
Book Section:
Franchini, D. orcid.org/0000-0003-4948-9444 (2024) Guarding the gates and shaping the battlefield: The role of domestic courts in the settlement of international cyber disputes. In: Tsagourias, N., Buchan, R. and Franchini, D., (eds.) The Peaceful Settlement of Inter-State Cyber Disputes. Hart Publishing (Bloomsbury Publishing) , pp. 73-94. ISBN 9781509960910

PART II

Institutions

3

Guarding the Gates and Shaping the Battlefield: The Role of Domestic Courts in the Settlement of International Cyber Disputes

DANIEL FRANCHINI

I. Introduction

The digital age has witnessed a dramatic rise in disputes stemming from the use of cyberspace. These disputes, encompassing issues like internet governance, privacy and surveillance, intellectual property, and online commerce, routinely find their way into domestic courtrooms.[1] However, the extent to which domestic courts engage with *international* cyber disputes – characterised by disagreements emerging primarily between sovereign states[2] – remains a complex question. While these disputes were traditionally considered beyond the purview of domestic courts, recent developments reveal a growing entanglement between their international and domestic legal dimensions.

At its core, international dispute settlement rests with dedicated international institutions, like the International Court of Justice (ICJ), or other means of dispute settlement agreed upon by states.[3] Domestic courts, as state organs whose findings are ordinarily confined within their national legal systems, seem ill-equipped

[1] See, in general, A Murray, *Information Technology Law: The Law and Society*, 5th edn (Oxford, Oxford University Press, 2023). See also Master of the Rolls, 'The Economic Value of English Law in Relation to DLT and Digital Assets' (25 July 2022) www.judiciary.uk/speech-by-the-master-of-the-rolls-the-economic-value-of-english-law-in-relation-to-dlt-and-digital-assets.

[2] See *Mavrommatis Palestine Concessions* (*Greece v Great Britain*) (Judgment of 30 August 1924) [1924] PCIJ Rep Series A No 2, 11; *Right of Passage Over Indian Territory (Portugal v India)* (Merits, Judgment) [1960] ICJ Rep 6, 34; *South West Africa Cases* (*Ethiopia v South Africa*; *Liberia v South Africa*) (Preliminary Objections, Judgment of 21 December 1962) [1962] ICJ Rep 319, 328. In line with the approach adopted by this book, the terms 'inter-state' and 'international' disputes will be used interchangeably. See Tsagourias (ch 1 in this volume) and Antonopoulos (ch 4 in this volume).

[3] On the principle of consent, see *Status of Eastern Carelia* (Advisory Opinion of 23 July 1923) [1923] PCIJ Rep Series B No 5, 27; *Fisheries Jurisdiction* (*Spain v Canada*) (Jurisdiction, Judgment of

to tackle inter-state conflicts. Principles of international law, like state immunity, further shield states from the jurisdiction of foreign courts,[4] seemingly reinforcing the divide.

However, this stark separation is increasingly challenged. The permeability of domestic legal systems to international legal norms has blurred the lines and domestic courts are increasingly tasked with interpreting and applying international law. As a result, domestic courts are vested with an 'international judicial function'.[5] They can act as 'enforcers' of international norms within their legal systems, for instance, when striking down or disapplying legislation or executive acts in violation of international law.[6] This can also occur when domestic courts do not directly apply international law but rely on domestic law provisions that reflect international legal standards.[7] In addition, although from a formal standpoint, they are 'merely facts which express the will and constitute the activities of States',[8] domestic courts' decisions can greatly impact the development of international law. They may confirm existing rules of custom through consistent application, or they may introduce novel interpretations, which in turn may spur reactions from other organs of the state or other states and ultimately shape the content of these rules.[9]

The international judicial function of domestic courts becomes particularly crucial in the context of international cyber disputes, where a tapestry of international legal norms – from human rights to international economic law – is often woven into the fabric of the conflict. Moreover, domestic courts frequently serve as the initial point of contact for individuals and corporations affected by cyber-attacks or other wrongful conduct in cyberspace – a role whose importance is heightened by the current absence of a centralised mechanism for compulsory settlement of international cyber disputes.

As a result of these dynamics, this chapter argues that domestic courts have a significant role to play in the settlement of international cyber disputes, both

4 December 1998) [1998] ICJ Rep 432 para 56; *Obligation to Negotiate Access to the Pacific Ocean* (*Bolivia v Chile*) (Judgment of 1 October 2018) [2018] ICJ Rep 507 para 165; UNGA, 'Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations' (24 October 1970) UN Doc A/RES/2625(XXV) (the Friendly Relations Declaration) para 5; UNGA, 'Manila Declaration on the Peaceful Settlement of International Disputes' (15 November 1982) UN Doc A/RES/37/10 (the Manila Declaration) para 3.

[4] On state immunity, see section III.A below.

[5] A Tzanakopoulos, 'Domestic Courts in International Law: The International Judicial Function of National Courts' (2011) 34 *Loyola of Los Angeles International and Comparative Law Journal* 133. See also International Law Association, 'Study Group on Principles on the Engagement of Domestic Courts with International Law: Final Report' (2016) www.ila-hq.org/en_GB/documents/conference-study-group-report-johannesburg-2016 paras 10–15; A Nollkaemper, *National Courts and the International Rule of Law* (Oxford, Oxford University Press, 2011) 6.

[6] Tzanakopoulos (n 5) 166; Nollkaemper (n 5) 6–9.

[7] Tzanakopoulos refers to these as 'consubstantial norms'; see Tzanakopoulos (n 5) 163.

[8] *Case Concerning Certain German Interests in Polish Upper Silesia (Germany v Poland)* (Merits, Judgment of 25 May 1926) [1926] PCIJ Rep Series A No 7, 19.

[9] See A Tzanakopoulos and CJ Tams, 'Introduction: Domestic Courts as Agents of Development of International Law' (2013) 26 *Leiden Journal of International Law* 531, 538–9.

'internally' with respect to the acts of the forum state and 'externally' concerning the acts of other states. Section II will focus on the internal function of domestic courts as 'guardians' of their state's international obligations in cyberspace and 'gatekeepers' with respect to international cyber disputes. In this sense, domestic courts can pre-empt international disputes by ensuring compliance with relevant international legal norms. Section III then shifts to the external function, analysing how domestic court judgments can shape international cyber disputes to which their states are parties. By contributing to articulating the legal reasoning behind the government's action, judicial pronouncements can advance claims against other states, influence diplomatic exchanges, and even, in certain instances, contribute to the settlement of international disputes. Finally, section IV will conclude by reflecting on the potential benefits and challenges of domestic courts' engagement with international cyber disputes, offering insights into the future trajectory of this evolving legal landscape.

II. Internal Engagement: Domestic Courts as 'Gatekeepers' of International Cyber Disputes of the Forum State

Domestic courts have a central role in 'moderating' international disputes that revolve around the forum state's compliance with its international obligations. This is because they represent the final avenue within a state where international law can be upheld, thus averting the engagement of the international responsibility of the state.[10] The significance of this role is further accentuated by the principle of exhaustion of local remedies, wherein individuals or entities affected by a state's internationally wrongful act must pursue all available domestic legal channels before escalating the dispute to the international legal plane.[11]

This section delves into two ways domestic courts internally engage with international cyber disputes. As reactive gatekeepers, domestic courts act as checks and balances against other state organs, reviewing and enforcing legislative and executive acts in cyberspace. Domestic courts can nip potential international disputes in the bud by ensuring these acts comply with international law. In other cases, international obligations demand proactive action by domestic courts. Failure to exercise their jurisdiction in these situations – for instance, in combating cybercrime or protecting human rights online – can trigger international responsibility for the state and risk escalating issues into full-blown disputes. Both scenarios are examined in turn.

