POLICY BRIEF NO.1

Oxford Institute
of Technology and Justice

LEGAL ACCOUNTABILITY FOR MALICIOUS CYBER OPERATIONS

POLICY BRIEF

AUTHORS

HARRIET MOYNIHAN (LEAD AUTHOR),
PHILIPPA WEBB, AMAL CLOONEY

SEPTEMBER 2025

https://www.doi.org/10.35489/BSG-OITJ-PB-1_2025-01

TABLE OF CONTENTS

EXECUTIVE SUMMARY

- This Brief considers the options for States to seek legal accountability for malicious cyber operations, examining both the application of the international law on the peaceful settlement of disputes to cyber operations, and the role of international and domestic courts in the prosecution of malicious cyber activity. The analysis is timely as cyber threats grow in scale, sophistication and gravity, yet too often, hostile threat actors are able to act with impunity.

- Over 130 States have experienced cyber disruption from a growing array of cyber actors, including States, criminal gangs and individual hackers. Malicious cyber operations are increasingly directed at national critical infrastructure, including hospitals, transport facilities and energy supplies. And the incidence of cybercrime has increased exponentially in recent years.

- To date, States that are directly or indirectly the victims of malicious cyber operations have mainly chosen to respond through diplomatic or political means, such as international and regional dialogue, naming and shaming the States alleged to be responsible, sanctions, or countermeasures. These responses, while important, come with limitations, including legal accountability gaps.

- In many cases, courts may not be well-suited to settle inter-State cyber disputes, particularly because of the reluctance by States to consent to a third party adjudicating in an area in which they may wish to maintain operational freedom; the difficulty of attributing a cyber operation to an individual or State; and the unsettled status of international law in this area. So far, no State has brought a claim against another State in response to a malicious cyber operation. But we can expect States to test this option in the future, and the available avenues are under-researched. This Policy Brief explores what the options would look like in practice.

- Using a hypothetical scenario based on a cyber operation carried out by one State that disrupts aviation services in another State, resulting in a plane crash, this Brief shows that a number of avenues exist for States to seek legal accountability for malicious cyber activity, where the facts are conducive to the claim. The Brief examines potential actions before the International Court of Justice (ICJ) or regional human rights mechanisms, as well as the option of seeking an Advisory Opinion before the ICJ. The Brief also considers other means of settling international cyber disputes, including fact-finding and arbitration.

- Where the cyber activity in question can be attributed to an individual or group, States may be able to prosecute the perpetrator in their domestic courts. For particularly serious cases involving cyber activity that that perpetrates or facilitates an international crime, it may also be possible for States or the International Criminal Court to prosecute the perpetrator for cyber-enabled international crimes.

- Increasing public–private collaboration on investigations into malicious cyber activity, developments in technical attribution, the recent adoption of the UN Cybercrime Convention, and other developments in international evidence-sharing make the option of prosecution of cybercriminals more promising.

- Dispute settlement options can operate in parallel and be complementary: for example, public attributions, sanctions and prosecutions may form part of a broader strategy of deterrence and accountability, and fact-finding may serve as a precursor to litigation.

- This Brief takes an incremental approach to the application of the law on the peaceful settlement of disputes in a cyber context, recognising that at the present time, States that are the victims of malicious cyber operations do not usually choose to frame their response as a 'cyber dispute'. However, as understandings of how international law applies in the cyber context mature, this is likely to change; indeed, some States have already begun seeking advice on the possibility of claims in this area.

- Therefore, more work is needed to clarify the options for States and to identify any gaps in this area; to promote knowledge, capacity and confidence among States, companies, civil society and individuals on cyber dispute settlement; to consider options for strengthening attribution and clarifying standards of evidence and proof; and to ensure that States have the necessary legislation to bring effective prosecutions for malicious cyber operations. This work will be a focus for the Oxford Institute of Technology and Justice, in collaboration with partners, in order to strengthen legal accountability for malicious cyber activity.

INTRODUCTION

1. Without accountability for malicious operations conducted in cyberspace, hostile actors have little incentive to refrain from cyber operations and are able to act with impunity. Accountability for malicious cyber activity can take different forms.[1] This Policy Brief focuses on options available to States for legal accountability for malicious cyber activity carried out by both State and non-State actors, the extent to which these options have been used so far, and the challenges that may prevent accountability in this context.

