GCSP
Geneva Centre for Security Policy

EU CYBER DIRECT

CICIR
中国现代国际关系研究院
CHINA INSTITUTES OF CONTEMPORARY INTERNATIONAL RELATIONS

Jurisdiction in Cyberspace

Tsvetelina van Benthem, Joanna Kulesza, Ye Liu, Nanxiang Sun

Sino-European Expert Working Group on the Application of International Law in Cyberspace (EWG-IL), Research Group Report 2024

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-018-1

About the partner organisations

China Institutes of Contemporary International Relations

The China Institutes of Contemporary International Relations (CICIR) is a longstanding, extensive, and multifunctional research and consultation complex focusing on international strategic and security studies. It covers all geographic areas and major strategic and comprehensive issues in the world. The CICIR has a staff of about 300, including researchers and administrative and logistical personnel, who work for 15 institutes, a number of centres, and several offices. For years it has participated in wide-ranging, thorough and high-end international academic exchanges. The CICIR is authorised to confer master's and doctoral degrees, and publishes three academic journals: Xiandai Guoji Guanxi, Contemporary International Relations and China Security Studies.

EU Cyber Direct

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen a rules-based order in cyberspace and build cyber-resilient societies. To fulfil this aim it conducts research, supports capacity-building in partner countries and promotes multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security, and peace. Governed by 55 Member States, this flagship foundation is supported by the Swiss government to provide a unique 360° approach to learn about and solve global challenges. Our mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions for a more peaceful future.

Xiamen University

Xiamen University (XMU), established in 1921, has long been listed among China's leading universities. With a graduate school, six academic divisions consisting of 33 schools and colleges, and 16 research institutes, XMU boasts a total enrolment of nearly 44,000 full-time students, and has over 3,000 full-time teachers and researchers, of whom 32 are members of either the Chinese Academy of Sciences or the Chinese Academy of Engineering.

Background

This report has been produced in the context of a larger research and dialogue project: The China Institutes of Contemporary International Relations (CICIR), the EU Cyber Direct, the Geneva Centre for Security Policy (GCSP), and Xiamen University convene a joint Sino-European Expert Working Group on the Application of International Law in Cyberspace (WG IL). The working group provides a platform for exchange among European and Chinese legal experts to examine the application of international law in cyberspace. The main goal of the work in research groups is to provide more thorough analysis of the selected topics and identify points of divergence and convergence between European and Chinese side with the purpose to create more evidence-based and trusted environment for the policy discussions in track 1.5. and track 1 processes.

Authors

Tsvetelina VAN BENTHEM, Lecturer in International Law, Diplomatic Studies Programme and Research fellow, Oxford Institute for Ethics, Law and Armed Conflict

Joanna KULESZA, Assistant Professor of International Law and Director of Lodz Cyber Hub Research Center, University of Lodz

Ye LIU, Ph.D candidate of International Law, Research Assistant of Cyberspace International Law Center, Xiamen University

Nanxiang SUN, Associate Professor, Institute of International Law of Chinese Academy of Social Sciences

Acknowledgements

On the European side, this report was sponsored by the Swiss Department of Foreign Affairs, whose generous support is greatly appreciated. The constructive feedback and valuable insights of the reviewers, Wei PEI and Pål WRANGE, whose expertise has contributed to the quality of this publication, are also acknowledged with gratitude.

Contents

1. Introduction

Sovereignty is a foundational principle of international law on which various rights and obligations are grounded.[1] Sovereignty denotes both the power of states to regulate behavior and processes and to enforce said regulations, as well as the protection states derive from international law against external interference.[2] What sovereignty empowers states to do and how it protects them from external threats change over time. This process of change, spurred by the evolving needs of the international community, including needs connected to the regulation of information and communications technologies (ICTs), is driven by developments in international law – the adoption of new treaties or the application of existing ones to new fact patterns, and the continuous identification and specification of customary rules. Sovereignty and jurisdiction are closely connected. The rules of jurisdiction under international law play an important role in the allocation of power among sovereign equals. They are, on the one hand, a manifestation of the power of states to regulate and enforce regulations and, on the other hand, a boundary to that power determined in light of the interests of other states and individuals.