[10] See Tzanakopoulos (n 5) 174.

[11] See Art 14 in ILC, 'Draft Articles on Diplomatic Protection, with Commentaries. UN Doc A/61/10' in *Yearbook of the International Law Commission. 2006, Volume II, Part Two: Report of the Commission to the General Assembly on the Work of its Fifty-Eighth Session* (New York, UN, 2006) 44.

A. Domestic Courts' Oversight of Legislative and Executive Acts in Cyberspace

The rise of digital technologies has significantly bolstered the capacity of government agencies to enact measures that could potentially infringe upon the rights of individuals and entities globally. The disclosure by Wikileaks in June 2013 of the involvement of the US National Security Agency (NSA) in a global surveillance program harvesting confidential online information, spotlighted this concern.[12] Domestic courts have the potential to serve as a crucial first line of defence against abuses of state power in cyberspace, although certain limitations on the courts' ability to hear these cases exist.[13] When scrutinising surveillance programs and intelligence-gathering initiatives, domestic courts should be capable – at least in principle – of ensuring their alignment with the international obligations of the forum state, especially in guaranteeing that these programs adhere to adequate international standards of ex ante and ex post oversight.[14] As examined in the next section, this type of judicial review may, in turn, be mandated by international law when human rights are at stake.[15]

Although domestic courts may not be able to review all law enforcement activities in the digital realm, they play a crucial role in defining the limits of state jurisdiction in cyberspace. The increasing fluidity and contested nature of jurisdictional boundaries are fuelled by the seamless flow of data across borders and its accessibility from anywhere in the world.[16] Traditionally, the rules of customary international law on state jurisdiction have been anchored in territoriality, granting states undisputed authority to regulate activities within their borders.[17] Furthermore, states may exercise extraterritorial jurisdiction under specific circumstances when a direct and substantial connection exists between the state and the regulated activity

[12] For an overview of Edward Snowden's revelations over the NSA programme, see E MacAskill and G Dance, 'NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained' (*The Guardian*, 1 November 2013) www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.

[13] See M Rumold, 'Regulating Surveillance through Litigation: Some Thoughts from the Trenches' in D Gray and SE Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge, Cambridge University Press, 2017) 579.

[14] See I Brown and D Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' (2014) 3 *European Human Rights Law Review* 243; A Deeks, 'An International Legal Framework for Surveillance' (2015) 55 *Virginia Journal of International Law* 291; C Forcese, 'One Warrant to Rule Them All: Re-conceiving the Judicialization of Extraterritorial Intelligence Collection' (*Ottawa Faculty of Law Working Paper No 2015-41*, 2015) ssrn.com/abstract=2622606; G Malgieri and P De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges' in D Gray and SE Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge, Cambridge University Press, 2017) 509.

[15] See section II.B below.

[16] U Kohl, 'Jurisdiction in Network Society' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace*, 2nd edn (Cheltenham, Edward Elgar, 2021) 69.

[17] See C Ryngaert, *Jurisdiction in International Law*, 2nd edn (Oxford, Oxford University Press, 2015) 42.

('prescriptive jurisdiction').[18] However, the lawful enforcement of such regulations remains confined to the state's territory ('enforcement jurisdiction').[19]

Applying the principle of territoriality to online activities raises considerable difficulties.[20] Algorithms often determine the location of data stored by multinational cloud service providers, meaning the location of the data can be uncertain. Solely relying on server location to determine jurisdictional entitlements could be overly restrictive and potentially arbitrary.[21] Indeed, states have consistently rejected this approach.[22] Significantly, however, though free to assert prescriptive jurisdiction based on factors other than territory, states have continued to rely on some forms of territoriality to justify jurisdiction in cyberspace.[23]

In particular, states have frequently advanced regulatory claims over cyber activities based on what Kohl has defined as the 'destination approach'.[24] According to this approach, jurisdiction is claimed based on the impact or effect of the online activity. However, there is some disagreement regarding the extent to which these effects must be felt within the state's territory.[25] The interesting aspect of the dynamics by which this practice is emerging is that, for the most part, it has been spearheaded by decisions of domestic courts.

The landmark *LICRA v Yahoo!* case, one of the earliest high-profile cases to adopt the destination approach, exemplifies this.[26] A French court held that France was entitled to apply its laws prohibiting the sales of Nazi memorabilia to Yahoo!'s .com site, even though it was hosted in the USA, simply by virtue that the site was accessible in France and caused harm there. Recent years have seen a parallel trend in US courts. In a trademark infringement case, the Court of Appeals for the First Circuit, overturning the district court's decision, asserted jurisdiction over Scrutinizer, a German company, citing its global web-based services that attracted numerous US customers.[27] Similarly, the Court of Appeals for the Fourth Circuit established jurisdiction over Russian music piracy websites, considering

[18] Alongside territoriality, other principles of jurisdiction include nationality, passive personality, universality, and the protective principle; see Ryngaert (n 17) 85ff. See also B Oxman, 'Jurisdiction of States' in *Max Planck Encyclopedia of Public International Law* (Oxford, Oxford University Press, 2007) [10]; J Crawford, *Brownlie's Principles of Public International Law*, 9th edn (Oxford, Oxford University Press, 2019) 442.

[19] See *Case of the SS 'Lotus'* (*France v Turkey*) (Judgment of 7 September 1927) [1927] PCIJ Rep Series A No 10, 18–19; Crawford (n 18) 462.

[20] See DJB Svantesson, 'A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft' (2015) 109 *American Journal of International Law Unbound* 69, 70.

[21] C Ryngaert, 'Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts' (2023) 24 *German Law Journal* 537, 548.

[22] Kohl (n 16) 89.

[23] See Ryngaert (n 21) 538.

[24] Kohl (n 16) 78.

[25] For instance, whether mere accessibility of online content from within the state is sufficient; see Kohl (n 16) 78.

[26] *LICRA v Yahoo! Inc & Yahoo France* (Tribunal de Grande Instance de Paris, 22 May 2000).

[27] *Plixer Int'l, Inc v Scrutinizer GmbH* 905 F 3d 1, 4 (1st Cir 2018).

the significant number of US visitors and personalised advertisements targeting US customers on the sites.[28]

These cases underscore the pivotal role of domestic courts in scrutinising and enforcing claims of jurisdiction in cyberspace. Domestic legislation, such as French laws against the promotion of Nazism or US trademark laws, is typically drafted in broad terms without specific provisions regarding its application to cyberspace. Consequently, domestic courts often grapple with defining the precise scope of these laws, thereby clarifying the jurisdictional claims of one state in relation to the conflicting claims of others. Depending on the type of remedy they issue – for instance, takedown or search orders – domestic courts' pronouncements may also include a component of enforcement jurisdiction, which has proven especially contentious when applied to the internet.[29] Thus, domestic courts' decisions frequently become critical milestones in either sparking or preventing international disputes concerning jurisdiction in cyberspace.[30]

The *Microsoft Ireland* case showcases the diverse roles domestic courts may play in this regard.[31] In the context of a US drug enforcement investigation, a warrant compelled Microsoft to disclose a customer's electronic communications stored on servers outside the US. Microsoft contested the warrant, arguing that, as the data was stored in Ireland, it fell outside the scope of the Stored Communications Act (SCA), the statute underlying the warrant. Prior to this dispute reaching US courts, there was uncertainty about the application of the SCA to data stored beyond US borders. A district court judge initially ruled against Microsoft,[32] precipitating a jurisdictional conflict between the US and the state where the data was located (Ireland) and potentially triggering a bilateral (cyber) dispute between the two states.[33] On appeal, however, the Court for the Second Circuit reversed the district court's decision, finding that the SCA did not have extraterritorial application.[34] This decision 'rectified' the previous assertion

[28] *UMG Recordings, Inc v Kurbanov* 963 F 3d 344 (4th Cir 2020).