2. This Brief first considers the ways in which peaceful means of inter-State dispute settlement might apply in the cyber context, both diplomatic and adjudicative – including the prospects of a claim before the International Court of Justice (ICJ), an arbitral tribunal or a regional human rights court. The Brief then considers the options for States to prosecute the individual perpetrators of cybercrime, as well as the prosecution of cyber-enabled international crimes by both international and domestic courts.

3. The Brief is not designed to be comprehensive but rather to offer fresh thinking in this area, and to test options that may be of increasing interest to States in the future. Legal accountability options available to other actors, including companies, Non-Governmental Organizations (NGOs) and individuals, will be explored in subsequent briefs.[2] 'Cyber' here is used to describe Information and Communication Technologies (ICTs) more broadly and may cover not only traditional malicious cyber operations (such as unauthorized hacking or ransomware) but also the use of the internet and social media for malign purposes.

4. This Brief focuses particularly on malicious cyber operations by one State that intentionally target another State with a view to causing significant effects in the victim State – for example, cyber sabotage operations that deliberately disrupt critical infrastructure such as healthcare, resulting in the cancellation of operations and delays in treatment.

The cyber threat landscape

5. Cyberspace is increasingly the site of inter-State clashes and contestation, both in peacetime and armed conflict. Over 130 countries have experienced cyber disruption,[3] including operations against supply chains that have cost billions,[4] and operations against elections that undermine democratic processes.[5] For example, in 2022, Albania suffered a wave of cyber operations targeting governmental services, including attempts to steal data, in an operation that Albania and other States attributed to Iran.[6] In 2022, Costa Rica was forced to declare a

[1] For broader framings of accountability in relation to malicious cyber activity, drawing on lessons from accountability in other policy areas, see Alison Pytlek and others, 'Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches' (Stimson Center, 8 July 2024) https://www.stimson.org/2024/advancing-accountability-in-cyberspace/; Patrick Pawlak, Accountability in Cyberspace: The Holy Grail of Cyber Stability? (Policy Brief, EU Cyber Direct, March 2024) https://www.universiteitleiden.nl/binaries/content/assets/governance-and-global-affairs/isga/accountability-in-cyberspace-patryk-pawlak-march-2024.pdf

[2] This includes claims for civil liability in domestic courts.

[3] Julia Voo and Virpratap Vikram Singh, 'Power across layers of cyberspace' (International Institute for Strategic Studies, 24 April 2025) https://www.iiss.org/charting-cyberspace/2025/04/power-across-layers-of-cyberspace/.

[4] Steve Morgan, 'Software Supply Chain Attacks To Cost the World $60 Billion by 2025' (Cybercrime Magazine, 3 October 2023) https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/.

[5] Samir Jeraj, 'Hacking democracy: How cyber attacks are undermining trust in voting' (The New Statesman, August 2023) https://www.newstatesman.com/spotlight/tech-regulation/cybersecurity/2023/08/hacking-democracy-electoral-commission-cyber-attacks.

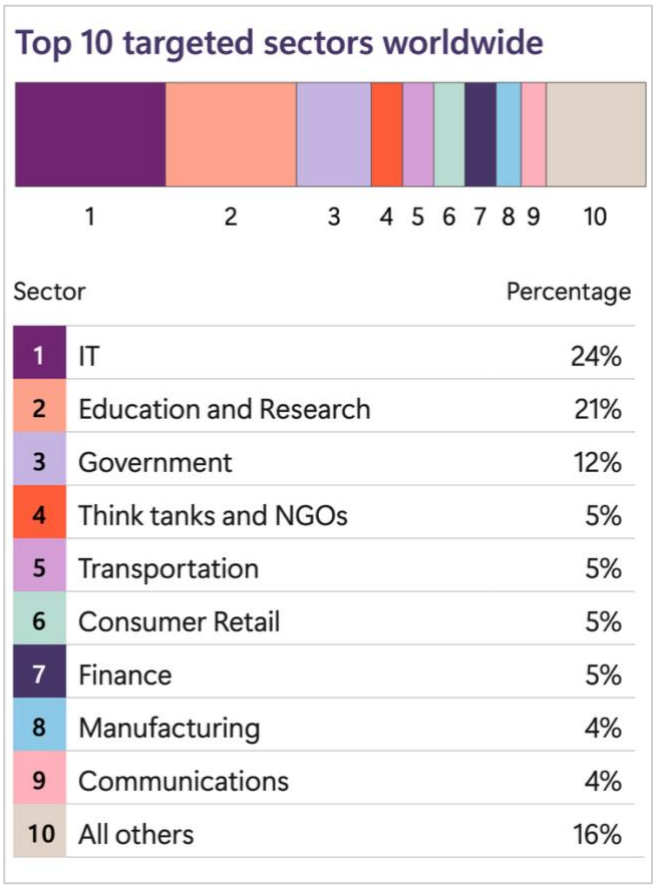
[6] See, for example, UK government, 'UK condemns Iran for reckless cyber attacks against Albania' (7 September 2022) https://www.gov.uk/government/news/uk-condemns-iran-for-reckless-cyber-attack-against-albania.

