Navigating Cyberspace: An International Legal Analysis from Regional and Domestic Perspectives

Thanapat Chatinakrob *
Faculty of Law, Thammasat University, Thailand
ORCID 0000-0003-1680-6247

DOI: 10.54103/milanoup.215.c445

Abstract

Information and communication technologies (ICTs) have become an integral part of modern societies, and their misuse, termed ICT threats, poses a escalating risks to international security and stability. These threats, whether arising from state or non-state actors, can undermine societal progress, economic growth, and human safety. Cyber-attacks targeting critical systems such as energy grids or financial institutions highlight the insufficiencies of current international laws in addressing these challenges. This paper examines legal instruments and policy frameworks that aim to address ICT threats, including those of the European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN). However, the enforcement of such regional regulations, policies, and recommendations is yet to be adequately enforced. From a domestic perspective, this paper has explored examples of legal instruments and policy frameworks from various countries, such as the UK, Germany, France, Finland, and Singapore. These examples demonstrate how different countries address ICT threats in their way and how they regulate cyber activities to ensure the security and stability of their respective digital domains. This paper underscores the pressing need for robust legal instruments and policy frameworks that can effectively address ICT threats and

* This is an excerpt from the full research report titled 'the application of international law to cyberspace: the dilemna of state soverignty violation, extraterritorial effects and cyberspace sovereignty', which is funded by the Research Promotion Committee of the Faculty of Law, Thammasat University. Another part of this full research, different from the current part, was published in Chinese Journal of International Law, Volume 23, Issue 1, March 2024, Pages 25-72. Any errors are the author's own.

safeguard state sovereignty in cyberspace. The review of regional and domestic legal instruments and policy frameworks provides a starting point for identifying the most effective strategies to counteract ICT threats and ensure digital security and stability for all.

Keywords

Cyberspace; International Law; Regional and Domestic Laws and Policy Framework; State Sovereignty Violation; Extraterritorial Effects; Cyberspace Sovereignty.

1. Introduction

The rapid evolution of information and communication technologies (ICT) has been significantly altered global interactions, presenting unparalleled opportunities and pressing challenges. In recent years, ICTs have become indispensable tools for daily operations across industries and societies. Events like the COVID-19 pandemic and ongoing geopolitical conflicts, including the Russia-Ukraine war, have emphasised their critical role. However, these developments also reveal vulnerabilities, as ICT threats have emerged as significant issues for global security.

ICT threats involve malicious actions by State and non-State actors, posing serious risks across various sectors.[1] These threats can be categorised into three primary groups. The first consists of cybercrimes targeting critical infrastructure,[2] disrupting public services[3] and undermining economic stability.[4] The second includes covert state-sponsored campaigns designed to destabilise systems, jeopardising international peace and causing harm to individuals.[5] Lastly, the third group involves terrorist activities that exploit ICTs to conduct attacks, recruit members, and incite violence, thereby threatening global peace and stability. [6]

Currently, there is no comprehensive international legislation specifically designed to address ICT-related risks, particularly those associated with state-sponsored cyber threats. Instead, existing international legal frameworks, such as Article 2(4) of the UN Charter, principles of sovereignty and non-intervention, and international human rights law, are applied to regulate cyber

1 UN General Assembly, 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (14 July 2021) UN Doc A/76/135, paras 6–14 [hereinafter GGE 2021 Report].

2 ibid para 8.

3 ibid para 10.

4 ibid.

5 ibid para 9.

6 ibid para 13–14.

activities. However, these frameworks are not specifically tailored to address the complexities of cyberspace. For instance, the Group of Governmental Experts (GGEs) has made notable contributions in recommending voluntary norms for responsible state behaviour in cyberspace, yet these recommendations remain non-binding and lack enforceability.[7]

Regional efforts have provided some legal instruments to address cyber-related issues. The Budapest Convention on Cybercrime, for instance, facilitates collaboration among signatory states to combat cybercrime by harmonising domestic laws and improving investigative measures.[8] In contrast, the African Union Convention on Cyber Security and Personal Data Protection has yet to come into force, though its aim is to establish a robust cybersecurity framework for Africa by regulating electronic transactions and protecting personal data.[9]

On a broader scale, international organisations have recognised the pressing need for governance in cyberspace. The United Nations Resolution 73/266 advocates for peaceful ICT use, conflict prevention arising from ICT misuse, and education about technological advancements.[10] Similarly, the European Union (EU) has developed a Cybersecurity Strategy to enhance cooperation among Member States,[11] while the ASEAN Cybersecurity Cooperation Strategy aims to bolster regional collaboration.[12] However, such initiatives often lack legal enforceability, limiting their effectiveness.

Despite these efforts, ICT threats remain pervasive, exposing gaps in international legal frameworks and state-level responses. These challenges highlight the need to reexamine foundational principles of international law, particularly

7 ibid paras 1–98.

8 Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS 185 [hereinafter Budapest Convention].

9 African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) [hereinafter Malabo Convention].

10 UN General Assembly, 'Resolution adopted by the General Assembly on 22 December 2018: Advancing responsible State behaviour in cyberspace in the context of international security' (2 January 2019) UN Doc A/RES/73/266 [hereinafter GGE 2019 Report].

11 European Union, 'Cyberspace: Strengthening cooperation in promoting security and stability' (European Union External Action, 17 May 2021) <https://www.eeas.europa.eu/eeas/cyberspace-strengthening-cooperation-promoting-security-and-stability_en> accessed 2 March 2023; European Commission, 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' (European Union Press Release, 16 December 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> accessed 2 March 2023.

12 ASEAN Secretariat, 'Joint Media Statement' (ASEAN, 28 January 2021) The 2nd ASEAN Digital Ministers' Meeting and Related Meetings <https://asean.org/wp-content/uploads/2022/01/2nd-ADGMIN-Joint-Media-Statement.pdf> accessed 2 March 2023; ASEAN Secretariat, 'ASEAN Cybersecurity Cooperation Strategy (2021–2025)' (ASEAN) <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf> accessed 2 March 2023.

state sovereignty. The issues arising from ICT threats can be categorised into three main areas.

First, ICT threats pose direct challenges to state sovereignty by targeting critical infrastructure. Even when such threats originate outside a state's territory, states may be held accountable for failing to mitigate or counteract them.[13] The GGEs report emphasises the need for states to prevent the misuse of their territories for illicit ICT activities[14] and to assist other states in responding to cyber incidents.[15]

Second, the enforcement of cyberspace regulations often encounters jurisdictional complexities. The transnational nature of ICT activities necessitates the development of harmonised rules that are enforceable across borders. However, such regulations may inadvertently infringe upon the sovereignty of other states, underscoring the need for carefully crafted legal instruments that respect international norms. Third, the concept of cyberspace sovereignty has gained prominence as states assert control over their digital domains.[16] While traditional notions of sovereignty pertain to territorial and governmental authority, cyberspace sovereignty extends these principles to the digital realm. This evolving concept warrants further exploration, especially given the increasing frequency of cyber incidents, such as the 2007 Estonia cyberattack[17] and the cyber dimensions of the 2022 Russia-Ukraine conflict.[18]

2. Legal considerations in cyberspace

In recent years, the growing use and reliance on cyberspace have raised several legal issues under international law. The infringement of State sovereignty, extraterritorial impacts, and cyberspace sovereignty are among the major concerns. These challenges have led to questions about the application of conventional international law principles to cyberspace, as well as the need for novel legal frameworks to regulate cyberspace activities.

The infringement of State sovereignty in cyberspace poses a significant threat to fundamental international law principles. Since time immemorial, States have enjoyed exclusive control over their territories and actions. However, cyberspace

13 GGE 2021 Report (n 1).

14 ibid, norm 13 (c).

15 ibid, norm 13 (h).

16 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) (1945) 1 UNTS XVI, art 2(1) [hereinafter UN Charter].

17 Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia' (*The New York Times*, 29 May 2007) <https://www.nytimes.com/2007/05/29/technology/29estonia.html> accessed 4 March 2023.

18 Center for Preventive Action, 'Conflict in Ukraine' (*Global Conflict Tracker,* updated 12 May 2022) <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine> accessed 4 March 2023.

presents a novel challenge to this notion. As cyberspace activities often transcend national boundaries, it becomes difficult to establish jurisdiction and applicable laws. This increases the likelihood of State sovereignty violations where the actions of one state may encroach on the sovereignty of another.

The impact of activities outside a state's territory is a legal issue in cyberspace. The notion of territorial sovereignty limits State authority to actions that take place within its borders. In contrast, cyberspace activities outside of a State's borders can have significant consequences inside the State. An instance is the destruction of critical infrastructure by a cyberattack from another State, leading to a violation of the targeted State's sovereignty. The extraterritorial effect of online operations has raised concerns regarding the application of established international law principles in cyberspace.

As ICT threats proliferate, they bring to the fore significant legal challenges under international law. The transboundary nature of cyberspace activities necessitates innovative approaches to address state sovereignty infringements, extraterritorial impacts, and the emerging concept of cyberspace sovereignty. The following sections analyse these critical issues in detail.

2.1 State sovereignty violation

Under international law, the principle of State sovereignty mandates that states exercise control within their territories without external interference.[19] Although 'territory' refers to both legal and political notions as well as physical or geographic areas,[20] the term can be extended to include regions that lack physical or geographical boundaries but possess legal components such as application, prescription, enforcement, and adjudication that may impact a State's sovereignty.[21] However, cyberspace presents unique challenges to this principle.

---

19 Jens Bartelson, *A Genealogy of Sovereignty* (CUP 1993) 26; Montevideo Convention on the Rights and Duties of States (concluded 26 December 1933, entered into force 26 December 1934) 165 LNTS 19; Daniel Bethlehem, 'The end of geography: the changing nature of the international system and the challenge to international law' (2014) 25 European Journal of International Law 9, 13; Nicolas G Onuf, 'Sovereignty: Outline of a conceptual history' (1991) 16 Alternatives: Global, Local, Political 425, 437.

20 Nicholas Tsagourias, 'The Legal Status of Cyberspace: Sovereignty Redux?' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2021) 13; Thomas Forsberg, 'Beyond sovereignty, within territoriality: Mapping the space of late-modern (geo) politics' (1996) 31 Cooperation and Conflict 355, 355; *Island of Palmas (United States of America v Netherlands)* [1928] RIAA 839; Richard T Ford, 'A history of jurisdiction' (1999) 97 Michigan Law Review 843, 853–854; John G Ruggie, 'Territoriality and beyond: Problematising modernity in international relations' (1993) 47 International Organisation 139.