[29] See Ryngaert (n 21) 539. For the idea that adjudicative jurisdiction may include the exercise of enforcement jurisdiction, see ST Mouland, 'Rethinking Adjudicative Jurisdiction in International Law' (2019) 29 *Washington International Law Journal* 173, 184.

[30] This divergence in outcomes can also be attributed to the fact that different domestic courts may reach varying conclusions on the same international law issues. For instance, following the French judgment in the *Yahoo!* case, a US district court determined it could not be enforced in the US due to its inconsistency with the First Amendment to the US Constitution regarding freedom of expression; see *Yahoo! Inc v La Ligue Contre le Racisme et l'Antisemitisme* 145 F Supp 2d 1168, 1180 (ND Cal 2001). This decision was later reversed by the Appeal Court; see *Yahoo! Inc v La Ligue Contre le Racisme et L'Antisemitisme* 433 F 3d 1199 (9th Cir 2006).

[31] *Matter of Warrant to Search a Certain E-Mail Acct Controlled & Maintained by Microsoft Corp* 829 F 3d 197 (2d Cir 2016), vacated and remanded sub nom. *United States v Microsoft Corp* 138 S Ct 1186, 200 L Ed 2d 610 (2018).

[32] *In re Warrant to Search a Certain E-Mail Acct Controlled & Maintained by Microsoft Corp* 15 F Supp 3d 466, 471 (SDNY 2014).

[33] *cf* Tzanakopoulos (n 5) 168.

[34] *Matter of Warrant to Search a Certain E-Mail Acct Controlled & Maintained by Microsoft Corp* 829 F 3d 197, 222 (2d Cir 2016).

of jurisdiction by limiting its extraterritorial reach, thereby preventing the escalation of the international dispute.[35]

Both rulings were based on divergent interpretations of domestic law. However, the presence of an international dispute became apparent following the Appeal Court's decision. As the case advanced to the Supreme Court, third parties, including Ireland and other foreign states affected by the litigation, submitted amici curiae briefs. Ireland expressed concerns about potential infringements on its sovereign rights in its submission. It argued that data stored on Irish servers should be accessed through the proceedings prescribed under the Ireland-US Mutual Legal Assistance Treaty (MLAT).[36] Conversely, the UK filed a brief arguing that the geographic storage location of data should not be the primary factor when determining whether a state should gain access to communications located abroad but accessible domestically.[37] The EU, in its submission, emphasised that, in any event, comity considerations would necessitate an analysis of potential conflicts with foreign laws, including the General Data Protection Regulation.[38]

Under these circumstances, the US Supreme Court was tasked with a dual role: interpreting the SCA domestically while considering its impact on the international legal plane. Depending on its interpretation, the Court could either exacerbate or prevent a dispute with other states. Although not bound to align with foreign states' claims, the Supreme Court had interpretative tools such as the presumption against extraterritoriality, the principle of comity, and the *Charming Betsy* doctrine to ensure that its interpretation of domestic law remained consistent with international law and minimised conflict with other states.[39] Ultimately, the case was withdrawn before the Supreme Court reached a verdict. However, this case illustrates how, in certain situations, domestic courts may function akin to international dispute settlement bodies, crafting interpretations that balance competing sovereign interests.

Beyond the specific dispute at hand, domestic litigation can also stimulate initiatives to settle future disputes arising from similar facts, especially when legislative and executive organs are better placed to offer these. The *Microsoft Ireland* case was crucial in prompting the US Congress to enact the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018.[40] This legislation overhauled

[35] In a similar way, see more recently T Cochrane, '*KBR v SFO*: the United Kingdom's Microsoft Ireland?' (*Just Security*, 25 February 2021) www.justsecurity.org/74875/kbr-v-sfo-the-united-kingdoms-microsoft-ireland.

[36] *United States of America v Microsoft Corporation*, Brief for Ireland as Amicus Curiae in Support of Neither Party (13 December 2017) 2017 WL 6492481.

[37] *In re Microsoft Corporation*, Brief of the Government of the United Kingdom of Great Britain and Northern Ireland as Amicus Curiae in Support of Neither Party (13 December 2017) 2017 WL 6398769.

[38] *In re Microsoft Corporation*, Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party (13 December 2017) WL 6383224.

[39] CA Bradley, *International Law in the US Legal System*, 2nd edn (Oxford, Oxford University Press, 2015) 10–20.

[40] See US Department of Justice (DOJ), 'CLOUD Act Resources' (24 October 2023) www.justice.gov/criminal/cloud-act-resources.

the system for accessing electronic information held by US-based global internet providers, clarifying rules for US law enforcement while authorising bilateral executive agreements to streamline cross-border data access for foreign governments. The CLOUD Act can thus be seen as key in pre-empting the emergence of future international cyber disputes on this matter, with the US having already concluded agreements with the UK[41] and Australia,[42] and other states expected to follow suit.[43]

In sum, domestic courts play a critical role as gatekeepers of legality in cyberspace, acting against state overreach, defining jurisdictional boundaries, and even facilitating international dispute settlement. By interpreting domestic law with international considerations in mind and encouraging further solutions, domestic courts can help promote the rule of law in cyberspace and prevent the escalation of conflicts between states.

B. Domestic Courts' Role in Fulfilling International Law Obligations in Cyberspace

Some obligations that states are subject to when operating in cyberspace necessitate active involvement from domestic courts for their fulfilment. Notably, domestic courts play a central role in realising obligations related to suppressing certain malicious cyber operations. Failure to exercise adjudicative jurisdiction in these circumstances will trigger the international responsibility of the forum state and is bound to generate international disputes.

The rise in criminal activities through information and communications technology (ICT) has led to the establishment of several international legal instruments to suppress 'cybercrime'.[44] Chief among them is the 2001 Convention on Cybercrime (Budapest Convention), drafted under the auspices of the Council of

[41] US DOJ, 'Cloud Act Agreement between the Governments of the US, United Kingdom of Great Britain and Northern Ireland' (3 October 2019) www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern. See J Daskal and P Swire, 'The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards' (*Just Security*, 8 October 2019) www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safeguards.

[42] US DOJ, 'Cloud Act Agreement between the Governments of the US and Australia' (15 December 2021) www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-and-australia.

[43] See, eg, US DOJ, 'United States and Canada Welcome Negotiations of a CLOUD Act Agreement' (22 March 2022) www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement. These agreements can be seen as an alternative to regulations arising from EU law; see M Rojszczak, 'CLOUD Act Agreements from an EU Perspective' (2020) 38 *Computer Law and Security Review* 1.