state of emergency after two major ransomware attacks, attributed to the Conti group that has links to Russia, paralysed essential services including nearly 30 government institutions.[7]

6. Cyber is also increasingly a tool used in conflict – a Russian cyberattack on Ukraine's power grid in 2015 left around 700,000 Ukrainians without power in the middle of winter;[8] Russian cyber activity against Ukraine surged by nearly 70% in 2024.[9] AI has lowered the barriers to entry for cyber operations, resulting in a proliferation of cyber threat actors and more sophisticated tactics and techniques.[10] Even if States or non-State actors do not have home-grown cyber capabilities, they can now easily buy cyber tools such as Worm GPT, or 'ransomware-as-a-service', off the shelf.[11]

7. It is predicted that by 2031, ransomware will cost victims $261 billion annually and attack a business or consumer device every two seconds.[12] According to Microsoft, there has been a 300% surge in ransomware attacks since 2015.[13] Healthcare is one of the industries most affected: in the US alone, in the period between June 2023 and June 2024, 389 healthcare institutions were successfully hit by ransomware, with a serious impact on patient care, including delayed operations and appointments.[14] A ransomware attack on the Irish healthcare system in 2021, attributed to the Conti group, disrupted healthcare services for months.[15] In 2024, the US indicted a North Korean military intelligence operative who hacked into US hospitals and healthcare providers to extort them.[16] As the chart below shows, other sectors targeted by cyber threat actors include IT, education and research, government, think-tanks and NGOs.

[7] 'Costa Rica declares national emergency amid ransomware attacks' (The Guardian, 12 May 2022) https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks.
[8] America Cyber Defence Agency, 'Cyber-Attack Against Ukrainian Critical Infrastructure' (20 July 2021) https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01#:~:text=SUMMARY-,On%20December%2023%2C%202015%2C%20Ukrainian%20power%20companies%20experienced%20unscheduled%20power,variety%20of%20critical%20infrastructure%20sectors.
[9] Center for Strategic & International Studies 'Significant Cyber Incidents' https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[10] Generative AI has been described as '[t]he adversary's new best friend'; see CrowdStrike, 2025 Global Threat Report: Latest Cybersecurity Trends & Insights (2025) https://www.crowdstrike.com/en-us/global-threat-report/.
[11] See, for example, Anthropic, 'Detecting and countering misuse of AI: August 2025' (27 August 2025) https://www.anthropic.com/news/detecting-countering-misuse-aug-2025.
[12] Steve Morgan, 'Ransomware Will Strike Every 2 Seconds by 2031' (Cybercrime Magazine, 28 June 2023) https://cybersecurityventures.com/ransomware-will-strike-every-2-seconds-by-2031/.
[13] Microsoft, 'US Healthcare at Risk: Strengthening resiliency against ransomware attacks' https://www.microsoft.com/en-us/security/security-insider/threat-landscape/us-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks.
[14] Microsoft, Microsoft Digital Defense Report 2024 (October 2024) https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf 3.
[15] 'HSE cyber-attack: Irish health service still recovering months after hack' (BBC News, 5 September 2021) https://www.bbc.co.uk/news/world-europe-58413448.
[16] US Department of Justice, 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting US Hospitals and Health Care Providers' (Press Release, 25 July 2024) https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.