21 Tsagourias, ibid; Frederick A Mann, 'The doctrine of international jurisdiction revisited after twenty years' in *Recueil Des Cours* (Martinus Nijhoff 1984); Peter J Taylor, 'The state as container: Territoriality in the modern world-system' (1994) 18 Progress in Human Geography 151, 151.

Cyber-attacks and ICT enabled activities often transcend physical borders, resulting in violations of sovereignty through acts such as data breaches, critical infrastructure sabotage, or disinformation campaigns. Addressing these violations requires clarifying the scope of sovereignty in the digital realm and establishing norms for state behavior in cyberspace.

With the current international regulations concerning cyberspace, particularly the illegitimate usage of ICT, it is observed that such actions may infringe upon other States' sovereignty. A crucial challenge in applying international law to cyberspace is determining whether it can be enforced within a State's territory.

The study conducted by GGE acknowledged the relevance of international law, specifically the UN Charter, in regulating State sovereignty principles in cyberspace. The Group emphasised that the conduct of ICT-related activities by States and their jurisdiction over ICT infrastructure within their territory should be subject to State sovereignty and related international norms and principles. The current obligations under international law are also applicable to States' ICT-related activities.[22]

This illustrates that ICT-related activities, despite not being carried out on the territory of another State, can violate the sovereignty of another State. States can exercise their sovereignty by exerting authority over individuals in their territory and over cyber infrastructure located in their territory, including their citizens residing within their sovereign area.[23] This can lead to passive nationality jurisdiction, which may result in activities that infringe on the sovereignty of other States.

The use of sovereignty in cyberspace should have limited legal implications and scope.[24] States have sovereignty over their information and communications technology infrastructure within their territory, but this use of sovereignty must not infringe on the sovereignty of another State. The use of ICT must not jeopardise other States' cyber infrastructure, especially cyberattacks on critical infrastructure that threatens the sovereignty of other States.[25] Such actions may

22 GGE 2021 Report (n 1) para 71 (b).

23 C-131/12, Google Spain SL v Agencia Española de Protección de Datos [2014] ECLI:EU:C:2014:317, paras 32–41; *Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v Belgium)* (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal) [2002] ICJ Rep 3, para 47.

24 US Department of Defense, 'DOD General Counsel Remarks at US Cyber Command Legal Conference' (Speech, 2 March 2020) <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> accessed 8 March 2023; Brian Egan, 'International law and stability in cyberspace' (2017) 35 Berkeley Journal of International Law 169, 169.

25 Nicholas Tsagourias (n 20) 22; Finland, 'Finland's national positions: international law and cyberspace' <https://um.fi/documents/35732/0/cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859> accessed 10 March 2023, 2–3; *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion)

support another State's sovereignty over its territory. Thus, any unauthorised or unjustified operation that interferes with a State's sovereign rights violates the principle of sovereignty, regardless of the degree of interference or damage, physical or non-physical effects, or whether the operation targets governmental services and infrastructure.[26]

2.2 Extraterritorial effects

The extraterritorial impact of cyber activities is another pressing concern. Actions originating in one State can cause significant harm in another, raising questions about jurisdiction and accountability.[27] Existing international legal frameworks often struggle to accommodate the dynamic and borderless nature of cyberspace. This section explores how extraterritoriality can be addressed through enhanced international cooperation, harmonised legal standards, and mechanisms for cross-border enforcement.

The issue of jurisdiction is crucial in cyberspace. The territorial boundaries of a State usually establish its jurisdiction in the physical world. However, with data and communications traversing multiple countries, determining the location of a particular action or participant in cyberspace can be challenging. Consequently, some argue that traditional jurisdictional concepts are inadequate in the digital environment and new approaches are necessary to ensure the effectiveness of international law in governing cyberspace.[28] The advancement of technology in various types of cyber activity, such as internet-based defamation, is one of the main reasons for the spread of significant extraterritoriality.[29] Many cyber acts are difficult to geographically pinpoint, which means that States may enact internally applicable laws only after considering other factors. These factors may include the effect on persons of their nationality, which may lead to the unlimited right of jurisdiction,[30] and the consequences in the

---

[1996] ICJ Rep 226, 393–394 (Dissenting Opinion of Judge Shahabuddeen); NCSC, 'UK and allies expose Russian attacks on coronavirus vaccine development' (*NCSC*, 16 July 2020) <https://www.ncsc.gov.uk> accessed 10 March 2023; Russell Buchan, *Cyber Espionage and International Law* (Hart 2018) 48–69.

26 Finland, ibid 2; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* [1986] ICJ Rep 14, paras 205 and 247.

27 Hannah L Buxbaum, 'The Practice(s) of Extraterritoriality' in Hannah L Buxbaum and Thibaut Fleury Graff (eds), *Extraterritoriality* (Hague Academy of International Law, Brill 2022) 3.

28 Michael N Schmitt, 'International Law in Cyberspace' (2013) 7 (1) Journal of National Security Law & Policy 1, 1–51.

29 Victor Stoica, 'Testing the Continued Viability of Traditional Jurisdictional Norms: The Challenges of Cybersecurity' in Hannah L Buxbaum and Thibaut Fleury Graff (eds), *Extraterritoriality* (Hague Academy of International Law, Brill 2022) 525–570.

30 Vaughan Lowe, *International Law* (OUP 2007) 174; Bruno Simma and Andreas Th Müller, 'Exercise and Limits of Jurisdiction' in James Crawford and Martti Koskenniemi (eds),

form of serious crimes under international law under universal jurisdiction.[31] Additionally, the impact may be prioritised, and domestic legislation within the country may have cross-border effects.

Another aspect of the extraterritorial effects of international law in cyberspace relates to State responsibility. States are obligated under international law to avoid infringing on the rights of other States and to compensate victims for their actions. Nonetheless, in the cyberspace context, identifying particular actions carried out by a single State can be difficult because they may be performed by non-State actors, necessitate the use of intermediaries, or entail routing through various States. Thus, alternative methods of establishing state responsibility in cyberspace, such as the notion of state responsibility for cyber operations, have been suggested.

Furthermore, there are worries about the application of domestic laws outside a state's territory in cyberspace. Usually, domestic laws are limited to the jurisdiction of a single State, but with data and communications traversing multiple countries in cyberspace, it can be challenging to determine which laws should govern specific conduct. As a result, there have been calls for increased international cooperation to ensure that the extraterritorial application of domestic laws does not result in conflicts or breaches of international law.[32]

The issue of extraterritoriality of international law in cyberspace is closely related to the topic of human rights in the digital realm. While the internet and other digital technologies have increased people's ability to communicate and access information, they have also raised concerns about privacy, freedom of expression, and other basic rights. To protect individuals from rights violations in this digital world, it has been suggested that international human rights laws should be extended to cyberspace.

The GGE report fails to address the issue of extraterritoriality, which can have severe consequences in the context of ICT-related activities. For instance, actively hacking a computer system located on a server beyond a State's territorial limits could harm a computer system in another country.[33] Furthermore, States may create domestic legislation to address cyber concerns within their borders, imposing obligations on other States. This may have an effect even if authorities stationed in other States do not access the territory of such enforcing

---

Cambridge Companion to International Law (CUP 2012) 134, 141–142; Michael Akehurst, 'Jurisdiction in International Law' (1973) 46 British Yearbook of International Law 145, 156.

31 Stephen Macedo et al, *Princeton Principles on Universal Jurisdiction* (Program in Law and Public Affairs 2001) 24; *Arrest Warrant* (n 23), 10–11.

32 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Border less World* (OUP 2006) 154–158 and 165–167.

33 Mireille Hildebrandt, 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace' (2013) 63 (2) The University of Toronto Law Journal 196, 197.

States. Consequently, the State may be subject to domestic law restrictions applicable in the territory of other States.

In summary, the extraterritorial effects of international law in cyberspace are complex and expanding, encompassing significant challenges related to jurisdiction, state responsibility, extraterritorial application, and human rights. Although scholars and experts are debating the best approach to address these issues, it is clear that novel methods are necessary to effectively regulate cyberspace under international law. Many international or regional laws, policies, or suggestions still require full implementation.

2.3 Cyberspace sovereignty

The discovery that cyberspace activities can affect both sovereignty and extraterritoriality across borders has led to suggestions for separating cyberspace from domestic law. Chinese President Xi Jinping has promoted the concept of cyber sovereignty, which defines a State's territory as the area in which it can exercise sovereignty.[34] A State's network refers to the ICT infrastructure composed of ICT systems built within its territory. This raises the issue of the extent to which States should be allowed to exert sovereignty over their ICT infrastructure.[35]

The concept of cyberspace sovereignty has gained traction as States seek to assert control over digital activities within their territories. This encompasses regulating data flows, securing critical infrastructure, and protecting citizens' digital rights. However, achieving a balance between State control and the inherently global nature of cyberspace remains a challenge.[36]

Defining cyberspace as a territory brings about cyberspace rights and duties. It grants cyberspace sovereignty, which entails basic rights to the territory. These rights comprise cyberspace independence, cyberspace equality, cyberspace self-defence, and cyberspace jurisdiction.[37]

The distinct nature of cyberspace poses a significant challenge in determining the issue of cyberspace sovereignty. Being a virtual realm with no tangible borders and constantly evolving, it's hard to define or set limits to it, making it

34 Ministry of Foreign Affairs of the People's Republic of China, 'Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference' (Wuzhen, 16 December 2015) <https://www.fmprc.gov.cn> accessed 14 March 2023; Michael Kolton, 'Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence' (2017) 2 (1) The Cyber Defense Review 119, 119; Rogier Creemers, 'China's Conception of Cyber Sovereignty: Rhetoric and Realization' in Dennis Broeders and Bibi van den Berg, *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020) 107–142; Binxing Fang, *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* (Springer 2018).

35 Binxing Fang, ibid 83.

36 ibid.

37 ibid 84.

challenging for authorities to regulate the internet within their territories. Also, as the Internet is a global network accessed by individuals and entities worldwide, no single state can claim complete authority over the entire network.