[44] See United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Vienna, UN, 2013); P Kastner and F Mégret, 'International Legal Dimension of Cybercrime' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace*, 2nd edn (Cheltenham, Edward Elgar, 2021) 254.

Europe but open to virtually all states.[45] Under this and other conventions that follow the same structure, State Parties are obligated to 'adopt such legislative and other measures as may be necessary to establish jurisdiction' over a number of cyber-offences.[46] In certain circumstances, they are also obligated to exercise adjudicative jurisdiction for the purpose of prosecuting an alleged offender. According to Article 24(6):

> If extradition for a criminal offence … is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.[47]

In other words, State Parties where the accused is found have a choice between submitting the case to their prosecuting authorities or extraditing the individual to a state willing to prosecute.[48] However, as the ICJ clarified, extradition is an option, while prosecution remains an international obligation whose violation constitutes a wrongful act engaging the responsibility of the state.[49] Thus, in conventions using this language, State Parties have a primary duty to prosecute, involving the exercise of domestic court jurisdiction.

Given the transnational nature of cybercrime, international legal instruments dedicated to its suppression also impose obligations concerning inter-state cooperation.[50] Article 25(1) of the Budapest Convention, for instance, mandates State Parties to provide mutual assistance for investigations or proceedings related

[45] Convention on Cybercrime (Budapest, 23 November 2001) ('Budapest Convention'). As of December 2023, the Budapest Convention has 68 Parties and 23 states have signed it or been invited to accede.

[46] See Budapest Convention, Art 22; Arab Convention on Combating Information Technology Offences (Cairo, 21 December 2010), Art 5 ('Arab Convention'); Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L218/8, Arts 3–8.

[47] See also Budapest Convention, Art 22(3); Arab Convention, Art 30(2).

[48] See K Kittichaisaree, *The Obligation to Extradite or Prosecute* (Oxford, Oxford University Press, 2018) 179.

[49] *Questions Relating to the Obligation to Prosecute or Extradite (Belgium v Senegal)* (Judgment of 20 July 2012) [2012] ICJ Rep 422 para 95.

[50] See, eg, Budapest Convention, Arts 23, 25, 27; Arab Convention, Arts 32, 34–35; Commonwealth of Independent States' Agreement on Cooperation in Combating Offences Related to Computer Information (Minsk, 1 June 2001) Arts 5–6; Agreement among the Governments of the Shanghai Cooperation Organization's Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009). Cooperation duties can also derive from agreements concerning the suppression of other offences; see, eg, International Convention for the Suppression of Terrorist Bombings (New York, 15 December 1997) Art 10. Several states have also concluded mutual legal assistance treaties (MLATs), making assistance between two states in criminal matters obligatory under international law; see B Zagarism, 'United States Treaties on Mutual Assistance in Criminal Matters' in M Cherif Bassiouni (ed), *International Criminal Law, Volume 2: Multilateral and Bilateral Enforcement Mechanisms* (Brill, Nijhoff, 2008) 385.

to criminal offences in cyberspace. This cooperation extends to the judicial authorities of the relevant states, particularly when judicial pronouncements are required for evidence production or the seizure and forfeiture of criminal assets.[51] When judicial cooperation forms part of the international obligations of a state, failure by its domestic courts to exercise jurisdiction – for instance, failure to respond to a request for mutual legal assistance under MLAT[52] – will once again engage the international responsibility of the state and likely lead to the emergence of international disputes.

Beyond specific treaty obligations, the question arises as to whether the exercise of domestic court jurisdiction for the suppression of cybercrime may be compelled by a general rule of custom, particularly in the context of a broader discussion on the existence of a duty of 'cyber due diligence' under international law.[53]

According to the *Tallinn Manual 2.0*, '[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States'.[54] This perspective aligns with the views of several states and scholars, arguing in support of the existence of binding due diligence obligations in cyberspace.[55] However, the acceptance of this stance is not universal and remains a subject of ongoing debate.

In its 2021 Report, the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security identified due diligence as part of a set of 'voluntary, non-binding norms

[51] For an example of a complex transnational operation to take down the infrastructure of malware and a botnet involving the judicial authorities of several states, see US DOJ, 'Emotet Botnet Disrupted in International Cyber Operation' (28 January 2021) www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

[52] For a discussion of the current MLAT system and the potential scope of proposed reforms, see J Daskal, 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues' (2015) 8 *Journal of National Security Law and Policy* 473; P Swire, 'Why Cross-Border Government Requests for Data Will Keep Becoming More Important' (*Lawfare*, 23 May 2017) www.lawfaremedia.org/article/why-cross-border-government-requests-data-will-keep-becoming-more-important.

[53] See K Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' (2014) 14 *Baltic Yearbook of International Law* 23, 23; MN Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) *The Yale Law Journal Forum* 68; R Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 *Journal of Conflict and Security Law* 429; J Kulesza, *Due Diligence in International Law* (Leiden, Brill Nijhoff, 2016); A Coco and T De Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law' (2021) 32 *European Journal of International Law* 771; J Kenny, 'Cyber Operations and the Status of Due Diligence Obligations in International Law' (2023) 73 *International and Comparative Law Quarterly* 135.

[54] Rule 6, in MN Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd edn (Cambridge, Cambridge University Press, 2017) 30.

[55] See, among others, Ministry of Armed Forces of France, 'Droit International Appliqué aux Opérations dans le Cyberspace' (2019) www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf 6–7; Federal Government of Germany, 'On the Application of International Law in Cyberspace. Position Paper' (March 2021) www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf 3; Italian Ministry for Foreign Affairs and International Cooperation, 'Italian Position Paper on International

of responsible State behaviour', stating that 'States *should* not knowingly allow their territory to be used for internationally wrongful acts using ICTs'.[56] Similarly, despite extensive discussion on the topic, the 2021 Final Report of the UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security failed to include any language on due diligence obligations due to the lack of consensus among states.[57] These, among other factors, have raised doubts about the existence of a customary duty of cyber due diligence under international law.[58]

Even if one accepts the existence of a customary international obligation of due diligence in cyberspace, there is ambiguity about its content. The *Tallinn Manual 2.0* states that compliance with the due diligence principle requires a state to take feasible measures to end cyber operations on its territory that adversely affect another state's rights.[59] According to the Manual, however, this duty does not extend to preventative measures,[60] '[n]or is there any obligation under the due diligence principle for the State to prosecute those engaging in the underlying cyber operations; rather, the obligation is limited to taking feasible measures to terminate the operations'.[61]

Divergent opinions exist among scholars on this matter. According to Buchan, the principle of cyber due diligence includes not only an obligation to prevent, but also 'a duty to investigate and, where appropriate, punish those responsible because such conduct serves "a critical preventative function by reinforcing the state's prohibitory measures and deterring other potential wrongdoers"'.[62] Similarly, Bannelier-Christakis found that measures to prevent and punish cyber

Law and Cyberspace' (2021) www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf 6–7. For a full list, see NATO Cooperative Cyber Defence Centre of Excellence et al, 'International Cyber Law: Interactive Toolkit. Due Diligence' cyberlaw.ccdcoe.org/wiki/Due_diligence. In the literature, see Schmitt (n 53) 80; Buchan (n 53) 451; Kulesza (n 53) 300–02; Coco and De Souza Dias (n 53) 774.

[56] UNGA, '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 (2021 GGE Report) 10, 17. See also Schmitt (n 53) 73.