This Working Paper explores the concept of jurisdiction in international law as it applies to the ICT environment. Part II focuses on general issues of jurisdiction, and more specifically on the methodological starting point from which the limits of state jurisdiction must be assessed, and on the different types of jurisdiction. Part III discusses the heads of prescriptive jurisdiction under customary international law in their application to cyberspace. Part IV concentrates on the application of enforcement jurisdiction in cyberspace. Part V concludes and provides suggestions for further academic inquiry.

1 2024 Working Paper *The Principle of Sovereignty and the Application of International Law in Cyberspace*, available at https://eucyberdirect.eu/research/the-principle-of-sovereignty-and-the-application-of-international-law.

2 J. D'Aspremont (2017) The Oxford Handbook of the Sources of International Law, Oxford, Oxford University Press, A. Schwabach and A.J. Cockfield (eds) (2009) International Law and Institutions, EOLSS Publications.

2. General issues of jurisdiction

Jurisdiction, in the context of international law, refers to the authority exercised by a state over individuals, objects, and events. This authority manifests in the formulation, application, and enforcement of laws and regulations. Essentially, jurisdiction encompasses two primary functions: prescriptive jurisdiction (the power to create binding regulations) and enforcement jurisdiction (the power to implement binding regulations).[3] While the capacity to engage in these functions stems from a state's sovereignty, the scope of jurisdiction is often limited by international law, including the prohibitions on the use of force and intervention, and obligations under international human rights law.

At the outset, it is important to stress that the customary rules on jurisdiction apply automatically to the use of ICTs, making it unnecessary to identify cyber-specific state practice and *opinio juris* for their application.

2.1 Methodological framework for identifying the relevant customary international law rules of jurisdiction

As the jurisdiction of states delineates their competence to create, apply, and enforce laws, determining the starting point for assessing that competence is of particular significance. Are states free to regulate and/or enforce regulations unless there is a prohibitive rule that demands abstention, or do states need to demonstrate a permissive basis to regulate and/or enforce regulations? In the former approach, the starting point is freedom. In the latter approach, the starting point is restriction of action.

No concerns arise with the exercise of regulatory or enforcement power within the state's territory. It is regulation and enforcement with extraterritorial reach that could potentially lead to interference with the interests of other states. In the 1927 Judgment of the Permanent Court of International Justice (PCIJ) in the S. S. Lotus case, the PCIJ distinguished between two scenarios. The first scenario concerned the exercise of jurisdiction within a state's own territory but related to acts having occurred abroad. According to the Court, this scenario calls for a freedom-based approach: it opined that international law *does not* contain "a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory". In such cases, according to the PCIJ, there is no need to seek permissive rules to exercise jurisdiction because the starting point is one of freedom.[4] In contrast, the second scenario, concerned with the *exercise of power* by one state *in the territory of another*, entails a restriction-based approach: "the first and foremost restriction imposed by international law upon a State is that, failing the existence of a permissive rule to the contrary, it may not exercise its power in any form in the territory of another State".[5]

3 The paper uses the categories of prescriptive and enforcement jurisdiction instead of the tripartite division of prescriptive, adjudicative and enforcement jurisdiction. Adjudicative jurisdiction can logically be understood as falling under the headings of prescription (creation or development of legal rules) and enforcement (the application of said rules).

4 PCIJ, S.S. Lotus (France v Turkey) 1927 PCIJ (ser. A) No. 10, §46.

5 Ibid, §45.

While the restrictive approach to the *exercise of enforcement power* in another state's territory continues to hold, it is today accepted that the starting point for determining state power to *extend and apply laws* to persons, property, and acts outside a state's territory is not one of complete freedom. Indeed, in a system of co-existing independent communities, a complete freedom to assert the applicability of a state's public laws extraterritorially would inevitably encroach upon the interests of other states.