The absence of established international legal rules and principles that apply to cyberspace presents a further challenge to resolving issues of cyberspace sovereignty. Although several international agreements and conventions exist on internet-related issues, such as the World Summit on the Information Society (WSIS)[38] and the GGE 2021 report,[39] there is no consensus on how these agreements should be implemented in cyberspace.

It can be argued that ICT threats can have effects that span from State sovereignty to cyberspace sovereignty. The idea of sovereignty in international law, particularly concerning State sovereignty, is important as it deals with the concept of sovereignty in terms of possessing territories, populations, and regimes within one's borders.

3. Existence of regional and domestic legal instruments and policy framework in cyberspace

The rapid emergence and ever-evolving nature of cyberspace have resulted in significant legal and policy challenges, given the increasing reliance of states and societies on digital technology. To address the complexities and dynamism of this environment, various international, regional, and domestic legal instruments and policy frameworks have been established. This article examines the presence of different tools and frameworks that can be categorised as either regional or domestic.

A number of regional organisations have established cyberspace-related legal and policy instruments. The European Union,[40] for example, has produced a number of directives and rules aimed at preserving individuals' privacy and security in the EU, including the General Data Protection Regulation (GDPR)[41] and the Network and Information Systems Directive (NIS2 Directive).[42] The

38 International Telecommunication Union (ITU), *WSIS+10 Statement on Implementation of WSIS Outcomes and the WSIS+10 Vision for WSIS Beyond 2015* (ITU 2014) 9–48.

39 GGE 2021 Report (n 1).

40 European Union (n 11).

41 Regulation (EU) 2016/679 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 and on the Free Movement of such Data, and repealing Directive 95/46/EC [hereinafter GDPR].

42 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333.

Association of Southeast Asian States (ASEAN)[43] has also produced the ASEAN Regional Forum (ARF) Work Plan on Security of and in the Use of Information and Communication Technologies,[44] with the goal of promoting conversation and cooperation on cyberspace-related problems.

At the domestic level, States have developed a range of legal and policy frameworks to address the challenges posed by cyberspace. These frameworks often cover a range of issues, including the protection of critical infrastructure, the prevention and investigation of cybercrime, and the regulation of the use of digital technologies by individuals and organisations. For example, the UK[45] has enacted a number of laws and regulations, including the Computer Misuse Act,[46] which criminalises unauthorised access to computer systems, and the Data Protection Act,[47] which regulates the processing of personal data. The UK has also established a National Cyber Security Centre,[48] which serves as the primary authority for cybersecurity issues in the country. The centre is responsible for providing guidance to organisations and individuals on how to protect their networks, and for coordinating the response to cyber incidents.

3.1 Regional laws and policy frameworks in cyberspace

In response to the growing importance of cyberspace in everyday life, regional legal and policy frameworks have arisen. These frameworks seek to improve cyberspace security, stability, and collaboration by addressing the specific issues that the digital realm presents. In this environment, some regional organisations have developed legal tools and policy frameworks to govern cyberspace activity in their particular territories. The European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN) have all built regional legal and policy frameworks.

---

43 ASEAN Secretariat (n 12); ASEAN Secretariat, 'ASEAN Leaders' Statement on Cybersecurity Cooperation' (ASEAN, 27 April 2018) The 32*nd* ASEAN Summit <https://asean.org/asean-leaders-statement-on-cybersecurity-cooperation/> accessed 14 March 2023.

44 ASEAN Secretariat, 'ASEAN Regional Forum Work Plan on Security of and in the Use of Information and Communications Technologies (ICTs)' (ASEAN, 7 May 2015) <https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf> accessed 14 March 2023.

45 Foreign, Commonwealth & Development Office, 'Application of international law to states' conduct in cyberspace: UK statement' (Policy Paper, 3 June 2021) <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement> accessed 15 March 2023.

46 Computer Misuse Act 1990, UK Public General Act 1990, c.18.

47 Data Protection Act 2018, UK Public General Act 2018, c.12.

48 National Cyber Security Centre, 'The National Cyber Security Centre' (NCSC) <www.ncsc.gov.uk/> accessed 16 March 2023.

The European Union has led regional attempts to control cyberspace activities. The EU has established a number of legal instruments, including the General Data Protection Regulation (GDPR),[49] the Network and Information Security Directive (NIS2 Directive),[50] and the Cybersecurity Act,[51] which establish a comprehensive legal framework for cybersecurity and data protection in the region. The GDPR, for example, establishes a uniform set of standards for the handling of personal data, whilst the NIS Directive strives to improve the cybersecurity of network and information systems throughout the EU. In contrast, the Cybersecurity Act establishes a European cybersecurity certification system to encourage a consistent level of cybersecurity throughout the EU.

Similarly, the OAS has created legal mechanisms to govern cyberspace activities in its Member States. In 2007, the OAS held a meeting of a group of governmental experts on cybercrime to strengthen and consolidate cooperation in the prevention and fight against cybercrime, leading to several workshops on cybercrime and the Inter-American Cooperation Portal on Cyber-Crime.[52] The OAS provided the Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA) to conclude existing cyber-crime legislation of the OAS Member States.[53] The OAS has also implemented the principles from the Council of Europe's Convention on Cyber-Crime.[54] Member States are required by the convention to criminalise specific cyber acts, such as illegal access to computer systems, electronic communication interception, and computer-related fraud.[55] Furthermore, the OAS has established the Inter-American Committee against Terrorism (CICTE) Cybersecurity Program,[56] which offers Member States technical help and capacity-building on cybersecurity-related issues.

The OSCE has also developed a framework for collaboration among its Member States in order to improve cyber security and stability. In 2012, the OSCE endorsed confidence-building measures (CBMs) in cyberspace, which outline voluntary actions to improve transparency and minimise the danger of

49 GDPR (n 41).

50 NIS 2 Directive (n 42).

51 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) [2019] OJ L 151.

52 OAS, 'The Inter-American Cooperation Portal on Cyber-Crime' (Cybercrime data AS) <www.cybercrimelaw.net/OAS.html> accessed 16 March 2023.

53 Department of Legal Cooperation, OAS, 'OAS Member State Legislation' (OAS) <http://www.oas.org/juridico/english/cyber_legis.htm> accessed 16 March 2023.

54 Budapest Convention (n 8).

55 Department of Legal Cooperation, OAS (n 53).

56 US Department of State, 'Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)' (US Department of State) <https://2001-2009.state.gov/s/ct/intl/io/cicte/index.htm> accessed 24 March 2023.

conflict in cyberspace.[57] The OSCE later adopted new OSCE CBMs in 2016.[58] The CBMs contain procedures for information exchange, cyber incident notification, and confidence-building measures such as the establishment of hotlines and collaborative cybersecurity exercises among Member States.

Finally, ASEAN has recognised the importance of regional collaboration in cyberspace. In 2018, ASEAN ratified the ASEAN Framework on Digital Data Governance,[59] which establishes a set of regional data governance standards. The agreement includes measures for personal data protection, cross-border data flows, and Member-State cybersecurity cooperation. Moreover, ASEAN has created the ASEAN Ministerial Conference on Cybersecurity,[60] which serves as a forum for Member States to debate cybersecurity challenges and foster cooperation in this field.

3.1.1 European Union (EU)

The EU has put in place a number of policies and legislative frameworks aimed at boosting cybersecurity, protecting individuals' rights and liberties, and stimulating economic development and innovation in cyberspace.

The EU's Cybersecurity Strategy, which was released in 2013,[61] outlines a comprehensive strategy for addressing cybersecurity concerns. The strategy's

57 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection' (CCDCOE) <https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/> accessed 24 March 2023; OSCE Permanent Council, 'Decision No. 1039 Development of Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (26 April 2012) PC.DEC/1039.

58 OSCE Permanent Council, 'Decision No. 1202 OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.

59 ASEAN Secretariat, 'Framework on Digital Data Governance' (ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), 6 December 2018) <https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf> accessed 25 March 2023.

60 Government of Singapore, 'Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020' (CSR Singapore, 7 October 2020) <https://www.csa.gov.sg> accessed 25 March 2023; Nur Azha Putra, 'Is ASEAN Doing Enough to Address Cybersecurity Risks?' (*The Diplomat*, 6 March 2018) <https://thediplomat.com/2018/03/is-asean-doing-enough-to-address-cybersecurity-risks/> accessed 25 March 2023.

61 Jorida Vela, 'The Development of the EU Cyber Security Strategy and its Importance' (FINABEL European Army Interoperability Centre, 2 August 2021) <https://finabel.org/info-flash-the-development-of-the-eu-cyber-security-strategy-and-its-importance/> accessed 26 March 2023; Commission, High Representative of the Union, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee

major goal is to keep the EU's digital single market open, safe, and secure.[62] It identifies five strategic priorities: creating cyber resilience, promoting cybersecurity standards and certification, establishing a cybercrime and incident response network, expanding cyber defence capabilities, and boosting international collaboration.

The EU has also proposed numerous legal measures to achieve the cybersecurity plan, notably the Network and Information Security Directive (NIS2 Directive),[63] which went into force in 2018. The NIS2 Directive intends to provide a high degree of cybersecurity throughout the EU's vital infrastructure and important services, such as energy, transportation, banking, and health.[64] The NIS2 Directive requires member states to identify critical infrastructure operators and develop a national cybersecurity framework.[65] In addition, the Directive requires these operators to apply suitable security measures, disclose security events, and collaborate with relevant authorities.[66]

The EU also implemented the GDPR,[67] which came into force in 2018, to safeguard individuals' basic rights and freedoms in the handling of personal data. The GDPR provides standards for personal data collection, use, storage, and transfer, as well as imposing duties on enterprises that process such data. Individuals can also use the regulation to exercise their rights to access, modify, and delete their personal data.

Furthermore, the EU has established the European Union Agency for Cybersecurity (ENISA), which acts as the Union's cybersecurity competence centre. The primary duties of ENISA are to provide guidance and advice to Member States and EU institutions, to support the formulation and implementation of the EU's cybersecurity strategy, and to promote cooperation and information sharing among Member States.[68]

In summary, the EU has put in place a comprehensive legal and regulatory framework to address cybersecurity concerns, safeguard individuals' basic rights and freedoms, and foster economic development and creativity in cyberspace. The EU's Cybersecurity Strategy, NIS Directive, GDPR, and ENISA are all critical tools for achieving these goals.