[57] UNGA, 'Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' (10 March 2021) UN Doc A/AC.290/2021/CRP.2.

[58] See, eg, UK Foreign, Commonwealth and Development Office, 'Application of International Law to States' Conduct in Cyberspace: UK Statement' (3 June 2021) 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 para 12; Government of Canada, 'International Law Applicable in Cyberspace' (April 2022) www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx para 26; R Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 *International Law Studies* 395, 403–44. See also Kenny (n 53) 156.

[59] Schmitt (n 54) 43.

[60] ibid 44–45.

[61] ibid 48.

[62] Buchan (n 53) 442, citing *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Judgment of 20 April 2010) [2010] ICJ Rep 14 para 158.

acts contrary to the rights of other states are '*one of the best ways* to implement the "due diligence" obligation'.[63]

This conclusion gains further weight when considering malicious cyber activities with harmful effects on specific human rights, such as cyberbullying, defamation, and hate speech.[64] International human rights law imposes both negative and positive duties on states, requiring them not only to refrain from violating human rights but also to take reasonable measures to protect individuals from threats posed by various entities according to a due diligence standard.[65] Even if a general due diligence obligation remains disputed, specific human rights obligations often imply due diligence requirements to prevent, halt, and remedy harms in cyberspace.[66] These may involve providing civil remedies and criminal provisions to facilitate effective investigations and prosecutions of human rights violations.[67]

In *KU v Finland*,[68] the European Court of Human Rights (ECtHR) exemplified this with respect to the right to private and family life under Article 8 of the European Convention on Human Rights. The case involved a false online advertisement using a child's name on a dating site. When Finnish courts failed to compel the internet service provider to disclose the perpetrator's identity, the ECtHR found a violation of the petitioner's rights, emphasising:

> States have a positive obligation inherent in Article 8 of the Convention to criminalise offences against the person, including attempted offences, and to reinforce the deterrent effect of criminalisation by applying criminal-law provisions in practice through effective investigation and prosecution.[69]

In essence, when confronted with malicious cyber activities prohibited under certain treaties or at least when these activities have detrimental effects on certain human rights, the involvement of domestic courts extends beyond being an opportunity for states to rectify wrongful acts; it becomes a substantive step

[63] Bannelier-Christakis (n 53) 35, drawing support for this duty from *Corfu Channel* (*United Kingdom of Great Britain and Northern Ireland v Albania*) (Merits, Judgment of 9 April 1949) [1949] ICJ Rep 4, 19–20.

[64] Coco and De Souza Dias (n 53) 795–97.

[65] See UN Human Rights Committee, 'General Comment No 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13 para 8; S Besson, 'Due Diligence and Extraterritorial Human Rights Obligations – Mind the Gap!' (2020) 9 *ESIL Reflections* 1, 2.

[66] See G Rona and L Aarons, 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace' (2016) 8 *Journal of National Security Law and Policy* 503, 516–22; Coco and De Souza Dias (n 53) 796.

[67] See, eg, UN Human Rights Committee, 'General Comment No 31 [80]' UN Doc CCPR/C/21/Rev.1/Add.13 paras 15, 18; UN Human Rights Committee, 'General Comment No 36. Article 6: Right to Life' (3 September 2019) UN Doc CCPR/C/GC/35 paras 27–28.

[68] *KU v Finland* App No 2872/02 (ECtHR, 2 March 2009).

[69] ibid para 46, citing *MC v Bulgaria* App No 39272/98 (ECtHR, 4 December 2003) para 150.

mandated to comply with international law. Domestic courts, therefore, play a crucial role in minimising the risk of international disputes across a diverse range of circumstances.

III. External Engagement: Domestic Courts' Contribution to Shaping International Cyber Disputes with Other States

Alongside their role as 'gatekeepers' of international cyber disputes, domestic courts may also shape international cyber disputes between their state and other states. Their direct involvement in international cyber disputes is, however, complex due to two sets of constraints: one imposed by international law and the other arising from considerations of comity and judicial propriety.

International law purports to set clear boundaries for the permissible actions of states, including limitations on their jurisdiction over matters affecting other sovereign entities. Principles like state jurisdiction and state immunity play a fundamental role in shielding states from unilateral actions by other states' domestic courts. Additionally, domestic courts often employ various 'avoidance techniques' to avoid potentially contentious inter-state issues.[70] These techniques, such as the act of state doctrine and the political question doctrine, act as procedural shields, deflecting the need for domestic courts to engage with international disputes.

However, when domestic courts are able to engage with inter-state cyber disputes, their action can be transformative. By articulating the state's claims concerning the legal qualifications of the relevant cyber activity, they effectively define the national position on the matter. These claims, in turn, can be 'positively opposed' by other states, laying the groundwork for a formal dispute.[71] In this sense, domestic courts can be seen as catalysts, allowing nascent international cyber disagreements to 'mature' into fully-fledged disputes between sovereign states.[72] Moreover, the pressure exerted through domestic litigation can serve as an incentive for negotiated settlements, encouraging states to resolve the dispute through one of the available means of dispute settlement.

Examples of this dynamic can be observed in two scenarios: the US 'indictment strategy' against foreign state actors involved in alleged cyberattacks, and domestic legal proceedings against private contractors accused of participating in such operations. Both examples will be examined in turn.

[70] See E Benvenisti, 'Judicial Misgivings Regarding the Application of International Law: An Analysis of Attitudes of National Courts' (1993) 4 *European Journal of International Law* 159.
[71] See *South West Africa Cases* (n 2) 328.
[72] See Tzanakopoulos (n 5) 168.

A. The US Indictment Strategy as a Tool for Domestic Courts' Engagement with International Cyber Disputes

Since 2014, the US Department of Justice (DOJ) has employed an 'all-tool approach' to counter cyberattacks allegedly perpetrated by foreign state actors.[73] This approach includes issuing indictments against individual hackers and officials allegedly affiliated with foreign governments, often as part of a broader strategy to pressure and engage with those states on cyber issues.[74] This 'indictment strategy' was first employed against five members of the Chinese People's Liberation Army (PLA), accused of hacking into the computer systems of American corporations and stealing trade secrets.[75] Subsequently, the number of indictments issued by the DOJ against alleged state-sponsored hackers has surged, covering a spectrum of malicious cyber activities globally.[76]

The indictments themselves rarely lead to actual prosecutions in US courts, as the targeted individuals are often beyond the reach of US enforcement agencies. Instead, they act primarily as 'speaking indictments', revealing important

[73] J Carlin, 'Remarks at the National Cyber-Forensics and Training Alliance' (23 September 2015) www.justice.gov/opa/speech/assistant-attorney-general-john-carlin-delivers-remarks-national-cyber-forensics-and.

[74] See CI Keitner, 'Attribution by Indictment' (2019) 113 *American Journal of International Law Unbound* 207; G Hinck and T Maurer, 'Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity' (2020) 10 *Journal of National Security Law and Policy* 525, 525; H Lee, 'Public Attribution in the US Government: Implications for Diplomacy and Norms in Cyberspace' (2023) 6 *Policy Design and Practice* 198, 204–05.

[75] US DOJ, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage' (19 May 2014) www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor. See J Goldsmith and RD Williams, 'The Failure of the United States' Chinese-Hacking Indictment Strategy' (*Lawfare*, 28 December 2018) www.lawfaremedia.org/article/failure-united-states-chinese-hacking-indictment-strategy.

