has recently risen as a key 'non-Western' economic and political power. Rapidly growing Chinese investments in strategic technology firms in other countries have drawn renewed public attention to the security risks posed by foreign investment and trade. This has contributed to the acceleration of the current backlash against economic globalisation. Since 2016, major Western economies have begun to introduce, or to tighten, foreign direct investment (FDI) screening mechanisms,[6] with cybersecurity serving as an important justification for this policy shift.[7] As major economies reassert control over borders, they may

[3] Drew Todd, 'Western Allies Blame Russia for DDoS Attack on Ukrainian Satellites' *Secureworld*, 11 May 2022, available at: www.secureworld.io/industry-news/allies-blame-russia-ddos-ukraine (accessed 30 September 2022). For social media disinformation and manipulation related to the Ukrainian war, see Zara Abrams, 'The Role of Psychological Warfare in the Battle for Ukraine' (2022) 53(4) *Monitor on Psychology* 18–21 at 18.

[4] James A. Lewis, 'How 5G Will Shape Innovation and Security: A Primer' (2018) *Center for Strategic and International Studies, A Report of the CSIS Technology Policy Program* 1–18.

[5] Michael J. Mazarr et al., 'Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity' (2022) *RAND Institute Research Report* 20–26, available at: www.rand.org/pubs/research_reports/RRA1180-1.html (accessed 30 September 2022).

[6] For example, OECD, 'Investment Policies Related to National Security and Public Order', available at: www.oecd.org/investment/investment-policy/investment-policy-national-security.htm (accessed 30 September 2022); UNCTAD, 'National Security-Related Screening Mechanisms for Foreign Investment: An Analysis of Recent Policy Developments' (2019) *Investment Policy Monitor*, available at: https://investmentpolicy.unctad.org/publications/1213/investment-policy-monitor-special-issue—national-security-related-screening-mechanisms-for-foreign-investment-an-analysis-of-recent-policy-developments (accessed 30 September 2022).

[7] This is discussed in Chapter 8.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

be tempted to rely on the concept of cybersecurity to pursue protectionist goals, thus fuelling the backlash against economic globalisation. These actions may also conflict with international law frameworks on trade and investment founded on the concept of economic openness.

These intensifying cyberthreats, increasing geopolitical tensions, and a backlash against economic globalisation call for a reassessment of cybersecurity governance.

1.2 Aims and Scope

This book examines cybersecurity challenges, governance responses to them, and their limitations, engaging in an interdisciplinary approach combining legal and international relations disciplines. It builds on the fundamental premise that cybersecurity challenges require a widely agreed-upon set of international norms. Domestic laws and regulations play a primary role in governing cyberspace. Although intergovernmental agreements (both binding and non-binding) between like-minded states[8] and private sector voluntary standards[9] tackle an increasing number of cybergovernance and cybersecurity issues, the world still lacks widely accepted norms on cybersecurity. States have attempted to agree on universal norms for cyber and cybersecurity governance at the United Nations (as discussed in detail in Chapters 2 and 4) and other forums[10] but so far have failed to produce a universally

[8] They include the Budapest Convention, the African Union Cyber Security and Protection of Personal Data Convention, League of Arab States' Arab Convention on Combating Information Technology Offences, OECD Online Identity Theft Guidelines, the Paris Call for Trust and Security in Cyberspace, the SCO's Codes of Conduct for Information Security, the Manila Principles on Intermediary Liability, the European Union & Council on Europe's Global Action on Cybercrime Extended (GLACY)+, the Association for Progressive Communications, the Association for Data and Cyber Governance, and the World Wide Web Consortium.

[9] They include Cybersecurity Tech Accord 2018, National Institute of Standards and Technology Cybersecurity Framework, CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures, International Organization for Standardization and International Electrotechnical Commission, The Global Network Initiative, the Association for Progressive Communications, the Principles of Internet Governance, the Internet Engineering Task Force, Internet Society, Internet Corporation for Assigned Names and Numbers, and the National Information Assurance Partnership programme.

[10] For example, the London Process/the Global Conference on Cyber Space (GCCS) was launched in 2017 with a view to 'establish internationally agreed "rules of the road" for behaviour in cyberspace'. Internet Society, 'Global Conference on Cyber Space (GCCS

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

agreed set of norms. Global cybergovernance now resembles a patchwork of diverse laws and policies. This book offers an interdisciplinary approach involving both law and international relations that explores ways of filling the gap.