What the practice of states shows is, first, that regulatory extensions beyond a state's territory are accompanied by an assertion of legal basis, and second, that states do object to exorbitant assertions of jurisdiction over the conduct of foreigners outside the territory of the asserting state.[6] Two main conclusions can be drawn from the practice of states: first, that a permissive basis for the exercise of such jurisdiction must be found in either treaty or customary law, and second, that these permissive bases typically evidence a 'linking point' — a connection between the regulating state and the conduct, object, or process to which the state seeks to extend its regulation.[7]

Cyberspace has not led to a fundamental reconceptualisation of the content of international law as it relates to the exercise of jurisdiction.[8] However, the global characteristics of cyberspace, alongside the increase in modalities and ease of interfering with state and individual interests across borders, influence states' understandings of the scope of jurisdictional limits and the specification of the law's application in particular cases. For instance, the concept of "vital interests" of states, which lies at the heart of the protective principle of prescriptive jurisdiction, could be engaged by a range of cyber activities with extraterritorial elements of data processing and/or effects. Similarly, the successful conduct of domestic criminal investigations might depend on cross-border access to data. Particular challenges in specifying the law's application to the ICT environment are highlighted in sections III and IV.

2.2 Types of jurisdiction

As explained by the PCIJ in the Lotus judgment, international law traditionally distinguishes between two main types of jurisdiction: prescriptive jurisdiction and enforcement jurisdiction.

Prescriptive jurisdiction, often equated with legislative authority, empowers state organs to enact, modify, and revoke binding regulations. This can occur through legislation, judicial decisions, or other binding legal instruments, depending on the state's legal system. The legal characteristics and procedures for civil enforcement differ significantly from those for criminal enforcement.

Enforcement jurisdiction pertains to the state's authority to compel compliance with its laws through its executive organs, such as the police, judiciary, and public prosecutors. Unlike prescriptive jurisdiction, which may extend beyond national borders, enforcement jurisdiction is typically restricted to the state's

6 C. Ryngaert (2008) Jurisdiction in International Law, Oxford University Press, p. 21.

7 R. O'Keefe (2004) "Universal Jurisdiction: Clarifying the Basic Concept", Journal of International Criminal Justice, 2, pp. 738.

8 See Government Offices of Sweden, Position Paper on the Application of International Law in Cyberspace (2022).

own territory. Extraterritorial enforcement is permissible with the consent of the state where the enforcement is to take place.

Prescriptive jurisdiction alone does not justify enforcement jurisdiction in another state's territory without consent. Enforcement typically requires prescriptive jurisdiction, but courts may apply foreign laws or assist in foreign judicial processes.

The practice of states concerning cyberspace activities may suggest a tension between established jurisdictional principles and the unique attributes of the digital environment. States have increasingly exercised both prescriptive and enforcement jurisdiction in cyberspace, often invoking extraterritorial reach. This has been observed in areas such as data protection, cybersecurity, and the regulation of online content. With regard to prescriptive jurisdiction, states are keen to enact laws that apply extraterritorially to regulate the behaviour of foreign entities and individuals when their actions have significant effects within the regulating state's territory. The European Union's (EU) *General Data Protection Regulation* (GDPR) is a relevant example, successfully ensuring personal data protection of data subjects against any entity processing the personal data of EU residents, regardless of the entity's location.

3. Prescriptive jurisdiction in cyberspace

Five general permissive customary principles exist in the field of jurisdiction in international law: *the territorial principle, the active personality principle, the passive personality principle, the protective principle, and the universality principle.*[9] All of them originate from state practice accepted as law. Given that the de-territorialised and virtual nature of cyberspace has made a great impact on the territoriality principle, this section will pay particular attention to its application in cyberspace.