[76] See C Cimpanu, 'DOJ Explains Recent Wave of Cyber-Espionage-Related Indictments' (*ZDNet*, 5 October 2018) www.zdnet.com/article/doj-explains-recent-wave-of-cyber-espionage-related-indictments/. Recent examples include: US DOJ, 'Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research' (21 July 2020) www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion; US DOJ, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace' (19 October 2020) www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and; US DOJ, 'Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe' (17 February 2021) www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and; US DOJ, 'Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research' (19 July 2021) www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion; US DOJ, 'Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide' (24 March 2022) www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

details of the malicious cyber operations to the public.[77] As argued by Hinck and Maurer, these serve multiple purposes, including attributing malicious activity to specific actors, disrupting hacker networks, coordinating with other US government agencies, providing restitution to victims and defenders, pressuring states to cease future attacks, and supporting the development of robust cyber norms.[78] Similarly, Keitner identified three functions served by the US indictment strategy. First, these indictments have a coercive function, as information gleaned through forensic investigations may form the basis for other governmental actions, such as the imposition of economic sanctions.[79] Second, they serve as a deterrent purpose by showcasing US capabilities in detecting potential cyber wrongdoers.[80] Third, these indictments possess an expressive function, enabling the USA to define and communicate standards of behaviour in cyberspace.[81]

The effectiveness of the indictment strategy as a tool for confronting international cyber threats remains a matter of debate. Critics argue its impact is limited, citing examples of Chinese state-affiliated hackers being charged without leading to any meaningful deterrence of cyber theft.[82] Some suggest alternative methods, such as disruption and sanctions, may be more effective.[83] Proponents, including former US Assistant Attorney General John Carlin, contend that the indictment strategy, as part of a comprehensive approach, is vital for disrupting and deterring state-sponsored hacking.[84]

Be that as it may, the decision to address malicious cyber operations through domestic criminal law proceedings, as opposed to or in conjunction with diplomatic demarches, sanctions, or other avenues,[85] holds significant weight. Criminal charges demand a high standard of evidence, requiring federal prosecutors to convince a grand jury or a federal judge of probable cause and later prove guilt 'beyond a reasonable doubt' before a jury.[86] Moreover, criminal charges focus on individuals rather than states, providing prosecutors with the option, when

[77] M Chalfant, 'Mueller's "Speaking Indictments" Offer Clues to Strategy' (*The Hill*, 24 August 2018) thehill.com/policy/national-security/402902-muellers-speaking-indictments-offer-clues-to-strategy.

[78] G Hinck and T Maurer, 'What's the Point of Charging Foreign State-Linked Hackers?' (*Lawfare*, 24 May 2019) www.lawfaremedia.org/article/whats-point-charging-foreign-state-linked-hackers.

[79] Keitner (n 74) 210–11.

[80] ibid 211.

[81] ibid. While these indictments are typically framed under US law, they may offer insights into the United States' stance on applicable international law in cyberspace. Indeed, some accompanying statements explicitly reference 'international norms'; see, eg, US DOJ, 'Two Chinese Hackers Working with the Ministry of State Security' (n 76).

[82] Goldsmith and Williams (n 75).

[83] P Machtiger, 'Disrupt, Don't Indict: Why the United States Should Stop Indicting Foreign State Actor Hackers' (*Just Security*, 3 April 2020) www.justsecurity.org/69104/disrupt-dont-indict-why-the-united-states-should-stop-indicting-foreign-state-actor-hackers.

[84] JP Carlin, 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats' (2016) 7 *Harvard National Security Journal* 391, 418.

[85] Lee found that US government actors publicly attribute cyber incidents through four distinct 'channels': criminal, technical, official policy, and unofficial policy; see Lee (n 74) 202.

[86] Hinck and Maurer (n 74) 529.

unveiling charges against proxy hackers, to decide whether to allege state sponsorship, influencing the impact of the accusations.[87]

Crucially for the current discussion, this strategy grants domestic courts a prominent role in any international dispute arising from these malicious cyber activities. By scrutinising the evidence presented by prosecuting authorities, domestic courts can offer a more detailed legal analysis of the cyber activities in question and their attribution to foreign states. This can contribute to articulating the government's claims and strengthening its position in the dispute with the relevant foreign state. Whether or not the perpetrators can be brought to justice, the mere act of issuing the indictment and potentially hearing the claims may already provide victims of cyber offences with a form of satisfaction for the harm suffered. It can also serve as the foundation for further reparation schemes.[88] Finally, domestic court proceedings may heighten the pressure on the offending state to cease wrongful acts and refrain from future malicious cyber activities.

Addressing cyber threats through domestic criminal law proceedings can be a significant factor in pushing relevant states to resolve disputes through available means of dispute settlement. Supporters of this strategy point to the 2014 PLA indictment as an example, suggesting its role in prompting a bilateral agreement between the US and China on curbing cyber-enabled economic espionage in 2015.[89] However, the success of the indictment strategy as a negotiation gambit has been inconsistent. Subsequent indictments have not yielded similar results, and the US-China trade war that began in 2018 witnessed a resurgence of Chinese cyber activities,[90] highlighting the limitations of relying solely on the indictment strategy.[91]

Another layer of complexity surrounding the indictment strategy involves the issue of functional immunity, which shields foreign state officials from prosecution in domestic courts for acts committed in their official capacity.[92] Herein lies

[87] ibid 530.

[88] On satisfaction as a form of reparation, see C Hoss, 'Satisfaction' in A Peters (ed), *Max Planck Encyclopedia of Public International Law* (Oxford, Oxford University Press, 2011).

[89] B Wittes, 'James Lewis on the China Cyber Deal' (*Lawfare*, 5 October 2015) www.lawfaremedia.org/article/james-lewis-china-cyber-deal.

[90] See DQ Wilber, 'China "Has Taken the Gloves Off" in Its Thefts of US Technology Secrets' (*Los Angeles Times*, 16 November 2018) www.latimes.com/politics/la-na-pol-china-economic-espionage-20181116-story.html.

[91] The USA responded with a series of criminal charges to put increased pressure on China, all of which have been part of the DOJ's 'China Initiative'; see US DOJ, 'Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage' (1 November 2018) www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

[92] Alongside functional immunity, which applies to acts performed in an official capacity by all state officials, international law also provides for personal immunity, which is granted to a limited group of high-ranking officials, protecting them from foreign court jurisdiction for all acts while in office; see UNGA, 'Immunity of State Officials from Foreign Criminal Jurisdiction: Memorandum by the Secretariat' (31 March 2008) UN Doc A/CN.4/596 paras 88–89; UNGA, 'Preliminary Report on Immunity of State Officials from Foreign Criminal Jurisdiction, by Roman Anatolevich Kolodkin, Special Rapporteur' (29 May 2008) UN Doc A/CN.4/601, 177; R Van Alebeek, *The Immunity of States and Their Officials in International Criminal Law and International Human Rights Law* (Oxford, Oxford

the conundrum of associating accused foreign hackers with a foreign state. On the one hand, establishing a connection between the malicious cyber operation and a state agent simplifies the attribution of said activity to the foreign state.[93] This is particularly important when, as mentioned earlier, indictments serve purposes beyond domestic court prosecution, such as providing the basis for issuing economic sanctions against the allegedly responsible state.[94] On the other hand, attributing the relevant activity to the state implies that the underlying acts were likely 'performed in an official capacity', preventing the individual state agent from standing trial before foreign domestic courts.[95]

The basis for functional immunity is typically found in the fact that, under international law, official acts of state representatives are imputable to the state.[96] In this sense, functional immunity operates as 'a mechanism for diverting responsibility to the state',[97] which is the actual defendant in the proceedings.[98] However, in similar circumstances, proceedings against the state would, in turn, be barred by the rules of state immunity, as malicious cyber operations ordinarily amount to 'sovereign activities' excluded from the jurisdiction of foreign domestic courts under the dominant theory of state immunity.[99] None of the existing immunity codifications contains an exception for malicious cyber operations, although certain activities may fall under other immunity exceptions in specific circumstances.[100]

University Press, 2008) 8; R Pedretti, *Immunity of Heads of State and State Officials for International Crimes* (Leiden, Brill Nijhoff, 2015) 2.