The book has three main aims. First, it examines the current political and legal context of cybersecurity governance, highlighting the divide between two contrasting models of cybergovernance. The first approach, taken by the Western countries, puts emphasis on the freedom of cyberspace, the free flow of information, the protection of civil and political rights, and privacy.[11] This book calls this approach the 'market-oriented' model. The other approach, exemplified by most member states of the Shanghai Cooperation Organization (SCO),[12] emphasises states' sovereignty over cyberspace (cyberspace sovereignty), treating information itself as a potential threat.[13] This book calls this approach the 'state-oriented' model. Certainly, there is no 'pure form' of market-oriented model or state-oriented model, as attested to, for example, by the emergence of the concept of 'digital sovereignty' in the European Union as a tool to enable protection and government intervention.[14] Nevertheless, the underlying reasons for governmental intervention,

2017)', available at: www.internetsociety.org/events/gccs-2017/ (accessed 30 September 2022).

[11] See, for example, Council of Europe, 'Internet Governance – Council of Europe Strategy 2016–2019: Democracy, Human Rights and the Rule of Law in the Digital World', available at: https://rm.coe.int/16806aafa9 (accessed 30 September 2022); David P. Fidler, 'Cyberspace and Human Rights', in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and Cyberspace*, 2nd ed. (Cheltenham: Edward Elgar Publishing, 2021), 94–117 at 111; Hitoshi Nasu and Helen Trezise, 'Cyber Security in the Asia-Pacific', in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and Cyberspace*, 2nd ed. (Cheltenham: Edward Elgar Publishing, 2021), 446–464 at 462.

[12] They are the People's Republic of China, the Kyrgyz Republic, the Russian Federation, the Republic of Tajikistan, and the Republic of Uzbekistan. For the list of countries that enforce severe internet censorship, see Paul Bischioff, 'Internet Censorship 2022: A Global Map of Internet Restrictions' *Comparitech*, 25 January 2022, available at: www.comparitech.com/blog/vpn-privacy/internet-censorship-map/ (accessed 30 September 2022).

[13] Laura DeNardis and Mark Raymond, 'Thinking Clearly about Multistakeholder Internet Governance' (2013) Paper Presented at Eighth Annual GigaNet Symposium 1–18 at 15; Nasu and Trezise, 'Cyber Security in the Asia-Pacific', 463.

[14] European Parliament, 'Digital Sovereignty for Europe' *EPRS Ideas Paper: Towards a More Resilient EU* 1–12, available at: www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (accessed 30 September 2022). This point is further discussed in Chapter 6.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

namely, protection of data and citizens' rights, on the one hand, and state control and surveillance, on the other, clearly differ.[15]

The divide between these two models blocks international cooperation on many cybersecurity matters.[16] This book explores this challenge by examining: (a) the liberal international order, the free and open (market-oriented) governance in cyberspace, and the challenges such governance has faced (Chapter 2); (b) China's cybersecurity policy and the concept of 'cyber sovereignty' as a manifestation of the state-oriented model (Chapter 3); and (c) the challenges the cybercrime convention negotiations at the United Nations have faced (Chapter 4).

Second, this book evaluates the success, potential, and limitations of current international and domestic legal frameworks to address emerging cybersecurity threats, focusing on the following specific issues: (a) states' recourse to self-defence and countermeasures under existing international law and through the application of domestic criminal law (Chapter 5); (b) domestic, international, and EU law approaches in the area of data protection (Chapter 6); (c) approaches to balancing liberalisation of digital trade with cybersecurity concerns adopted in multilateral and regional trade agreements (Chapter 7); and (d) the tension between domestic cybersecurity measures and obligations under international investment agreements (IIAs) (Chapter 8).

Third, this book examines the responsibilities and roles of states and private actors in shaping cybersecurity governance. The principle of 'multistakeholderism', which engages all stakeholders, including states, international institutions, technology companies, academics, civil society, and technical experts in discussions, has been accepted as an internet governance principle since the Working Group on Internet Governance

[15] Summer Walker and Ian Tennant, 'Control, Alt, or Delete? The UN Cybercrime Debate Enters a New Phase' *Global Initiative against Transnational Organized Crime*, 22 December 2021, 5, available at: https://globalinitiative.net/analysis/un-cybercrime-debate/ (accessed 22 September 2022).