---

of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (7 February 2013) JOIN/2013/01 final.

62 Joint Communication to the European Parliament, ibid.

63 NIS 2 Directive (n 42).

64 ibid.

65 ibid.

66 ibid.

67 GDPR (n 41).

68 ENISA, 'About ENISA – The European Union Agency for Cybersecurity' (ENISA) <https://www.enisa.europa.eu/about-enisa> accessed 26 March 2023; Cybersecurity Act (n 51).

3.1.2 Organization of American States (OAS)

The OAS is a global organisation with 35 member countries from North, Central, and South America, as well as the Caribbean.[69] The Organization of American States has acknowledged the necessity of tackling cyberspace concerns and has launched a variety of initiatives and regulations to do so.

To address cybersecurity challenges in the Americas, the OAS has launched a number of programs and regulations. The Inter-American Committee against Terrorism (CICTE), for example, has been attempting to encourage member governments to cooperate to prevent and combat cybercrime.[70] Furthermore, the OAS has established the Inter-American Committee on Telecommunications (CITEL) Cybersecurity Program, which aims to support the development of national cybersecurity policies and regulations, as well as collaboration and information-sharing among Member States.[71] The initiative also offers Member States technical help and cybersecurity training.

In addition to these initiatives and policies, the OAS has established the Cybersecurity Technical Assistance Missions, which provides technical assistance to Member States on a variety of cybersecurity issues, such as developing national cybersecurity strategies and implementing international cybersecurity standards.[72]

Notwithstanding these efforts, the OAS has considerable obstacles in tackling cybersecurity threats throughout the Americas. One significant difficulty is the lack of a coordinated and unified strategy for cybersecurity among Member States, which can stymie effective collaboration and information exchange.[73] Moreover, increased awareness and capacity-building among Member States are required, notably in creating and executing national cybersecurity plans and regulations.

In conclusion, the OAS has developed a variety of initiatives and policies to address cybersecurity challenges in the Americas, including the formation of the CICTE and the passage of multiple cybercrime resolutions. Yet, the OAS has substantial obstacles in addressing cybersecurity concerns in the region,

69 OAS, 'Who We Are' (OAS) <www.oas.org/en/about/who_we_are.asp> accessed 20 March 2023; Editors of Encyclopaedia Britannica, 'Organization of American States' (Britannica, Last Update 12 February 2023) <www.britannica.com/topic/Organization-of-American-States> accessed 27 March 2023.

70 US Department of State, 'Organization of American States/Inter-American Committee Against Terrorism (OAS/CICTE)' (US Department of State) <https://2001-2009.state.gov/s/ct/intl/io/cicte/index.htm> accessed 27 March 2023.

71 OAS, 'The Inter-American Telecommunication Commission' (OAS) <www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/citel> accessed 27 March 2023.

72 Cybil, Cybersecurity Technical Assistance Missions (Cybil) <https://cybilportal.org/projects/cybersecurity-technical-assistance-missions/> accessed 27 March 2023.

73 OAS, *NCS: Lessons Learned and Reflections from the Americas and Other Regions* (OAS) 12.

including the need for increased cooperation and capacity-building among member governments.

3.1.3 Organization for Security and Cooperation in Europe (OSCE)

The OSCE is a regional security organisation that has 57 Member States from North America, Europe, and Asia.[74] The organisation's goal is to improve regional security, stability, and collaboration by tackling a wide variety of security challenges, particularly those in cyberspace.[75]

The OSCE acknowledges the rising importance of cyberspace as an arena for international cooperation and has established a number of policy documents and initiatives to address emerging cyberspace concerns.[76] The OSCE's approach to cyberspace, like the EU's, is founded on the principle of a free, open, and secure cyberspace.[77]

The OSCE has accepted various cyberspace policy publications, notably the Tallinn Manual on International Law Applicable to Cyber Warfare, which was prepared in collaboration with NATO and several other organisations in 2013.[78] The guidebook presents a thorough examination of international law related to cyberspace, including armed conflict law, human rights law, and State responsibility law.[79] It is largely considered a reliable source of international law in cyberspace.

In addition to the Tallinn Manual, the OSCE has approved a number of other policy papers, notably the 2013 OSCE Confidence Building Measures (CBMs) to mitigate conflict risks associated with the use of information and communication technology.[80] CBMs involve frequent information exchanges,

74 OSCE, 'Participating States' (OSCE) <www.osce.org/participating-states> accessed 28 March 2023.

75 OSCE, 'Who we are' (OSCE) <www.osce.org/who-we-are> accessed 28 March 2023.

76 Alena Kupchyna, 'Confronting the Challenges of Working in Cyberspace' (OSCE, 4 October 2021) <https://www.osce.org/blog/confronting-the-challenges-of-working-in-cyberspace> accessed 28 March 2023.

77 ibid.

78 Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Operations* (CUP 2013).

79 ibid.

80 The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection' (CCDCOE) <https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/> accessed 28 March 2023; OSCE Permanent Council, 'Decision No. 1039 Development of Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (26 April 2012) PC.DEC/1039.

discussions, and visits among participating governments, as well as the development of emergency communication channels.[81]

The OSCE has also created a variety of capacity-building projects to help member governments improve their cybersecurity capabilities. For example, the International Cyber Security Capacity Building Program offers member governments training and technical help in incident response, cybersecurity strategy, and cybersecurity risk assessment.[82]

Overall, the OSCE's cyberspace legislation and policy framework is built on the idea of a free, open, and safe cyberspace. The group has created a comprehensive approach to cyberspace security that includes policy papers, confidence-building measures, and capacity-building activities. The OSCE's activities in this field contribute significantly to the establishment of international norms and standards for responsible state behaviour in cyberspace.

3.1.4 Association of Southeast Asian Nations (ASEAN)

After analysing the topic of international law in cyberspace, it leads to a smaller framework, namely the ASEAN Member States' framework. ASEAN is also a group of countries that profit from and are harmed by technological advancement. While not as visible as other regional countries, ASEAN has positioned itself to deal with dangers that may arise at any time. Consequently, this part will discuss ASEAN's broad legal and policy challenges, as well as notable cases from specific Member States. It will use three major countries as examples: Indonesia, Singapore, and Thailand. Indonesia and Singapore are ASEAN member nations that are specialists in the GGE and have long contributed to the research and development of the subject. While Thailand is not a member of any international bodies, it has some noteworthy policy initiatives that will be addressed in further depth later.

Through the principle of comprehensive security,[83] Article 1(8) of the ASEAN Charter mandates effective activities to address all types of threats, transnational crimes, and transboundary issues. This Article does not explicitly discuss catastrophes and actions performed in ASEAN cyberspace; rather, it covers all types of risks, including ICT threats.

In 1996, ASEAN, which had only seven Member States at the time, convened multiple meetings on internet possibilities and challenges.[84] A number of issues were discussed at the time to prepare citizens for digital collaborations

81 ibid.

82 ICT4Peace, 'International Cyber Security Capacity Building Program' (ICT4Peace, 27 August 2018) <https://ict4peace.org/wp-content/uploads/2018/09/Outline-Capacity-Building-20180827.pdf> accessed 28 March 2023.

83 ASEAN Charter, art 1 (8).

84 ASEAN Secretariat, *Joint Press Release of the ASEAN Forum on Internet, Singapore, 2-4 September 1996* (ASEAN Secretariat 1996).

such as the e-ASEAN framework agreement and information and communications technology (ICT) capacity building[85], responding to cybercrime issues[86], terrorist use of the internet[87], and disinformation and misinformation dissemination.[88]

ASEAN, on the other hand, has not implemented any actual rules or regulations. However, it has been decided by the issuing of policies that are applicable to all ASEAN Members, particularly the 2020 ASEAN ICT Masterplan[89], the 2025 ASEAN Connectivity Master Plan[90], and the ASEAN Smart Cities Network.[91] Furthermore, ASEAN has held a number of meetings on cyber issues at various levels, including the ASEAN Regional Forum, the ASEAN Defence Ministers' Meeting, the ASEAN Ministerial Meeting on Transnational Crime, the ASEAN Digital Ministers' Meeting, and the ASEAN Ministerial Conference on Cybersecurity.[92]

More diplomatic sensitivities surrounding espionage will be explored within the ASEAN framework, highlighting political intent, legal ambiguity, and a lack of competence.[93]

---

85 ASEAN Secretariat, 'e-ASEAN Framework Agreement' (ASEAN, 24 November 2000) <https://agreement.asean.org/media/download/20140119121135.pdf> accessed 28 March 2023; ASEAN Secretariat, 'Brunei Action Plan "Enhancing ICT Competitiveness: Capacity Building"' (ASEAN, 19 September 2006) <https://asean.org/brunei-action-plan-enhancing-ict-competitiveness-capacity-building/> accessed 28 March 2023.

86 ASEAN Secretariat, 'ASEAN Document Series on Transnational Crime: Terrorism and Violent Extremism; Drugs; Cybercrime; and Trafficking in Persons' (ASEAN Jakarta 2007) <https://asean.org/wp-content/uploads/2021/01/ASEAN-Document-Series-on-Transnational-Crime-FINAL-with-link2.pdf> accessed 28 March 2023.

87 ASEAN Secretariat, 'Chairman's Statement of the Thirteenth ASEAN Regional Forum Kuala Lumpur, 28 July 2006' (ASEAN, Kuala Lumpur, 28 July 2006) <https://asean.org/chairmans-statement-of-the-thirteenth-asean-regional-forum-kuala-lumpur-28-july-2006/> accessed 28 March 2023; ASEAN Secretariat, 'ASEAN Regional Forum (ARF) Statement on Preventing and Countering Terrorism and Violent Extremism Conductive to Terrorism (VECT)' (26*th* ASEAN Regional Forum, Bangkok, Thailand, 2 August 2019) <https://aseanregionalforum.asean.org/wp-content/uploads/2019/08/ARF-Statement-on-Counter-Terrorism-and-VECT_FINAL.pdf> accessed 28 March 2023.

88 See, for example, ASEAN Learning Center, Department of Local Administration, 'ASEAN Ministers Agree on Framework to Combat Fake News' (Department of Local Administration, 11 May 2018) <https://asean.dla.go.th/> accessed 28 March 2023.