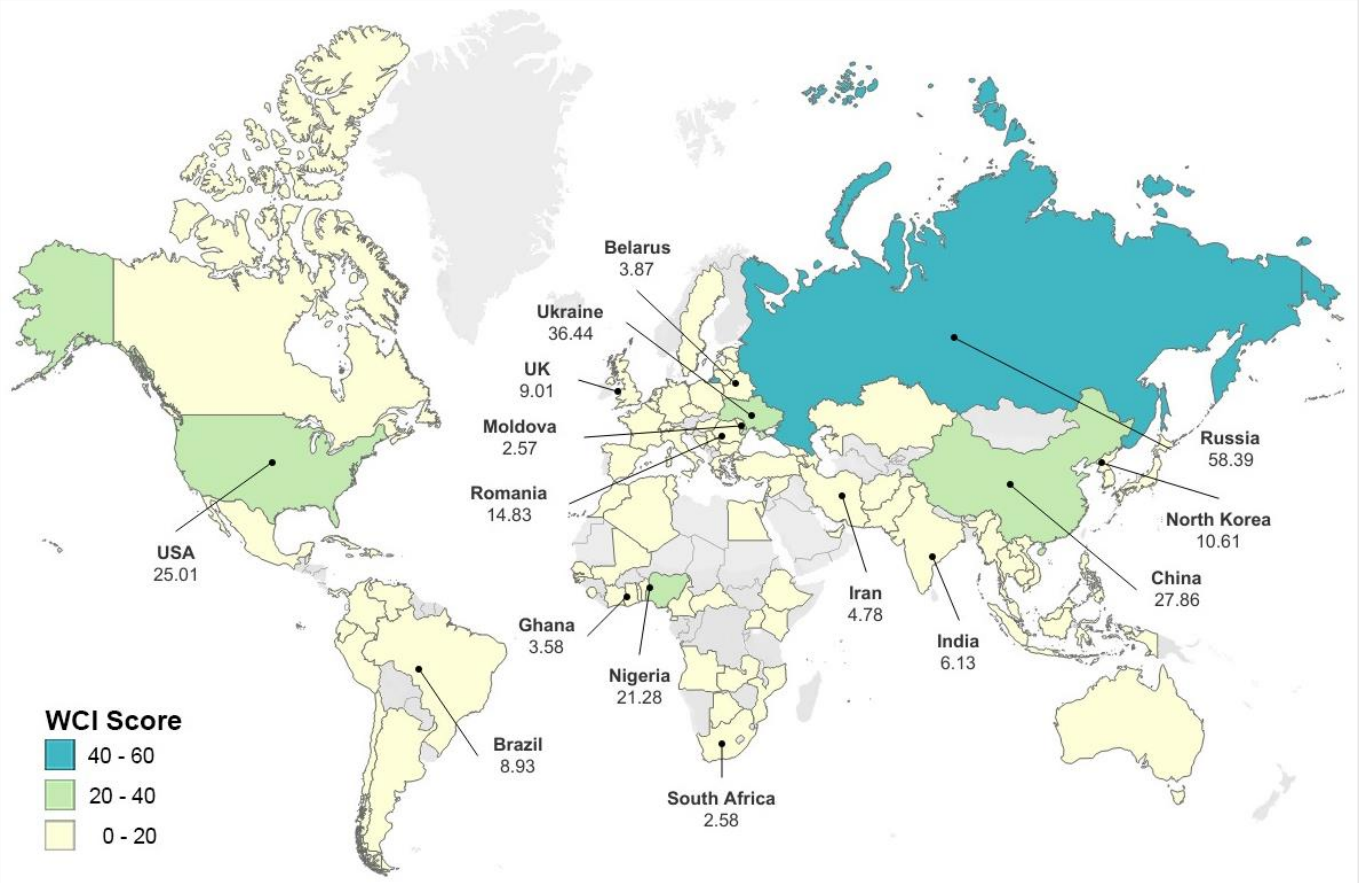


Source: Microsoft Threat Intelligence: nation-state notification data

8. According to the Council on Foreign Relations, 34 countries are suspected of sponsoring cyber operations since 2005. Of these, the CFR reports that China, Russia, Iran and North Korea sponsored 77% of all cyber operations in which it is suspected that a State was involved.[17] In practice, however, many cyber operations (nearly half, according to a recent report) remain unattributed to a State.[18] Some will be carried out by individuals operating alone, or by criminal groups; others may involve a State tolerating or supporting such actors but without sufficient evidence to link the operation to a State.

[17] Council on Foreign Relations, 'Cyber Operations Tracker' https://www.cfr.org/cyber-operations/.
[18] International Society of Automation (ISA) Global Cybersecurity Alliance, 'Defending Against State-Sponsored Cyberattacks in 2025' https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025.

9. A 2024 study by the University of Oxford found that cybercrime currently emanates from a relatively small number of countries, with most operations coming from the territories of Russia, Ukraine, China, the US and Nigeria.[19] Of course, what is not visible is the extent of cyber espionage and influence operations by many States, including Western States, which may also have effects, some of which may be harmful. These operations, while also important, are outside the scope of this Brief.