[16] Fidler, 'Cyberspace and Human Rights', 97; Anders Henriksen, 'The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace' (2019) 5(1) *Journal of Cybersecurity* 1–9 at 5; Martin Ney and Andreas Zimmermann, 'Cyber-Security beyond the Military Perspective: International Law, "Cyberspace", and the Concept of Due Diligence' (2016) 58 *German Yearbook of International Law* 52–66 at 60; Jutta Brunnée and Tamar Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (2016) 58 *German Yearbook of International Law* 129–168 at 159; Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' (2020) 12(2) *Hague Journal on the Rule of Law* 283–305 at 287.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

(WGIG) adopted the following working definition of internet governance:

> [T]he development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.[17]

While debates continue on whether multistakeholderism should apply to different areas of internet governance,[18] successful cybersecurity governance as a component of internet governance (as discussed below) requires the involvement of both the public and private sectors, the latter being defined broadly here to include business industries (in particular technology companies), technical experts, academics, and civil society groups. Neither public nor private sectors alone can sufficiently address cybersecurity threats.[19] The public sector plays an essential role, as cybersecurity requires, for example, setting mandatory laws and regulations and co-operation with other governments in prosecuting cybercriminals. The fact that the primary aim of technology companies, as

[17] UN, 'Report of the Working Group on Internet Governance, Château de Bossey, June 2005' ('WGIG Report'), para. 10. It is observed that, before the WGIG, 'the notion of multistakeholder participation was fairly alien to most governments and even many stakeholders'. William J. Drake, 'Why the WGIG Still Matters', in William J. Drake (ed.), *The Working Group on Internet Governance: 10th Anniversary Reflections* (Association for Progressive Communications, 2016), 10–31 at 12. See also William H. Dutton, 'Multistakeholder Internet Governance?' (2016) *World Development Report Digital Dividends* 20–21, available at: https://thedocs.worldbank.org/en/doc/591571452529901419-0050022016/original/WDR16BPMultistakeholderDutton.pdf (accessed 25 September 2022); Peng Hwa Ang and Sherly Haristya, 'Multistakeholderism and the Democratic Deficit', in William J. Drake (ed.), *The Working Group on Internet Governance: 10th Anniversary Reflections* (Association for Progressive Communications, 2016), 123–140.

[18] See, for example, Dutton, 'Multistakeholder Internet Governance?'; Stefaan G. Verhulst, 'The Practice and Craft of Multistakeholder Governance: The Case of Global Internet Policymaking' (2016) *Global Partners Digital*, available at: www.gp-digital.org/wp-content/uploads/pubs/thepracticeandcraftofmultistakeholderpoliymaking.pdf (accessed 25 September 2022); Mark Raymond and Laura DeNardis, 'Multi-stakeholderism: Anatomy of an Inchoate Global Institution', in Global Commission on Internet Governance, *Who Runs the Internet?: The Global Multi-stakeholder Model of Internet Governance* (2016), 18–43, available at: www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202.pdf (accessed 25 September 2022); DeNardis and Raymond, 'Thinking Clearly about Multistakeholder Internet Governance', 2.

[19] Eugenia Lostri, James Andrew Lewis, and Georgia Wood, 'A Shared Responsibility: Public-Private Cooperation for Cybersecurity' (2022) *Center for Strategic and International Studies* 1–10 at 1–2.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

with any other companies, is to maximise profits, also sets certain limits on the role of the private sector.[20]

On the other hand, cyberspace technological innovations typically come from the private sector, and purely domestic and public-centred responses will fail to address emerging cyberthreats in an effective and timely manner.[21] Corporations operate critical infrastructure (e.g. servers, security protocols, and network access points) and possess relevant expertise to evaluate threat levels and propose tools to defend against cyberthreats[22] and are better suited to constantly update cybersecurity standards and best practices. This underscores the need for incorporating these standards and practices into the norms of cybersecurity governance. Based on these considerations, Chapter 9 provides a comparative analysis of the existing domestic public–private partnership (PPP) mechanisms on cybersecurity, including the National Institute of Standards and Technology (NIST) cybersecurity framework,[23] and addresses the challenge of optimising private and public co-operation to tackle cybersecurity threats globally. Chapter 10 further discusses the role of the private sector and examines its limits in cybersecurity governance.