[93] Under Art 4 of the International Law Commission's Articles on State Responsibility, the conduct of 'any state organ' is attributable to a state, even if it 'exceeded its competence under internal law'; see ILC, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries' in *Yearbook of the International Law Commission. 2001, Volume II, Part Two: Report of the Commission to the General Assembly on the Work of its Fifty-Third Session, as Corrected* (New York, UN, 2008) 40. See also *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v Serbia and Montenegro*) (Judgment of 26 February 2007) [2007] ICJ Rep 43 para 385.

[94] See text at nn 78–9 above.

[95] However, debate exists as to the exact scope of functional immunity; see CI Keitner, 'Foreign Official Immunity and the Baseline Problem' (2011) 80 *Fordham Law Review* 605, 614; Z Douglas, 'State Immunity for the Acts of State Officials' (2012) 82 *British Yearbook of International Law* 281, 296; R Van Alebeek, 'Functional Immunity of State Officials from the Criminal Jurisdiction of Foreign National Courts' in T Ruys, N Angelet and L Ferro (eds), *The Cambridge Handbook of Immunities and International Law* (Cambridge, Cambridge University Press, 2019) 499.

[96] See D Akande and S Shah, 'Immunities of State Officials, International Crimes, and Foreign Domestic Courts' (2010) 21 *European Journal of International Law* 815, 826; Douglas (n 95) 322–23; *Prosecutor v Blaškić* (Judgment (on the Request for Review of the Decision of 18 July 1997) of 29 October 1997) ICTY IT-95-14 para 38; *Re Rissmann* (1973) 71 ILR 577, 581 (Italy). It is also possible that the conduct may be attributable to the individual state official; see UNGA, 'Preliminary Report on Immunity of State Officials' UN Doc A/CN.4/601, 179–80.

[97] Akande and Shah (n 96) 826.

[98] See Douglas (n 95) 287.

[99] The 'restrictive theory' of state immunity distinguishes between immune sovereign acts and non-immune private acts, and is today the most widely adopted approach among states; see P-H Verdier and E Voeten, 'How Does Customary International Law Change? The Case of State Immunity' (2015) 59 *International Studies Quarterly* 209; Crawford (n 18) 472–73.

[100] In a recent lawsuit concerning the alleged use of Pegasus spyware, the English High Court ruled that the exception for injuries sustained within UK territory precluded Saudi Arabia's claim of state

Others have proposed that amending immunity legislation, such as the US Foreign Sovereign Immunities Act (FSIA), by creating a new and tailored cyber exception, may be the best way to ensure accountability for states that threaten human rights with cyber tools and conduct cyber economic espionage.[101]

To date, the DOJ has largely downplayed these concerns. In a statement accompanying the 2014 PLA indictment, the then Assistant Attorney General for National Security, John Carlin, asserted:

> State actors engaged in cyber espionage for economic advantage are not immune from the law just because they hack under the shadow of their country's flag. Cyber theft is real theft and we will hold state sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws.[102]

This stance, however, remains untested in both domestic and international courts, potentially paving the way for future disputes regarding the scope of state immunity in cyberspace. These challenges may also account for some recent developments explored in the following section.

B. Engagement through Proceedings against Private Cyber Contractors

While directly holding foreign states accountable for malicious cyber operations through domestic courts faces hurdles due to state immunity, a novel approach has emerged in light of governments' increasing reliance on external experts to design, construct, or execute malicious cyber operations.[103] Instead of targeting foreign sovereign states, recent cases have seen lawsuits brought against private contractors allegedly involved in hacking on behalf of these states.

immunity; see *Al-Masarir v Saudi Arabia*, [2023] QB 475. In the US, some argue that certain cyber operations may fall under the terrorism exceptions contained in the Foreign Sovereign Immunities Act of 1976 (FSIA); see JS Goldman and B Strong, 'Overcoming Immunity of Foreign Gov't Cyberattack Sponsors' (*Anderson Kill*, 2 December 2020) www.andersonkill.com/Publications/Overcoming-Immunity-of-Foreign-Govt-Cyberattack-Sponsors; JJ Martin, 'Hacks Dangerous to Human Life: Using JASTA to Overcome Foreign Sovereign Immunity in State-Sponsored Cyberattack Cases' (2021) 121 *Columbia Law Review* 119.

[101] See S Kleiner and L Wolosky, 'Time for a Cyber-Attack Exception to the Foreign Sovereign Immunities Act' (*Just Security*, 14 August 2019) www.justsecurity.org/65809/time-for-a-cyber-attack-exception-to-the-foreign-sovereign-immunities-act/; AL Silow, 'Bubbles over Barriers: Amending the Foreign Sovereign Immunities Act for Cyber Accountability' (2021) 12 *Journal of National Security Law and Policy* 659.

[102] US DOJ, 'US Charges Five Chinese Military Hackers' (n 75).

[103] See Silow (n 101) 660–61; JH Dwan, TP Paige and R McLaughlin, 'Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers?' (2022) 4 *Law, Technology and Humans* 49; S Feldstein and B (Chun Hey) Kot, 'Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses' (*Carnegie Endowment*, 14 March 2023) carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

In October 2019, WhatsApp, an online messaging platform owned by Facebook Inc (now Meta), filed a lawsuit against NSO Group (NSO) before the district court for the Northern District of California.[104] NSO, an Israeli company specialising in surveillance technology, developed the Pegasus spyware, enabling remote intelligence extraction from mobile devices. While NSO claims to sell its software to government agencies exclusively for law enforcement operations, investigative reports have revealed numerous instances of misuse against journalists, lawyers, and activists.[105] In its complaint, WhatsApp alleged that NSO used its servers without authorisation to transmit malicious code to around 1,400 users, aiming to infect their devices for surveillance, in breach of the Computer Fraud and Abuse Act and other US statutes.[106]

NSO moved to dismiss the case, claiming 'derivative immunity' because foreign governments used its spyware technology for law enforcement activities ordinarily covered by immunity.[107] The district court rejected this plea, finding that state immunity had no bearing on this case given that the lawsuit targeted the company and its agents in their individual capacities, not their sovereign customers:

> defendants have not argued that any of their foreign sovereign customers would be forced to pay a judgment against defendants if plaintiffs were to prevail in this lawsuit. … [T]he court can craft injunctive relief that does not require a foreign sovereign to take an affirmative action. Thus, plaintiffs do not seek to enforce a rule of law against defendants' customers.[108]

This decision is in line with customary international law, according to which non-state entities do not enjoy state immunity simply by being complicit in the wrongful acts of foreign states.[109] This holds true even when domestic courts must assess the legal position of said states to decide the case.[110] On appeal, the Court for the Ninth Circuit affirmed the district court's decision, holding that entities like NSO, which do not qualify as foreign states, cannot claim foreign sovereign immunity under the FSIA.[111] This precedent will likely have a bearing on another suit against NSO, filed by Apple, accusing NSO of enabling clients to hack into Apple users' devices through its spyware.[112]

[104] *WhatsApp Inc et al NSO Group Techs Ltd et al* No 3:19-cv-07123 (ND Cal, 29 October 2019) Complaint.