89 ASEAN Secretariat, 'The ASEAN ICT Masterplan 2020' (ASEAN 2020) <https://asean.org/wp-content/uploads/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf> accessed 28 March 2023.

90 ASEAN Secretariat, 'Master Plan on ASEAN Connectivity 2025' (ASEAN 2016) <https://asean.org/wp-content/uploads/2021/08/8_compressed.pdf> accessed 28 March 2023.

91 ASEAN Smart Cities Network (ASCN), 'ASEAN Smart Cities Framework' (ASCN 2018) <https://asean.org/wp-content/uploads/2019/02/ASCN-ASEAN-Smart-Cities-Framework.pdf> accessed 28 March 2023.

92 Elina Noor, 'Positioning ASEAN in Cyberspace' (2020) 15 (2) Asia Policy 107, 109.

93 ibid 111.

To begin with, decisions on any cyber activity are frequently political in nature. It indicates that the discovered advanced persistent threats are merely a subset of Southeast Asia's overall threat landscape, and certain ASEAN Member States have been involved in comparable advanced persistent threat operations.[94] In this sense, ASEAN may have both regional and national interests to consider in building its framework. Political calculation frequently works against naming and shaming perpetrators.

On the second point, while the applicability of international law in cyberspace is widely agreed upon, the criteria and specifics remain unclear.[95] Therefore, further features must be determined by country or within the framework of the region. There is currently no clear rule for ASEAN on how to determine the limits.

Finally, if a cyber attack is an act that an ASEAN State's domestic law designates as a crime under its domestic law. This problem may not be explicitly expressed by all ASEAN Member States or may be addressed by differing responsibility scopes. As a result, the legal, technical, or judicial capability action should be specified.[96] These are still not expressed directly in the ASEAN framework.

3.2 Examples from some countries

Since the employment of cyberspace has grown in popularity in modern society, several States have enacted domestic rules and regulations to regulate the activities that occur within it. The Computer Misuse Act of 1990,[97] for example, criminalises unauthorised access to computer systems and associated offences in the United Kingdom. Similarly, Germany passed the Federal Office for Information Security Act,[98] which sets steps to safeguard the security and resilience of government information technology systems. France has enacted the Military Planning Law,[99] which improves cyber defences and enables

94 Jason Thomas, 'Cyber warfare in Vietnam' (*The ASEAN Post*, 4 October 2019) <https://theaseanpost.com/article/cyber-warfare-vietnam> accessed 28 March 2023.

95 GGE 2021 Report (n 1).

96 International Telecommunication Union (ITU), 'Global Cybersecurity Index 2020' (ITU Publications 2020) <www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> accessed 28 March 2023.

97 Computer Misuse Act (n 46).

98 Act on the Federal Office for Information Security (BSI Act - BSIG), BSI Act of 14 August 2009 (Federal Law Gazette I p. 2821).

99 Cours des comptes, 'The French Military Programming Law (LPM) 2019-2025 and the Capacities of the Armed Forces' (Press Release, 11 May 2022) <https://www.ccomptes.fr/system/files/2022-07/20220511-press-release-The-French-military-programming-law-2019-2025-and-capacities-of-armed-forces.pdf> accessed 28 March 2023.

offensive cyber responses to certain threats. The Information Society Code[100] governs electronic communications in Finland, whereas the Computer Misuse and Cybersecurity Act[101] in Singapore forbids illegal access and calls for the development of a national cybersecurity agency. These instances demonstrate the numerous ways in which countries use domestic legislation to handle cyberspace challenges.

3.2.1 The United Kingdom

The United Kingdom has established an extensive legal and policy framework to cover various areas of cyberspace. The framework is made up of both domestic laws and international treaties. In addition, the UK government has released a number of policies and measures to improve its cybersecurity posture and preserve its national interests.

Domestically, the United Kingdom has enacted a number of laws and regulations to combat cybercrime, cyber assaults, and data protection. The Computer Misuse Act 1990[102] criminalises illegal access to computer systems, while the Police and Justice Act 2006[103] makes it an offence to initiate a cyber assault that results in the interruption of services. Moreover, the Data Protection Act 2018[104] brings the EU GDPR[105] into the United Kingdom and establishes principles for the processing and protection of personal data.

The UK government has also established a number of organisations and entities to guarantee that these laws are implemented and enforced. The National Cyber Security Centre (NCSC),[106] which is part of the Government Communications Headquarters (GCHQ), is responsible for identifying and mitigating cyber threats in the United Kingdom. The NCSC also advises and assists organisations and individuals in improving their cybersecurity posture.[107]

At the international level, the United Kingdom is a signatory to many cybersecurity treaties, including the Budapest Convention on Cybercrime[108] and the

100 Ministry of Transport and Communication, Act on Electronic Communications Services (917/2014; amendments up to 1207/2020 included) (translation from Finnish) <https://www.finlex.fi> accessed 29 March 2023.

101 Computer Misuse and Cybersecurity (Amendment) Act 2017 (No 22 of 2017), Government Gazette Acts Supplement (12 May 2017).

102 Computer Misuse Act (n 46).

103 Police and Justice Act 2006, UK Public General Act 2006, c.48.

104 Data Protection Act 2018 (n 47).

105 Please note that even though the UK has leaved the EU and all EU regulations shall not be applied to the UK, the UK has legalised the GDPR in its Data Protection Act 2018, resulting that the GDPR substances are still applied to the UK jurisdiction.

106 National Cyber Security Centre, 'What We Do' (NCSC) <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> accessed 29 March 2023.

107 ibid.

108 Budapest Convention (n 8).

NATO Coordinated Cyber Defence Centre of Excellence (CCDCOE).[109] The United Kingdom also takes part in a number of international forums and conferences to address cybersecurity challenges and share best practices.

In addition to these legal and legislative frameworks, the United Kingdom has created a number of policies and efforts to strengthen its security strategy. The National Cyber Security Strategy 2022-2030 outlines the UK government's strategy and goals for cybersecurity in the country.[110] Among the elements in the strategy are investments in cybersecurity research and development, boosting the country's cyber defences, and enhancing international collaboration.

Overall, the United Kingdom's legal and legislative framework for cyberspace is extensive, reflecting the country's commitment to defending its national interests and preserving citizens' security. Yet, because cybersecurity threats are continually developing, the UK government must continue to examine and adapt its policies and plans in order to keep ahead of emerging risks and difficulties.

3.2.2 Germany

To meet the difficulties posed by cyberspace, Germany has built a comprehensive legal and policy framework. The country has taken several initiatives to defend its critical infrastructure and prevent cybercrime, while also emphasising the need for international collaboration in dealing with cybersecurity challenges.

The IT Security Act 2.0 (IT-Sicherheitsgesetz 2.0),[111] enacted in 2021, is an important legal instrument in Germany's cyber strategy. The Act compels firms that operate vital infrastructure to take specific cybersecurity measures and to notify the Federal Office for Information Security of any serious cybersecurity incidents (BSI).[112] The Act also established the BSI as Germany's national authority for information security, in charge of coordinating the country's cybersecurity activities as well as offering guidance and help to businesses and people.

Germany has also taken initiatives to prevent cybercrime, such as passing the Act to Improve the Enforcement of Criminal Law in Cyberspace (Gesetz zur Verbesserung der Durchsetzung von Rechten im Cyberspace) in 2017.[113] The

109 CCDCOE, 'About Us' (CCDCOE) <https://ccdcoe.org/about-us/> accessed 29 March 2023.

110 HM Government, 'Government Cyber Security Strategy: Building a cyber resilient public sector 2022-2030' (HM Government) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf> accessed 29 March 2023, 18–27.

111 Federal Office for Information Security, 'Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)' (Translation version) (BSI, 2021) <https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html> accessed 29 March 2023.

112 ibid.

113 Sandra Schmitz and Christian M Berndt, 'The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?' (Working Paper, 2019) <https://papers.ssrn.

Act criminalises a variety of cyber crimes, including hacking, cyber espionage, and malware creation and dissemination.[114]

In addition to these domestic measures, Germany has been an active participant in international efforts to improve cybersecurity. The government has been a significant supporter of the creation of international norms and guidelines for responsible cyberspace behaviour and has backed projects such as the Tallinn Manual on International Law Applicable to Cyber Warfare[115] and the Global Commission on Cyberspace Stability.[116]

Germany's cybersecurity law and regulatory framework is broad and aggressive, with a heavy emphasis on protecting vital infrastructure and combatting cybercrime as can be seen from its position paper on cyberspace.[117] The country's emphasis on international collaboration and the formation of standards and guidelines for responsible cyberspace behaviour indicates its appreciation of the importance of a coordinated and collaborative approach to resolving the issues posed by the digital age.

3.2.3 France

France has been working hard to build and execute legal and legislative frameworks to combat cyber threats. The government acknowledges that cyberspace poses a significant threat to national security and has made efforts to strengthen its legal and institutional capacities to address cyber threats.

France has enacted a number of rules and regulations to protect its critical infrastructure and combat cybercrime on a national level. For example, the National Cybersecurity Agency (ANSSI) was formed under the 2013 Military Programming Law (LPM) to manage the country's cybersecurity activities.[118] ANSSI has been crucial in defining critical infrastructure regulations and standards, as well as offering advice to government agencies and the private sector.

France passed a new cybersecurity and data protection and privacy law in 2018, with the goal of improving the country's ability to prevent, detect, and

---

com/sol3/papers.cfm?abstract_id=3306964> (accessed 29 March 2023) 1–41; Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (G-SIG: 16019378), Federal Law Gazette I, XVI/343.

114 Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums, ibid.

115 Schmitt (n 78).

116 Hague Centre for Strategic Studies (HCSS), 'Global Commission on the Stability of Cyberspace (GCSC)' (HCSS) <https://hcss.nl/global-commission-on-the-stability-of-cyberspace-homepage/> accessed 29 March 2023.

117 The German Federal Foreign Office and the German Federal Ministry of Defence, 'On the Application of International Law in Cyberspace' (German position paper, March 2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf> accessed 30 March 2023.

118 National Cybersecurity Agency of France (ANSSI), 'The National Cybersecurity Agency of France' (SSI) <https://www.ssi.gouv.fr> accessed 30 March 2023.

respond to cyber threats.[119] The law compels critical infrastructure operators to implement network security measures and to report cyber events to ANSSI. The law also gives ANSSI the authority to perform vulnerability assessments, monitor network traffic, and intervene to prevent cyber assaults.[120]

France has formed various international partnerships to combat cyber risks in addition to its legal and regulatory framework. The country is a member of the European Union's Cybersecurity Agency (ENISA)[121] and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE),[122] and it has taken part in a number of international cybersecurity efforts.