3.1 Subjective and objective territoriality in cyberspace

Given that many states exercise prescriptive jurisdiction over conduct that starts, continues, or finishes on their territory, the territorial principle is interpreted as including both *subjective territoriality* and *objective territoriality,*[10] which follows the so-called "constituent elements" approach. Based on *objective territoriality,* a state can exercise jurisdiction if the act has taken place abroad but is completed in its territory, while a state can exercise jurisdiction based on *subjective territoriality* if the act has been initiated in the territory but is completed abroad.[11]

When it comes to cyberspace, the principle of subjective territoriality faces challenges. On the one hand, it would make *forum shopping* easier than before because the conductor has the freedom to obey the law of a state that is more beneficial to them by selecting or changing the location of data processing. For instance, the conductor can store and publish content which is illegal in their home state into another to evade strict laws and regulations. As a result, the content is accessible from the place where the conductor actually wanted it to be accessible, even if it was in violation of the laws of the country from which it was accessed.[12] On the other hand, from a technical perspective, it is not easy to identify the exact location of data processing, especially in the era of cloud computing. Data processing can be divided into numerous parts and stored respectively in different cloud servers located in different countries. It is almost a technological black box for regulators to target data processing. Due to the uncertainty of the location of conduct in cyberspace, it appears that there is increasing emphasis on objective territoriality instead of subjective territoriality. For instance, the European Union has chosen objective territoriality and other bases of jurisdiction instead of subjective territoriality in its data protection law.[13] Arguably, China also adopts objective territoriality in this field.[14]

The application of objective territoriality in cyberspace has many advantages. Firstly, the foreseeability of the application of objective territoriality is more suitable for allocating jurisdiction between states than that of subjective territoriality.

9 ILC (International Law Commission) (2006) Annual Report, A/61/10, Annex V, "Extraterritorial Jurisdiction"; Harvard Research on International Law (1935) "Draft Convention on Jurisdiction with Respect to Crime", The American Journal of International Law Supplement, pp. 445.

10 Restatement (Fourth) of US Foreign Relations Law (2018) §408, comment c.

11 C. Ryngaert (2015) Jurisdiction in International Law, Oxford University Press, pp. 78-79.

12 T. Schultz (2008) "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface", European Journal of International Law, 19(4), pp. 811.

13 General Data Protection Regulation, art 3.

14 Personal Information Protection Law of People's Republic of China, art 3.

The results of data processing can easily be identified and proved by the state on whose territory the results are produced. The results in cyberspace, for example, are recognised as the accessibility of a website, interference with computer data/system, damages to the devices, or injuries to persons. Secondly, the state that asserts jurisdiction on the basis of objective territoriality might arguably have stronger jurisdictional interests than the state that has subjective territoriality jurisdiction because the conduct of data processing can be placed on an overseas server. The country where the server is located might have little substantial interest in relation to the conduct.

3.2 The effects principle in cyberspace

As one of the grounds for exercising jurisdiction, the *effects principle* is widely accepted by many states in the field of economic law. Under this principle, a state can exercise jurisdiction with respect to conduct that has substantial effects within its territory, particularly in anti-monopoly and anti-competitive affairs.[15] Some differences exist between objective territoriality and the effects principle. We would speak of the effects principle rather than objective territoriality when no constituent element of the offence takes place within the territory of the state.[16] The conduct's *results* are one of the typical constituent elements of offences. Scholars have sometimes conflated these two principles, particularly concerning the role of effects as the constituent results element of an offence. It may be difficult to distinguish between effects, as such, and results elements in specific cases. When analysing jurisdiction under Article 3 of the GDPR, scholars often put it into the principle of effects rather than objective territoriality.[17]