[105] See S Kirchgaessner et al, 'Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon' (*The Guardian*, 18 July 2021) www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

[106] *WhatsApp Inc et al* (n 104) 809.

[107] ibid. See R Buchan and D Franchini, '*WhatsApp v NSO Group*: State Immunity and Cyber Spying' (*Just Security*, 16 April 2020) www.justsecurity.org/69684/whatsapp-v-nso-group-state-immunity-and-cyber-spying.

[108] *WhatsApp Inc NSO Group Techs Ltd* 472 F Supp 3d 649, 665 (ND Cal 2020).

[109] See D Franchini, 'State Immunity and Third-Party Limits on the Jurisdiction of Domestic Courts' (2023) 72 *International and Comparative Law Quarterly* 819, 825–26.

[110] ibid.

[111] *WhatsApp Inc NSO Group Techs Ltd* 17 F 4th 930, 937 (9th Cir 2021).

[112] *Apple Inc NSO Group Techs Ltd et al* No 5:21-cv-09078 (ND Cal, 23 November 2021) Complaint.

The differentiation between domestic proceedings targeting foreign states involved in malicious cyber operations and those focusing on their private contractors opens new avenues for domestic courts' involvement in international cyber disputes. Even if direct legal action against states remains shielded by immunity, the process of evidence gathering and judicial review in cases against private contractors offers crucial insights into the 'what' and 'how' of malicious cyber operations. This contributes to establishing findings related to attribution and the application of relevant international legal rules, which government agencies may utilise for executive action. In a notable example, in November 2021, the Biden administration added surveillance technology companies, including NSO Group, to the Commerce Department's list of sanctioned entities, citing reports of misuse originating partly from domestic court litigation.[113]

Engaging in international cyber disputes through litigation against private contractors may also enable domestic courts to contribute to the development of the international legal framework governing cyberspace. By clarifying key concepts and legal qualifications applicable to malicious cyber activities, these cases set important precedents for future disputes and contribute to cross-fertilisation in cyber law-making.[114] Some domestic courts may also consider and incorporate relevant international legal principles, such as the principle of 'territorial sovereignty',[115] into their decisions. Integrating international norms into domestic legal proceedings further contributes to their development and solidifies their acceptance among states.

IV. Conclusion

Far from having a limited role in settling international cyber disputes, domestic courts emerge as pivotal actors, wielding influence both within and beyond their borders. This chapter has identified two crucial roles played by these courts: an 'internal' gatekeeping function concerning the forum state and an 'external' shaping function vis-à-vis other states.

Internally, domestic courts can scrutinise cyber-related activities of their own legislatures and executives. This may ensure alignment with international law

[113] See Anon, 'United States Makes Efforts to Curb Misuse of Surveillance Technology' (2022) 116 *American Journal of International Law* 426.

[114] This may help alleviate concerns about the perceived overreliance on self-regulation within the private tech sector; refer to I Kilovaty, 'Privatized Cybersecurity Law' (2020) 10 *UC Irvine Law Review* 1181.

[115] For instance, in the *Tidal* case, the Norwegian Supreme Court found that a search against the music streaming company carried out within the country using access credentials provided by its employees did not violate the principle of territorial sovereignty; see *Tidal Music AS v The Public Prosecution Authority* (28 March 2019) HR-2019-610-A (case no 19-010640STR-HRET) para 71. In an earlier case, a Canadian judge found that extraterritorial intrusive surveillance presumptively impinged on the territorial sovereignty of foreign states; see *Re Canadian Security Intelligence Service*

obligations and prevent potential violations, which is vital in pre-empting the emergence of international cyber disputes. In some circumstances, particularly with respect to suppressing certain cyber offences and cyber activities harming human rights, exercising domestic court jurisdiction may itself form part of the state's international obligations.

Externally, domestic courts can actively shape international cyber disputes between sovereign states. When capable of exercising jurisdiction over malicious cyber activities of state-sponsored foreign actors, such as in the case of recent US indictments, domestic courts can contribute to articulating the government's claims and strengthening the state's position in the dispute. The pressure generated by domestic litigation can also nudge states towards negotiation and settlement of cyber disputes through one of the available means. Finally, domestic courts, through their judicial pronouncements, can contribute to the development of international legal norms and principles governing cyberspace.

While the increasing involvement of domestic courts in international cyber disputes holds tremendous potential, it also raises concerns about politicisation. Their participation in politically sensitive matters may expose them to geopolitical pressures, potentially compromising their impartiality. Safeguarding judicial independence, upholding the rule of law, and ensuring transparent processes are, therefore, crucial to maintaining the integrity of domestic courts. Striking a balance between addressing cybersecurity threats and preventing undue interference can be achieved by developing international legal frameworks that specify circumstances requiring domestic court action. Instruments such as the Budapest Convention and mutual legal assistance treaties can be seen as meaningful steps towards minimising these risks.[116]

While international judicial cooperation is undoubtedly crucial in combating cyber threats, any legal instruments aimed at promoting this must tread a delicate tightrope. The Budapest Convention, for instance, has been long criticised for its potential to be misused by governments seeking to limit the enjoyment of fundamental rights online.[117] Similarly, the ongoing initiative within the UN General Assembly to formulate a Comprehensive Cybercrime Convention has come under scrutiny for comparable reasons.[118]

Act [2008] SCRS-10-07, 2008 CF 301 para 50. See generally S Watts and T Richard, 'Baseline Territorial Sovereignty and Cyberspace' (2018) 22 *Lewis and Clark Law Review* 771.

[116] See section II.B above.

[117] See Council of Europe Commissioner for Human Rights, *The Rule of Law on the Internet and in the Wider Digital World* (*COE*, 2014) rm.coe.int/the-rule-of-law-on-the-internet-and-in-the-wider-digital-world-issue-p/16806da51c, 17.

[118] UNGA, 'Resolution Adopted by the General Assembly on 27 December 2019: 74/247. Countering the Use of Information and Communications Technologies for Criminal Purposes' (20 January 2020) UN Doc A/RES/74/247. See D Brown, 'Cybercrime is Dangerous, but a New UN Treaty Could be Worse for Rights' (*Just Security*, 13 August 2021) www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights; C Ohanian, 'The UN Cybercrime Treaty has a Cybersecurity Problem in It' (*Just Security*, 17 October 2022) www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it.

However, abandoning efforts at developing a comprehensive legal framework for international judicial cooperation may not be the ideal answer. A more effective path forward may lie in crafting international legal agreements that empower domestic courts to strike a balance between competing interests in this area. These agreements should enable a measured degree of executive action to address legitimate cybersecurity concerns while safeguarding respect for all relevant human rights obligations, providing vital checks and balances against potential abuses.

Only through such carefully constructed legal frameworks can domestic courts be empowered to navigate this complex and ever-evolving legal landscape effectively. This, in turn, will enable them to play a central role in promoting the rule of law in cyberspace.