Notwithstanding these efforts, however, France continues to confront substantial challenges in coping with the expanding cyber threat scenario. Some high-profile cyber assaults have occurred in the nation, notably the 2017 WannaCry ransomware outbreak, which damaged thousands of systems globally.[123] France must continue to strengthen its legal and institutional skills in order to handle these concerns, notably by encouraging international collaboration and information exchange.

Finally, France has made tremendous progress in building and implementing its cyberspace legal and policy frameworks as appeared in the open-ended working group paper.[124] The government recognises the importance of cybersecurity to national security and has made initiatives to improve its response capabilities to cyber attacks. To meet the expanding cyber threat scenario, the government must stay attentive and continue to modify its legislative and institutional structures.

3.2.4 Finland

To address cybersecurity challenges, Finland has built a comprehensive legislative and policy framework. The country's approach to cybersecurity is a mix of domestic regulation, international collaboration, and public-private

119 Anne-Laure Villedieu, 'Data Protection and Cybersecurity Laws in France' (CMS, 2021) <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/france> accessed 30 March 2023; LOI n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, 10 May 2018, INTX1728622L.

120 Villedieu, ibid.

121 ENISA (n 68).

122 CCDCOE (n 109).

123 Kaspersky, 'What is WannaCry Ransomware?' (Kaspersky) <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry> accessed 31 March 2023; RFI, 'French Researchers Crack Open WannaCry Ransomware' (RFI, 20 May 2017) <https://www.rfi.fr/en/france/20170520-french-researhers-crack-open-wannacry-ransomware> accessed 31 March 2023.

124 France, 'International law applied to operations in cyberspace' (Open-ended working group, December 2021) <https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf> accessed 31 March 2023.

partnerships. Finland has also been an active promoter of international cybersecurity rules and standards.

On a national level, Finland has adopted a number of cybersecurity legislation and regulations. The most important of them is the Act on the Protection of Privacy in Electronic Communications, which regulates personal data processing and electronic communication secrecy.[125] The Information Security Act,[126] the Criminal Code,[127] and the Data Protection Act[128] are all significant statutes. These laws offer the legal foundation for maintaining critical infrastructure security and punishing cyber criminals.

Finland has a cyber security strategy, which was initially published in 2013 and was recently revised.[129] The plan specifies the country's cybersecurity goals and objectives, such as improving the cybersecurity skills of government agencies, critical infrastructure operators, and other stakeholders. In addition, the policy emphasises the necessity of international cooperation in solving cybersecurity concerns.

Finland is also an active participant in worldwide cybersecurity activities in addition to its national efforts. Since its founding in 2014, Finland has been a member of the EU's Network and Information Security Cooperation Group (ENISA),[130] as well as a member of the NATO CCDCOE.[131] Finland has also been a key contributor to the establishment of international cybersecurity rules and standards, such as the Tallinn Manual on International Law Applicable to Cyber Warfare[132] and the Paris Call for Trust and Security in Cyberspace.[133]

Generally, Finland's cybersecurity law and policy framework is extensive and well-developed. This includes its national positions dealing with cyber threats.[134] To meet the complex and developing difficulties of cyberspace, the country's

125 Act on the Protection of Privacy in Electronic Communications (516/2004; amendments up to 365/2011 included) (Unofficial Translation) <https://www.finlex.fi> accessed 31 March 2023; DLA Piper, *Data Protection Laws of the World: Finland* (DLA Piper) 1–16.

126 Government Decree on Information security in central government (681/2010) (Unofficial Translation) <https://https://finlex.fi/en> accessed 31 March 2023.

127 Finland Penal Code, Chapter 38, section 8.

128 Jukka Lang and Tuomas Haavikko, 'Data Security and Cybercrime in Finland' (Lexology, 14 January 2019) <https://www.lexology.com/library/detail.aspx?g=9d2dd419-3a42-464a-8df0-ed1ffb9dedd7> accessed 31 March 2023.

129 Ministry of Foreign Affairs of Finland, 'Cyber security and the cyber domain' (Ministry of Foreign Affairs) <https://um.fi/cyber-security-and-the-cyber-domain> accessed 31 March 2023.

130 ENISA (n 68).

131 CCECOE (n 122).

132 Schmitt (n 78).

133 Paris Call for Trust and Security in Cyberspace <https://pariscall.international/en/call> accessed 31 March 2023.

134 Finland (n 25).

approach to cybersecurity incorporates national law, international collaboration, and public-private partnerships.

3.2.5 Singapore

Singapore is a leader in the implementation of international law in cyberspace. As Singapore presided over ASEAN in 2018, a framework for the ASEAN Cyber Capacity Program was formed,[135] as was the ASEAN Ministerial Conference on Cybersecurity,[136] which included the formation of the ASEAN-Singapore Cyber Center of Excellence.[137] The Centre's goal is to provide training, research, and information sharing on strategic, policy, legal, and operational cyberspace concerns. These initiatives are intended to integrate cyber diplomacy efforts with operational challenges in order to achieve regional collaboration toward a single stance on international platforms.[138] Australia, Canada, the European Union, South Korea, New Zealand, and the United Kingdom all contribute to the Centre's activities.[139]

Singapore's stance on the application of international law in cyberspace is clearer than that of the other ASEAN members. Singapore contemplates dealing with cyberspace regulations, particularly during the State action in international law is critical in ensuring an open, safe, stable, accessible, peaceful, and interoperable ICT environment for digitalisation.[140] Singapore has said unequivocally that the laws regulating cyberspace under international law are governed by the United Nations Charter.[141] Singapore has also said unequivocally that State sovereignty is a principle that applies equally to States. Other common law concepts of international law, such as the prohibition of interference, peaceful resolution of conflicts, self-defence, armed attack, and use of force, can also apply to cyber concerns. It is a basic value enshrined in the United Nations Charter.[142] Other principles may also be implemented to the extent practicable. It is critical to evaluate the consequences of cyber activity. Malicious cyber activity

135 International Telecommunication Union (ITU), 'Global Cybersecurity Index 2020' (ITU Publications 2020) <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> accessed 1 April 2023.

136 ASEAN Secretariat (n 12).

137 Cyber Security Agency of Singapore (n 32).

138 Government of Singapore (n 60).

139 Noor (n 92) 113.

140 United Nations, 'Singapore's Views on Developments in the Field of Information and Telecommunications in the Context of International Security, Pursuant to General Assembly Resolutions 73/27 and 73/266' (UN 2019) <https://www.un.org/en/> accessed 1 April 2023.

141 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'National position of Singapore (2021)' (CCDCOE, 25 November 2021) <https://cyberlaw.ccdcoe.org/wiki/National_position_of_Singapore_(2021)> accessed 1 April 2023; United Nations General Assembly (n 178) para 83.

142 CCECOE, ibid; UN General Assembly, ibid paras 83–84.

attributable to a State, for example, that interferes with the normal governing functions of a victim State is an example of an internationally unlawful act.[143]

4. Applicability of regional and domestic legal instruments and policy framework in cyberspace

Cyberspace is a complicated and rapidly evolving domain that presents various legal issues. These challenges include personal data security, cyber behaviour regulation, and cybercrime prevention. Several legal tools and policy frameworks have been established at the international, regional, and national levels to tackle these issues.

Regional organisations have also established legal tools and policy frameworks to handle legal challenges in cyberspace. The Convention on Cybercrime of the Council of Europe,[144] for example, is a regional legislative framework that strives to improve cybersecurity and safeguard personal data in their respective regions.

Some States have built their legal frameworks and strategies to address cyberspace legal challenges on a domestic basis.[145] Legislation that criminalises cybercrime, regulates online activity, and safeguards personal data is included in these frameworks. Local legislative frameworks also provide tools for international collaboration in the fight against cyber threats and the promotion of cybersecurity.

In this regard, the unique nature of cyberspace, as well as its implications for issues of State sovereignty, extraterritoriality, and the idea of cyberspace sovereignty, are obstacles to the application of international law principles. The numerous legal difficulties that exist in cyberspace are discussed here, as well as how international law might be used to overcome them.

143 United Nations General Assembly, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law applies to the Use of Information and Communications Technologies by States submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266' (13 July 2021) UN Doc A/76/136, para 84.

144 Budapest Convention (n 8).

145 See, for example, Foreign, Commonwealth & Development Office (n 45); German Federal Foreign Office and the German Federal Ministry of Defence (n 117); France (n 124); Finland (n 25).

4.1 Regional and domestic legal instruments and policy framework to State sovereignty violation

4.1.1 Regional level

Regional legal instruments and policy frameworks play an important role in dealing with abuses of state sovereignty in cyberspace. To solve these problems, some regional organisations have adopted legal tools and policy frameworks. The EU, the OAS, the OSCE, and the ASEAN and their approaches to state sovereignty violations in cyberspace will be examined in this research.

The EU's approach to state sovereignty violations in cyberspace is founded on the principles of state sovereignty, territorial integrity, and critical infrastructure protection. The EU's Cybersecurity Strategy highlights the necessity of protecting critical infrastructure from cyber attacks while also encouraging collaboration among member states and private sector stakeholders.[146] The EU also backs international initiatives to encourage responsible state behaviour in cyberspace, such as the creation of rules and confidence-building measures.[147] The EU's efforts in this area have resulted in the creation of legislative instruments such as the EU Cybersecurity Act[148] and the NIS2 Directive,[149] which aim to improve cybersecurity and protect the EU's critical infrastructure.

The OAS's approach to state sovereignty violations in cyberspace is based on the principles of non-intervention and human rights protection. The OAS has created the Inter-American Convention Against Cybercrime, which criminalises cyber actions such as hacking, cyber fraud, and the distribution of dangerous software.[150] The Convention also establishes a framework for international cooperation in cybercrime investigation and prosecution. Furthermore, the OAS encourages the development of cybersecurity capabilities in its Member States, including the formulation of national cybersecurity policies and the adoption of international standards.