With the aims described above, this book focuses on cybersecurity governance as an element of 'internet governance'.[24] In other words, it examines cybersecurity governance *in the Internet* – the most important

[20] See Section 10.7.

[21] Raquel Vázquez Llorente, 'A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity' (2018) *LSE Ideas, Strategic Update* 1–13; Scott J. Shackelford, Scott Russell, and Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* 1–50; Shin-Yi Peng, 'Private Cybersecurity Standards: Cyberspace Governance, Multistakeholderism, and the (Ir)Relevance of the TBT Regime' (2018) 51 (2) *Cornell International Law Journal* 445–470.

[22] Annegret Benedek, 'Due Diligence in Cyberspace, Guidelines for International and European Cyber Policy and Cybersecurity Policy' (2016) *SWP Research Paper* 1–33 at 16. It is observed that 'Many attacks succeed because of a failure to observe basic cybersecurity measures, like patching . . . or using multi-factor authentication' (Lostri et al., 'A Shared Responsibility', 3).

[23] For the NIST cybersecurity framework, see generally www.nist.gov/cyberframework (accessed 30 September 2022).

[24] 'Internet governance' also includes the issues of internet names and addresses, critical internet resources, and intellectual property rights. UN, 'WGIG Report', para. 12. DeNardis and Raymond identify the following six areas of internet governance: (a) control of 'critical internet resources', (b) setting internet standards, (c) access and interconnection co-ordination, (d) cybersecurity governance, (e) the policy role of information intermediaries, and (f) architecture-based intellectual property rights

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

information technology infrastructure in cyberspace.[25] Rather than trying to comprehensively cover all areas of cybersecurity regulation, this book seeks to draw lessons from various domestic, international, public, and private approaches to create a more agile regulatory framework for cybersecurity.

The book adopts a narrow definition of cybersecurity, from the Oxford English Dictionary – '[t]he state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this' – an interpretation that excludes unintentional computer and human errors. Therefore, in the understanding of this book, cybersecurity governance involves the development of a set of principles, norms, rules, and processes concerning the protection of the Internet against unauthorised use or attempted such use.

1.3 Overview of the Chapters

The book begins with the analysis of international relations frameworks for cybersecurity and discusses market-oriented and state-oriented models of internet regulation. Chapter 2, authored by Kiichi Fujiwara and Paul Nadeau, offers an analysis of the challenges for governments and the private sector in cybersecurity governance from a systemic perspective. It first identifies the challenges that the liberal international order, characterised by political liberalism, economic openness, and international co-operation, has faced in the area of cybersecurity governance. It also observes that there have so far been no successful global efforts to harmonise rules or create a unified regime. This chapter then

enforcement (DeNardis and Raymond, 'Thinking Clearly about Multistakeholder Internet Governance', 3).

[25] Kuehl defines cyberspace as 'a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'. Daniel T. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2011), 24–42 at 28 (italics in the original). Cyberspace consists of social (persona), logical, and physical (infrastructural) layers. Erick D. McCroskey and Charles A. Mock, 'Operational Graphics for Cyberspace' (2017) 85(2) *Joint Force Quarterly* 42–49 at 44. See also Nicholas Tsagourias, 'The Legal Status of Cyberspace', in Nicholas Tsagourias and Russell Buchan (eds.), *Research Handbook on International Law and Cyberspace*, 2nd ed. (Cheltenham: Edward Elgar Publishing, 2021), 13–29 at 15; Nezir Akyeşilmen, 'Cyber Good Governance: A New Challenge in International Power Politics?' (2018) 3(5&6) *Cyberpolitik Journal* 2–21 at 3.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

emphasises how the private sector's essential role as innovators possessing technological expertise is unique to cybergovernance and explains how the interplay of different actors, both public and private, has practical meaning for states and actors.

Wakako Ito offers, in Chapter 3, a detailed account of Chinese cybersecurity policy as an example of a state-oriented model of internet governance. After describing China's early attitudes towards cyberspace, it analyses in detail its cybersecurity policy under the Xi Jinping administration, and how its concept of 'cyber sovereignty' differs from Western countries' approaches to cyberspace. It also examines China's efforts to export the Chinese model of cyber laws and regulations based on the concept of cyber sovereignty to non-liberal countries. It also analyses how the country is actively involved in the formation of international rules for cybersecurity in order to spread this concept.