Applying the effects-based principle to cyberspace poses some challenges. Historically, it is in areas like economic law — such as antitrust and securities law — that states have recognised the effects-based principle as a basis for exercising prescriptive jurisdiction. Beyond the economic field, some have questioned the application of effects-based jurisdiction.[18] Secondly, the threshold of the principle of effects is uncertain. Thus, the effects principle may prove challenging to apply for both conceptual and pragmatic reasons.[19] If the threshold of effects is unclear, it would leave a wide discretion to states. Some states exercise prescriptive jurisdiction over an intended effect even in the absence of an actual effect.[20] Courts often apply the effects principle based on their sovereign interests, especially in cyberspace where everything can be argued to affect almost everything else. This reliance on effects rather than constituent elements may raise concerns about a potential shift from the territorial principle toward universal jurisdiction.[21]

15 Restatement (Fourth) of US Foreign Relations Law (2018) §409.

16 ILC (International Law Commission) (2006) Annual Report, A/61/10, Annex V, "Extraterritorial Jurisdiction", §§11-12.

17 L. Mitrou (2017) "The General Data Protection Regulation: A Law for the Digital Age?", in T.E. Synodinou et al. (eds), EU Internet Law: Regulation and Enforcement, Springer International Publishing, pp. 32.

18 X. Song (2021) "The Systematic Structure of Extraterritorial Jurisdiction: the Distinction between Legislative Jurisdiction and Judicial Jurisdiction", Chinese Journal of Law[法学研究], 43(3), pp. 188.

19 A.L. Parrish (2008) "The Effects Test: Extraterritoriality's Fifth Business", Vanderbilt Law Review, 61(5), pp. 1478-1479.

20 Restatement (Fourth) of US Foreign Relations Law (2018) §409, reporter's note 4.

21 M. Akehurst (1973) "Jurisdiction in International Law", British Yearbook of International Law, 46, pp. 154.

3.3 Other principles

The *active personality principle* (or 'nationality' principle) refers to the jurisdiction that a state may exercise with respect to the activities of its nationals abroad.[22] This principle is universally accepted and less controversial. The latest draft of the *United Nations Convention against Cybercrime* (UNCC) also put forward that if a stateless person has a habitual residence in a state's territory, that state may also have the authority to establish its jurisdiction over his or her cybercrime.[23] Besides nationality and residence, some states have developed a control-based jurisdiction regarding the national's control over a foreign entity (e.g. a subsidiary or branch) as a genuine connection to the state, even if the foreign entity is not its national, notably in the field of ICT and data protection.[24] Since some regard this extension of jurisdiction as controversial, it needs to be further discussed.

The *passive personality principle* may be understood as referring to the jurisdiction that a state may exercise with respect to conduct abroad that injures its nationals.[25] It is mainly applied to terrorist and other organised attacks on a state's nationals by reason of their nationality or to assassinations of state diplomatic representatives or other officials.[26] According to the UNCC draft, it is suggested that a state may establish its jurisdiction when an offence is committed against a national of the state.[27] If the Convention with this provision is adopted, the passive personality principle may cover all cybercrimes in the Convention, not just traditional terrorism or other serious crimes.

The *protective principle* means that a state may exercise jurisdiction with respect to the conduct of persons or processes abroad which constitute a threat to the vital interests of a state, such as a foreign threat to its national security.[28] China adopts the protective principle in cybersecurity and data security laws. Any overseas institution, organisation, or individual that attacks, intrudes into, disturbs, destroys or otherwise damages the critical information infrastructure of China, causing any serious consequence, is subject to legal liability in accordance with the law.[29] If any entity conducting data processing activity outside the territory of China causes detriment to national security, public interest, or the lawful rights and interests of citizens and organisations of China, they are held legally liable in accordance with the law.[30]

The *universal principle* permits all states to exercise jurisdiction over certain crimes in the interest of the international community, such as genocide, war crimes, and crimes against humanity.[31] These crimes violate universal values and humanitarian principles.[32] Some divergences remain to be resolved in the definition, scope,

22 International Law Commission, Annual Report (2006), A/61/10, Annex V. Extraterritorial Jurisdiction, §14.

23 UN (United Nations) (2024) Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System), Article 22(2)(b), A/AC.291/22/Rev.3, 23 May.