The OSCE's approach to State sovereignty violations in cyberspace is guided by principles of human rights, basic freedoms, and the rule of law. The OSCE's cyber/ICT security Concept emphasises the necessity of safeguarding critical infrastructure and encouraging international collaboration in combating cyber threats.[151] The OSCE also fosters the development of confidence-build-

146 Vela (n 61); Joint Communication to the European Parliament (n 61).
147 CCDCOE (n 80).
148 Cybersecurity Act (n 51).
149 NIS 2 Directive (n 42).
150 US Department of State (n 70).
151 CCDCOE (n 80); OSCE Permanent Council (n 80); OSCE Permanent Council, 'Decision No. 1202 OSCE Confidence-Building Measures to reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.

ing measures[152] and the adoption of rules for responsible state behaviour in cyberspace. In addition, the OSCE has launched a variety of capacity-building projects to assist its Member States in improving their cybersecurity capabilities.

The ASEAN approach to state sovereignty violations in cyberspace is built on the principles of non-intervention and respect for country sovereignty. ASEAN has established the ASEAN Regional Forum Declaration on Cooperation in the Area of Information and Communication Technology (ICT) Security, which underlines the necessity of member-state collaboration in dealing with cyber threats.[153] ASEAN also encourages the establishment of capacity-building programs and the implementation of international cybersecurity rules and standards.[154]

In conclusion, regional legal instruments and policy frameworks play an important role in resolving violations of state sovereignty in cyberspace. Various regional organisations have produced legal instruments and policy frameworks that reflect their particular regional environments and agendas. The EU, OAS, OSCE, and ASEAN all have various ways of dealing with state sovereignty violations in cyberspace, but they all have the same aim of improving cybersecurity and preserving critical infrastructure.

4.1.2 Domestic level

Domestic legal instruments and policy frameworks are also important in dealing with state sovereignty violations in cyberspace. To address these issues, some countries have established legal instruments and policy frameworks. This analysis will examine the approaches of the UK, Germany, France, Finland, and Singapore to State sovereignty violations in cyberspace.

The UK's approach to State sovereignty violations in cyberspace is based on the concepts of national security and critical infrastructure protection. The United Kingdom's National Cyber Security Strategy establishes a comprehensive strategy for cybersecurity, including efforts to safeguard critical infrastructure, improve intelligence capabilities, and foster international collaboration.[155] The UK has also passed the Cybersecurity Information Sharing Act, which establishes a legal framework for the exchange of cybersecurity data between public and private sector institutions.[156]

152 CCDCOE, ibid.

153 ASEAN Secretariat (n 86); ASEAN Secretariat (n 87); ASEAN Secretariat (n 89).

154 Government of Singapore (n 60); Nur Azha Putra (n 60).

155 National Cyber Security Centre (n 106).

156 Foreign & Commonwealth Office, 'Guidance on Cyber-threat intelligence information sharing guide' (GOV.UK, 8 March 2021) <www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide> accessed 3 April 2023.

Germany's approach to State sovereignty violations in cyberspace is grounded in the principles of human rights and critical infrastructure protection. To counter cyber risks, the German government has created a variety of legislative instruments, including the Cybersecurity Act[157] and the IT Security Act.[158]

France's approach to State sovereignty violations in cyberspace is based on the concepts of national security and critical infrastructure protection. The French government has created a variety of legislative tools to combat cyber risks, including the Military Programming Law[159] and the National Cybersecurity Strategy.[160]

Finland's approach to State sovereignty violations in cyberspace is built on the principles of human rights and critical infrastructure protection. To counter cyber risks, the Finnish government has created a variety of legislative instruments, including the Act on the Protection of Privacy in Electronic Communications[161] and the Cybersecurity Strategy.[162]

Singapore's approach to State sovereignty violations in cyberspace is based on national security and critical infrastructure protection principles. The Singapore government has created a variety of legislative tools to combat cyber threats, including the Cybersecurity Bill which later becomes the Cybersecurity Act.[163]

In conclusion, domestic legal instruments and policy frameworks are crucial for dealing with violations of State sovereignty in cyberspace. Many States have created legal instruments and policy frameworks that reflect their situations and agendas. The approaches employed by the UK, Germany, France, Finland, and Singapore to resolve State sovereignty violations in cyberspace vary, but they all have the same aim of boosting cybersecurity and preserving key infrastructure. These laws aim to strengthen cybersecurity and protect critical infrastructure by introducing clear cybersecurity standards for corporations and government agencies.

157 Sandra Schmitz and Christian M Berndt (n 113) 1–41; Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (G-SIG: 16019378) (n 113).

158 Federal Office for Information Security, 'Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)' (Translation version) (BSI, 2021) <www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html> accessed 3 April 2023.

159 Cours des comptes (n 99).

160 National Cybersecurity Agency of France (ANSSI) (n 118).

161 Act on the Protection of Privacy in Electronic Communications (516/2004; amendments up to 365/2011 included) (n 125).

162 Ministry of Foreign Affairs of Finland, 'Cyber security and the cyber domain' (Ministry of Foreign Affairs) <https://um.fi/cyber-security-and-the-cyber-domain> accessed 4 April 2023.

163 Singapore Government Agency, 'Cybersecurity Act' (Cyber Security Agency of Singapore) <https://www.csa.gov.sg/legislation/Cybersecurity-Act> accessed 2 March 2023.

4.2 Regional and domestic legal instruments and policy framework for extraterritorial effects

4.2.1 Regional level

Regional legal instruments and policy frameworks play a significant role in tackling extraterritorial effects in cyberspace. The potential of activities made in one state to have an influence on another is referred to as extraterritoriality. This might result in complicated legal challenges requiring international collaboration and coordination. The purpose of this part is to look at how the EU, the OAS, the OSCE, and the ASEAN deal with extraterritoriality in cyberspace.

The EU has created a comprehensive framework for dealing with extraterritoriality in cyberspace. The EU's GDPR applies to all companies, regardless of location, that process the personal data of EU citizens.[164] This implies that companies operating outside the EU must follow EU data protection standards if they process EU citizens' data. The GDPR also includes the right to be forgotten, which permits individuals to request that their personal data be deleted from online platforms situated outside of the EU.[165] In addition, the EU has a number of bilateral and multilateral agreements with other States in place to enhance international collaboration and coordination on cybersecurity issues.[166]

The OAS has developed a variety of legislative instruments to address extraterritoriality in cyberspace. The Inter-American Cooperation Portal on Cyber-Crime establishes a framework for collaboration among OAS Member States in cybercrime investigation and prosecution.[167] The OAS also runs a Cybersecurity Program, which offers Member States technical support to help them enhance their cybersecurity capabilities.[168]

The OSCE has established an extensive strategy for dealing with extraterritoriality in cyberspace. The OSCE's Confidence-Building Measures (CBMs) in Information and Communication Technology seek to improve openness and collaboration among OSCE member states on cybersecurity problems.[169] The OSCE also operates a Cybersecurity Capacity Building Program, which offers Member States training to assist them to strengthen their cyberspace competency.[170]

---

164 GDPR (n 41).

165 GDPR, ibid art 17; Ben Wolford, 'Everything You Need to Know about the "Right to be Forgotten"' (GDPR) <https://gdpr.eu/right-to-be-forgotten/> accessed 4 April 2023.

166 NIS 2 Directive (n 42); Cybersecurity Act (n 51); Jorida Vela (n 61); Joint Communication to the European Parliament (n 61).

167 OAS, 'The Inter-American Cooperation Portal on Cyber-Crime' (Cybercrimedata AS) <https://www.cybercrimelaw.net/OAS.html> accessed 5 April 2023.

168 US Department of State (n 70).

169 CCDCOE (n 80); OSCE Permanent Council (n 80).

170 ICT4Peace (n 82).

ASEAN has set up a number of legal mechanisms to deal with extraterritoriality in cyberspace. The e-ASEAN framework agreement and information and communications technology (ICT) capacity building establishes a framework for ASEAN member states to collaborate on cybersecurity challenges.[171] The ASEAN Cybersecurity Cooperation Strategy also includes a road map for improving regional cybersecurity cooperation and coordination.[172]

In conclusion, regional legal instruments and policy frameworks are important in tackling extraterritoriality in cyberspace. The EU, OAS, OSCE, and ASEAN all take various approaches to these concerns, but they all share the objective of strengthening international collaboration and coordination on cybersecurity issues. These regional frameworks are critical for dealing with the complex legal challenges that arise in cyberspace and maintaining a safe and secure digital environment for all.

4.2.2 Domestic level

Domestic legal instruments and policy frameworks are equally significant in dealing with extraterritoriality in cyberspace. This analysis looks at how the UK, Germany, France, Finland, and Singapore approach extraterritoriality in cyberspace through domestic legal instruments and policy frameworks.

The UK has taken several measures to address extraterritoriality in cyberspace. The Data Protection Act 2018 of the UK applies to all companies that process the personal data of UK citizens, regardless of where they are located.[173] This means companies operating outside of the UK must follow UK data protection legislation if they process data from UK residents. In addition, the UK has a variety of regulations in place to combat cybercrime, notably the Computer Misuse Act of 1990[174] and the Police and Justice Act of 2006.[175]

Germany has also taken measures to combat extraterritoriality in cyberspace. The German Federal Data Protection Act applies to all enterprises, wherever they occur, that process the personal data of German residents.[176] The Act also includes a right-to-be-forgotten provision, which allows individuals to request that their personal data be deleted from online platforms situated outside of Germany.[177] Germany recently approved the Network Enforcement Act, which

171 ASEAN Secretariat (n 86).
172 ASEAN Secretariat (n 12).
173 Data Protection Act 2018 (n 47).
174 Computer Misuse Act (n 46).
175 Police and Justice Act 2006 (n 103).
176 Federal Data Protection Act (BDSG) (Federal Law Gazette I, p. 1858; 2022 I p. 1045).
177 Didomi, 'Germany's data privacy protection laws: Everything you need to know' (Didomi, 26 February 2023) <https://blog.didomi.io/en/germany-data-privacy-protection-laws-everything-you-need-to-know> accessed 6 April 2023.

mandates that social media firms remove illegal content within 24 hours or face fines.[178]

France has implemented a number of efforts to combat extraterritoriality in cyberspace. The French Data Protection Act applies to all enterprises, regardless of geography, that process the personal data of French citizens.[179] France recently ratified the Military Programming Law 2019-2025, which contains steps to strengthen the country's cybersecurity capabilities and battle cyber threats.[180]

Under its Cyber Security Strategy, Finland has put in place measures aimed at combating extraterritoriality in cyberspace.[181] The Strategy establishes a framework for improving cybersecurity cooperation and coordination among Finland and other States. Finland has also approved the Data Protection Act, which applies to all enterprises, irrespective of where they operate, that process the personal data of Finnish citizens.[182]

Through its Cybersecurity Act, Singapore has put in place safeguards to counter extraterritorial effects in cyberspace.[183] The Act requires key information infrastructure owners to implement cybersecurity safeguards for their systems and regulates cybersecurity service providers.[184] Singapore has also set up a Cyber Security Agency, which is in charge of coordinating cybersecurity operations and responding to cyber attacks.[185]

Consequently, domestic legal instruments and policy frameworks are critical in tackling extraterritoriality in cyberspace. The United Kingdom, Germany, France, Finland, and Singapore all take various approaches to these concerns, but they all share the objective of ensuring a safe and secure digital environment for their inhabitants. These domestic frameworks are critical for handling the complex legal challenges that occur in cyberspace, as well as for encouraging international collaboration and coordination on cybersecurity matters.