Summer Walker and Ian Tennant examine interstate corporation on combating cybercrime and its limitations in Chapter 4. The chapter situates the current negotiations of a new legal instrument to counter cybercrime within the UN's historical framework of efforts to enhance co-operation against general organised crime and cybercrime. In particular, it analyses the main issues that have held back progress on enhancing co-operation. It then proceeds to examine the current negotiation process and the prospects for effective co-operation once the negotiations come to an end, highlighting the potentially impactful legal implications of the work of the UN ad hoc committee on cybercrime.

Chapter 5, authored by Yarik Kryvoi, examines the distinction between public and private cyberattacks and responses to them in domestic law (e.g. application of criminal law) and international law (e.g. self-defence and countermeasures). After describing the different purposes, nature, and effects of cyberattacks committed by public and private actors, it argues that the determination of whether a particular cyberattack is of a public or private nature should define how states respond to cybersecurity risks. It then argues that the existing domestic and international law frameworks regulating cyberattacks suffer from serious limitations, and proposes a holistic approach for responding to cyberattacks, taking into account the difference between public and private cyberattacks.

In Chapter 6, Jens Hillebrand Pohl explores the question of how different domestic and international law approaches to regulating the international transfer of personal data deal with cybersecurity threats. It examines the 2016 EU General Data Protection Regulation, the 2021 UK

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

National Security and Investment Act, and the 2018 United States–Mexico–Canada Agreement as representing distinct approaches for regulating international data transfers, namely data protection legislation, investment-screening legislation, and digital trade agreements. The analysis demonstrates that a lack of uniformity in terms of what constitutes an adequate level and design of data protection mechanisms has left the issue of how to distinguish between acceptable and non-acceptable data-transfer restrictions largely unresolved.

Chapter 7, authored by Elizabeth Whitsitt, analyses how trade agreements balance liberalisation of digital trade with cybersecurity concerns. The chapter identifies the strengths, weaknesses, and ambiguities facing digital trade regulation in these agreements. As a way to address the tension between international trade law and cybersecurity, it examines security exception clauses in different trade agreements. It also analyses the efforts found in recent regional trade agreements to direct state parties to have regard to international standards concerning cybersecurity issues. It concludes that harmonisation of such standards would suggest the possibility of a greater coherence in the cybersecurity governance.

In Chapter 8, Tomoko Ishikawa discusses cybersecurity from the perspective of human rights protection. It first identifies adopting border measures as one approach to fulfilling a state's duty to protect its citizens against human rights violations caused by cybercrimes. It then examines the tension between these FDI restrictive border measures and states' investment protection and promotion obligations under IIAs. The analysis demonstrates a limitation in the current international law framework in which invoking the concept of national security remains the only means for states to address cyberthreats, which involves the risk of an accelerating shift to protectionism.

Aleks Kalisz examines, in Chapter 9, cybersecurity public–private partnerships (PPPs). Chapter 9 argues that PPPs bring together the lawmaking powers of the states with the know-how of the private sector, that both are necessary to effectively deal with cybersecurity threats, and that the benefits of PPPs outweigh their limitations. It then empirically analyses the laws and regulations surrounding cybersecurity PPPs in eighteen different domestic jurisdictions to find a common denominator that could be transposed into international cybersecurity PPPs. Finally, it discusses the modalities which international cybersecurity PPPs could take and proposes a new international treaty incorporating PPPs, under which states undertake to establish domestic mechanisms for collaborating with the private sector in cybersecurity.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press

Based on the findings and analyses presented, Chapter 10 gives an overview of possible approaches to cybersecurity governance. Considering the existing limits to global cybersecurity co-operation, it proposes to use regional co-operation as a starting point. It analyses existing regional cybersecurity treaties to highlight the differences in these treaties that reflect the divide between the state-oriented and market-oriented models of internet governance, and to find possible areas of convergence that may pave the way towards global co-operation. It also discusses the role and limitations of the private sector, including IT industries, technical experts, and civil societies, in cybersecurity governance.

https://doi.org/10.1017/9781009374576.001 Published online by Cambridge University Press