24 C. Ryngaert (2015) Jurisdiction in International Law, Oxford University Press, pp. 109.

25 International Law Commission, Annual Report (2006), A/61/10, Annex V. Extraterritorial Jurisdiction, §15.

26 Ryngaert, 2015, pp. 112.

27 UN (United Nations) (2024) Convention against Cybercrime (Crimes Committed through the Use of an Information and Communications Technology System), Article 22(2)(a), A/AC.291/22/Rev.3, 23 May.

28 International Law Commission, Annual Report (2006), A/61/10, Annex V, Extraterritorial Jurisdiction, §13.

29 Cybersecurity Law of the People's Republic of China, art 75.

30 Data Security Law of the People's Republic of China, art 2.

31 International Law Commission, Annual Report (2018), A/73/10, Annex I, Universal Criminal Jurisdiction, §7.

32 Ibid, §§5-6.

and application of the universal principle.[33] For instance, it is worth discussing further whether cyberterrorism has crystallised as a crime entailing individual criminal responsibility and universal jurisdiction under custom.[34]

3.4 Navigating overlapping jurisdiction

As explained, international law recognises grounds for the extraterritorial application of state laws.[35] These grounds acknowledge the various ways in which particular conduct or processes can engage state interests in a manner that justifies extraterritorial extensions of domestic regulation. Justifiable as they may be, such grounds lead to complex questions of overlapping jurisdiction. Overlapping jurisdiction arises where more than one state can make a claim to apply their laws to particular conduct, person or process. The key question then becomes one of prioritisation of claims.

While there is no customary rule that regulates overlapping jurisdiction, there are a number of options that could be used to navigate the challenges stemming from it. For instance, states can develop practices of restraint based on a 'balance of interests' analysis. However, this approach may be too reliant on unilateral discretion. Further, states could seek to establish a hierarchy of jurisdictional grounds, though this approach has pitfalls, including that it would be difficult to establish priority rules in a non-arbitrary way. For instance, it is not always the case that the interests of the territorial state of the conduct will be those most impacted by it. Indeed, the harm might be directed externally at another state that applies its law under the protective principle. Finally, a viable way forward could be practices of treaty-based or institutional procedures for the harmonisation of state policies in the assertion of jurisdiction. However, even if states were willing to sit at the negotiating table, they would still confront the question of how to allocate the jurisdiction in specific situations. To put it differently, it is necessary to establish a general rule for allocating jurisdictions, just as private international law has done.

33 Ibid, §8.

34 K.A. Gable (2010) "Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", Vanderbilt Journal of Transnational Law, 43(1), pp. 104-108.

35 C. Staker (2018) "Jurisdiction", in M. Evans (ed.), International Law, Oxford University Press. In the context of internet governance, see D.J.B. Svantesson (2017) Solving the Internet Jurisdiction Puzzle, Oxford University Press; J. Hörnle (2021) Internet Jurisdiction Law and Practice, Oxford University Press; U. Kohl (2014) Jurisdiction and the Internet: A Study of Regulatory Competence Over Online Activity, Cambridge University Press.

4. Enforcement jurisdiction in cyberspace

Enforcement jurisdiction in cyberspace poses more intricate challenges than the application of the principles of prescriptive jurisdiction. As traditionally understood under customary law, enforcement jurisdiction is territorial, and the lawful exercise of extraterritorial enforcement jurisdiction is contingent upon either "valid consent by a foreign government to exercise jurisdiction on its territory" or "a specific allocation of authority under international law."[36] Recent state practice in cyberspace may prima facie come into tension with this customary principle, however, and suggest a rethinking of the boundaries of permissible extraterritorial enforcement.