178 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech' (Library of Congress, 2021) <www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/> accessed 6 April 2023.

179 OneTrust DataGuidance, 'The Data Protection Act' (DataGuidance) <www.dataguidance.com/sites/default/files/france_data_protection_act.pdf> accessed 6 April 2023.

180 ANSSI (n 118).

181 Ministry of Foreign Affairs of Finland (n 162).

182 Lang, Haavikko (n 128).

183 Singapore Government Agency, 'Cybersecurity Act' (Cyber Security Agency of Singapore) <https://www.csa.gov.sg/legislation/Cybersecurity-Act> accessed 6 April 2023.

184 ibid.

185 Singapore Government Agency, 'Who We Are' (CSA) <http://www.csa.gov.sg> accessed 6 April 2023.

4.3 Regional and domestic legal instruments and policy framework for cyberspace sovereignty

4.3.1 Regional level

Regional legal instruments and policy frameworks are critical in resolving the challenges of cyberspace sovereignty. This examination will look at how the EU, the OAS, the OSCE, and the ASEAN deal with these issues.

The EU has implemented several measures to address cyberspace sovereignty issues. The EU Cybersecurity Act, passed in 2019, creates a European cybersecurity certification system with the goal of improving the cybersecurity of goods, processes, and services.[186] In addition, the EU has adopted a variety of laws and efforts to support the free movement of data inside the EU while protecting personal data and other rights. Furthermore, the EU has formed the ENISA, which provides cybersecurity advice and support to EU member states.[187]

The OAS has also taken measures to deal with concerns about cyberspace sovereignty. The OAS has adopted a variety of cybersecurity resolutions, including the Inter-American Cybersecurity Strategy[188] and the Declaration on the Protection of Critical Infrastructure from Emerging Threats.[189] The OAS has also formed the CICTE, which encourages member governments to work together to combat cyberspace risks.[190]

The OSCE has put in place a number of measures to address cyberspace sovereignty challenges. The OSCE has established a variety of CBMs targeted at increasing openness and lowering the danger of cyber warfare.[191] The OSCE also encourages conversation and collaboration among Member States on cybersecurity problems through its annual Confidence-Building Measures Conference and its informal cybersecurity expert group.[192]

ASEAN has made initiatives to resolve cyberspace sovereignty challenges through its 2020 ASEAN ICT Masterplan.[193] The Plan contains initiatives targeted at improving cybersecurity cooperation among ASEAN Member

186 Cybersecurity Act (n 51).

187 ENISA (n 68).

188 OAS, 'A comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity' (OAS) <http://www.oas.org/juridico/english/cyb_pry_strategy.pdf> accessed 7 April 2023.

189 Inter-American Committee Against Terrorism (CICTE), 'Declaration on the Protection of Critical Infrastructure from Emerging Threats' (23 March 2015) OEA/Ser.L/X.2.15, CICTE/doc.1/15.

190 US Department of State (n 70).

191 CCDCOE (n 80); OSCE Permanent Council (n 80); OSCE Permanent Council (n 151).

192 OSCE, 'Confidence and Security Building Measures' (OCSE) <https://www.osce.org/secretariat/107484> accessed 8 April 2023.

193 ASEAN Secretariat (n 89).

States and fostering the establishment of a secure and resilient digital environment.[194] ASEAN has also established the ASEAN Ministerial Conference on Cybersecurity, which provides a forum for Member States to debate cybersecurity challenges and foster collaboration.[195]

In conclusion, regional legal instruments and policy frameworks are essential for tackling cyberspace sovereignty challenges. The EU, OAS, OSCE, and ASEAN all take various approaches to these concerns, but they all share the objective of creating a safe and secure digital environment for their inhabitants. These regional frameworks are critical for encouraging international collaboration and coordination on cybersecurity challenges, as well as resolving the complex legal issues that develop in cyberspace.

4.3.2 Domestic level

Domestic legal instruments and policy frameworks also play an important role in resolving cyberspace sovereignty challenges. In this part, they include the analysis of the UK, Germany, France, Finland, and Singapore dealing with cyberspace sovereignty challenges.

The UK has implemented a lot of measures to address cyberspace sovereignty concerns. The National Cyber Security Strategy of the UK seeks to make the country a safe and resilient digital nation.[196] The policy includes safeguards for important national infrastructure, increased cybersecurity skills and awareness, and collaboration with foreign partners to combat cyber attacks.[197] The United Kingdom has also established the National Cyber Security Centre (NCSC), which provides cybersecurity advice to organisations and individuals.[198]

Germany has also begun addressing the problems of cyberspace sovereignty. Germany's cybersecurity plan includes efforts to protect key infrastructure, encourage cybersecurity research and development, and strengthen international cybersecurity cooperation.[199] The German government has also formed the Federal Office for Information Security (BSI), which is in charge of guaranteeing the security of government and critical infrastructure operators' information technology systems.[200]

Through its National Strategy for Cybersecurity, France has adopted measures to address the challenges of cyberspace sovereignty. The policy includes initiatives to improve critical infrastructure cybersecurity, encourage cybersecurity research and development, and strengthen international cybersecurity

194 ibid.
195 Government of Singapore (n 60); Nur Azha Putra (n 60).
196 HM Government (n 110).
197 ibid.
198 National Cyber Security Centre (n 106).
199 German Federal Foreign Office and the German Federal Ministry of Defence (n 117).
200 Federal Office for Information Security (n 158).

cooperation.[201] In addition, the French government formed the ANSSI, which is in charge of defending the government and critical infrastructure networks.[202]

Finland has implemented measures to address issues related to cyberspace sovereignty through its National Cyber Security Strategy.[203] The policy includes efforts to secure key infrastructure, strengthen Finnish organisations' and people's cybersecurity capabilities, and collaborate with international partners to address cybersecurity concerns.[204] In addition, the Finnish government formed the Finnish Transport and Communications Agency (Traficom), which is in charge of guaranteeing the security of Finland's communications networks.[205]

Singapore has undertaken efforts to resolve cyberspace sovereignty challenges through its Cybersecurity Strategy.[206] The policy includes efforts to secure key infrastructure, improve the cybersecurity capabilities of Singaporean businesses and individuals, and collaborate with international partners to address cybersecurity concerns. The Singaporean government has also formed the Cyber Security Agency (CSA), which is in charge of advising businesses and people on cybersecurity matters.[207]

Therefore, domestic legal instruments and policy frameworks are beneficial in resolving cyberspace sovereignty challenges. The UK, Germany, France, Finland, and Singapore have all enacted cybersecurity measures to defend their population and key infrastructure from cyber attacks. These domestic frameworks are critical for maintaining a safe and secure digital environment as well as dealing with the complex legal challenges that arise in cyberspace.

5. Conclusion

The rapid digital transformation of society has presented unique opportunities and challenges, particularly at the regional and domestic levels. As cyberspace becomes increasingly integral to daily life, the need for robust regional collaboration and effective domestic strategies has become more pressing. Countries and regional organisations are navigating this complex landscape with tailored legal frameworks and policies aimed at addressing the multifaceted threats posed by ICT vulnerabilities.

---

201 France (n 124).

202 ANSSI (n 118).

203 Ministry of Foreign Affairs of Finland (n 162).

204 ibid.

205 'New approaches to regulating transport in Finland: Case study on the Transport and Communications Agency (TRAFICOM)' (OECD Library) <www.oecd-ilibrary.org/sites/a3fe77bc-en/index.html?itemId=/content/component/a3fe77bc-en> accessed 11 April 2023; Traficom, 'About Traficom' (Traficom) <www.traficom.fi/en/traficom/about-traficom> accessed 11 April 2023.

206 Singapore Government Agency (n 183).

207 Singapore Government Agency (n 185).

Regional initiatives have demonstrated the value of cooperative approaches in combating cyber threats. Frameworks such as the EU's cybersecurity directives and ASEAN's regional strategies highlight the importance of harmonising efforts across member states. These initiatives not only enhance cybersecurity capabilities but also foster shared standards that allow for coordinated responses to emerging threats. The adaptability of these regional frameworks is a critical factor in ensuring their relevance in an ever-evolving digital environment.

At the domestic level, nations have implemented a diverse array of legal instruments and policies to address specific cybersecurity challenges. For instance, countries like the UK and Germany have developed comprehensive national strategies to protect critical infrastructure, while Singapore and France have emphasised data protection and privacy through forward-thinking legislation. These domestic efforts reflect the distinct priorities and resources of individual states, demonstrating the necessity of tailored approaches to cyber governance.

The intersection of regional and domestic strategies underscores the importance of collaboration in addressing cybersecurity challenges. By aligning domestic priorities with regional objectives, states can build resilient frameworks that are both locally effective and regionally cohesive. This synergy ensures that the dynamic nature of cyber threats is met with equally dynamic solutions, capable of safeguarding both national and regional interests.

In an era defined by rapid technological advancement, the future of cybersecurity governance lies in the ability of regional and domestic actors to innovate and adapt. Through continued cooperation and the refinement of legal and policy frameworks, nations and regions can establish a robust defense against the complexities of cyberspace while fostering an environment of security, trust, and shared progress.