The discussion on enforcement jurisdiction in cyberspace has focused primarily on the legality of access to data abroad by executive organs of states for the purposes of criminal investigations. Thus, to combat cybercrime, state executive bodies may require the cross-border collection of electronic evidence. How the customary rules of extraterritorial enforcement are traditionally understood may pose particular challenges in cyberspace. First, when seeking the consent of the state that stores the data or relying on traditional international cooperation, mutual legal assistance treaties (MLATs), and other forms of cross-border collaboration, the slow pace of these procedures may hamper the timely collection of electronic evidence and fail to adapt to the changeability of the digital environment. Second, the location of the data may be unknown, posing obstacles to the identification of a particular state that needs to consent. Given these difficulties, practices of cross-border data collection have emerged whereby executive bodies access extraterritorial data either directly or, more often, indirectly through the state's territorial power over intermediaries who control that data.

Given the relative paucity of such practices and state reactions to them, the following section identifies key questions related to extraterritorial enforcement jurisdiction without advancing particular views on any potential changes to customary law in the area.

4.1 The interaction between cross-border access to data and the customary regulation of enforcement jurisdiction

This section identifies five main questions of relevance to the application of the customary rule of enforcement jurisdiction to practices of cross-border access to data.

First, what does 'enforcement' mean in relation to cyberspace activities? Broadly speaking, the rules on enforcement jurisdiction are about the "limits on the executive branch of government responsible for implementing law, such as law enforcement agencies".[37] Is a state exercising enforcement jurisdiction when it issues a production order to a cloud service provider? If a state issues an order to a specific subject, this kind of jurisdiction may belong to enforcement jurisdiction. Concrete administrative acts belong to enforcement jurisdiction, and

36 Tallinn Manual 2.0 (CUP 2017), Rule 11.

37 A. Mills (2014) "Rethinking Jurisdiction in International Law", British Yearbook of International Law, 84(1), p. 187.

abstract administrative acts (administrative legislation) belong to prescriptive jurisdiction. While some academics have observed a blurring of the distinction between prescriptive and enforcement jurisdiction in relation to cyberspace activities,[38] states have not suggested such blurring in their national positions on the application of international law to cyberspace.

Second, is the rule of extraterritorial enforcement tied to state understandings of the content of other rules of international law, such as a self-standing rule of sovereignty? For instance, the national position of the Netherlands aptly points out, in the context of exercising investigative powers in a cross-border context, that "[f]rom the perspective of law enforcement (which is part of a state's internal sovereignty), the manner in which the *principle of sovereignty* should be applied has not fully crystallised".[39] If the regulation of enforcement jurisdiction is tied to other rules, such as sovereignty, non-intervention, and non-use of force, then how states specify the elements of these rules (threshold of harm, presence of subjective elements) will impact the boundaries of permissible enforcement.

Third, what does "extraterritorial" enforcement mean? Determining "extraterritoriality" may be complex. For instance, the Tallinn Manual Group of Experts considered that access to electronic data that is publicly available is to be considered territorial even if the data is hosted on servers located abroad. In their opinion, this is to be contrasted with access to data that is "stored on a private computer abroad [...] that is not meant to be accessible".[40] More research is needed in this area.

Fourth, what are the modalities for giving consent to the exercise of extraterritorial enforcement jurisdiction? Consent can be given on an ad hoc basis or ex ante through a bilateral[41] or multilateral treaty. On ad hoc consent, states may have different national procedures for its conferral. For instance, Article 24 of China's Personal Information Protection Law provides that China will process a request for personal information stored within the territory of China from a foreign judicial or law enforcement authority in accordance with applicable laws, international treaties, and agreements concluded by or acceded to China, or under the principle of equality and reciprocity. On consent in treaties, the parties to the Council of Europe Budapest Convention on Cybercrime have, by becoming parties to that agreement, given consent to the acquisition of computer data by the process set in it: a state party can "access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system' or 'access publicly available (open source) stored computer data, regardless of where the data is located geographically".[42]

Fifth, does the emerging practice observed provide evidence of the potential development of customary international law that will form a lex specialis for

38 C. Ryngaert (2023) "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts", German Law Journal, 24, p. 537, 541, 549.

39 National position of The Netherlands (2019). Emphasis added.

40 Tallinn Manual 2.0 (CUP 2017), Rule 11, paras 12-14.

41 T. Cochrane (2023) "Enforcement Jurisdiction and CLOUD Act Agreements: Clarity or Confusion?", in M. Ó Floinn et al. (eds), Transformations in Criminal Jurisdiction: Extraterritoriality and Enforcement, Hart, pp. 260-265.

42 Budapest Convention, art 32.

enforcement jurisdiction in cyberspace? It bears emphasis that, for custom to develop, there needs to be a general (sufficiently widespread, representative, and consistent) practice accepted as law.[43] While it may be too early to speak of such customary developments,[44] a close eye must be kept on the evolution of this practice.

4.2 Practices that may affect the application of enforcement jurisdiction in cyberspace: data localisation

Data localisation refers to the practice of storing and processing data within a specific geographic location. While practices of data localisation may "territorialise" data in ways that assist the determination of territorial/extraterritorial enforcement, such practices may also lead to a heavy burden of compliance, substantial barriers for free data flows, and fragmentation of data governance, among others.

Currently, China has established a fairly well-developed legal mechanism for cross-border data flow, providing three main legal tools for cross-border data flow: *security assessment, standard contract, and personal information protection certification.* The promotion to cross-border data flow and the desire for international cooperation in this field has become a general policy trend in today's China. The EU has favored the free flow of data while at the same time ensuring strict data protection laws to guarantee individuals' right to the protection of their personal data.

Given the complex dynamics between the free flow of data and data localisation, states continue to search for the right balance.

43 International Law Commission, Draft Conclusions on the Identification of Customary International Law (2018), Conclusion 8.

44 C. Ryngaert (2023) "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts", German Law Journal, 24, p. 537, 543.

5. Suggestions

As mentioned above, the customary rules of jurisdiction apply to the ICT environment. However, the question of *how* to apply jurisdiction in this environment requires further theoretical and practical exploration. Through the above research, European and Chinese colleagues have reached some fundamental consensus, and based on this consensus, we put forward the following suggestions:

First, the concept of extraterritorial jurisdiction in cyberspace needs further clarification of scope. The practice of extraterritorial jurisdiction in cyberspace may look differently across areas, from competition law through anti-corruption and financial practice to international human rights law.[45] The EU and China, as leading players, seek to reshape the understanding of cyberspace jurisdiction. Reaching global consensus will, however, inevitably take time.

Second, jurisdiction in cyberspace should avoid conflicts with existing international treaties and customary international law, including human rights law. Regarding the allocation of jurisdiction, current international law confirms the customary nature of the territorial, personality, protective, and universal principles of prescriptive jurisdiction. When considering overlapping jurisdictional claims, the principles of international comity and reciprocity, among others, should be considered, and the legality of extraterritorial jurisdiction should be carefully justified in individual cases.

Third, the construction of the extraterritorial jurisdiction system of law is not only the output of legal obligations but also the output of legal rights, especially legitimate data, due process, and other human rights. In cyberspace, when the state claims jurisdiction, it should guarantee all relevant parties are protected in accordance with domestic and international law. The legitimate rights of remote parties should be protected in judicial processes, such as through equal litigation rights of the parties and the right to obtain fair judgment.

Many areas in the topic of jurisdiction in cyberspace remain unexplored, such as cross-border access to data and gatekeeper responsibilities of digital platforms, which merit further research. This paper solidified important areas of consensus on methodology and types of jurisdiction and identified concrete legal questions that must be answered to ensure a fuller understanding of the application of customary jurisdictional rules to cyberspace.

45 N. Krisch (2022) "Jurisdiction Unbound: (Extra)territorial Regulation as Global Governance", European Journal of International Law, 33.

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-018-1