Source: World Cybercrime Index, showing the cybercrime threat level per country

[19] Miranda Bruce and others, 'Mapping the global geography of cybercrime with the World Cybercrime Index' (2024) 19(4) PLOS ONE 1.

EXAMPLES OF THE DISRUPTIVE EFFECTS OF RECENT MALICIOUS CYBER OPERATIONS

1. **Cyber espionage to steal sensitive data:**
   - → **Kremlin-backed operation against Embassies in Moscow, July 2025:** Kremlin-backed hackers reportedly used Russian internet service providers to plant malware on diplomats' computers, allowing them to see passwords and bank details and to change what users see, potentially showing them fake login pages.[20]
2. **Cyber activity to facilitate lethal strikes in a war zone:**
   - → **Mariupol Theatre operation, March 2022:** Russian GRU Unit 26165 is alleged to have conducted online reconnaissance to facilitate missile strikes against Mariupol, including the bombing of the Mariupol Theatre, resulting in the death and injury of many civilians.[21]
3. **Cyber operations on critical infrastructure**:
   - → **Operation against Iran's maritime sector, August 2025:** a hacker group known as Lab-Dookhtegan claimed responsibility for a cyberattack on Iran's maritime sector, disabling communications on more than 60 oil tankers and cargo ships.[22]
   - → **Operation against Ukraine power grid attack, December 2015:** Russia is alleged to have conducted a cyber operation on Ukraine's power grid by planting malware to disrupt the operation of industrial control systems. This attack led to unscheduled power outages affecting approximately 225,000 customers in the middle of Winter.[23]
4. **Distributed denial-of-service (DDoS) operations**: operations that overwhelm a website, server, or online service with massive amounts of traffic sent simultaneously from many compromised computers, causing the system to slow down, crash, or become unavailable to legitimate users.
   - → **Ukraine power grid operation, December 2015:** in the operation against Ukraine's power grid (see above), DDoS operations were also employed to overwhelm call centres, hindering the response efforts.
5. **GPS jamming of aircraft and interference with airports:**
   - → **EU Commission President GPS jamming, September 2025:** President Ursula von der Leyen's plane experienced jamming over Bulgaria, forcing it to circle Plovdiv Airport for an hour using hard copy maps.[24]
6. **Ransomware operations:** operations that block access to computer or files, usually by locking or scrambling them. The attackers then demand a ransom to unlock the data:
   - → **US hospitals, July 2024:** the US Department of Justice indicted a North Korean national for orchestrating ransomware operations targeting US hospitals and healthcare providers. According to the Department of Justice, malware was used to extort ransom payments, which

[20] Tom Chivers, 'Kremlin-backed hackers target foreign embassies in Moscow' (Semafor, 1 August 2025) https://www.semafor.com/article/08/01/2025/kremlin-backed-hackers-target-foreign-embassies-in-moscow.
[21] UK Government, Profile: GRU cyber and hybrid threat operations (Policy Paper, 18 July 2025) https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations.
[22] Safety4Sea, 'Hackers launch cyber attack targeting Iranian fleet' (25 August 2025) https://safety4sea.com/hackers-launch-cyber-attack-targeting-iranian-fleet/.
[23] America Cyber Defence Agency, 'Cyber-Attack Against Ukrainian Critical Infrastructure' (20 July 2021) https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01#:~:text=SUMMARY-,On%20December%2023%2C%202015%2C%20Ukrainian%20power%20companies%20experienced%20unscheduled%20power,variety%20of%20critical%20infrastructure%20sectors.
[24] Maia Davies and Will Vernon, 'EU chief von der Leyen's plane hit by suspected Russian GPS jamming' (BBC News, 1 September 2025) https://www.bbc.co.uk/news/articles/c9d07z1439zo.

were then laundered through China. The funds were subsequently used to finance cyber intrusions into defence, technology and government entities worldwide, including US agencies and contractors.[25]

- → **Costa Rica, May 2022:** Costa Rica declared a state of emergency after two major ransomware operations, attributed to the Conti Group, paralysed essential services, including nearly 30 government institutions.[26]
- → **Ireland Health Service Executive, May 2021:** Ireland's public health service's IT systems were compromised, leading to significant disruptions across Ireland's healthcare services. The attack forced the HSE to revert to paper-based systems, causing delays and cancellations of medical appointments and treatments.[27]
- → **LockBit ransomware group:** LockBit is one of the world's most active and dangerous ransomware groups, operating since 2019. It runs a ransomware-as-a-service model by providing its malware to affiliates who attack organizations, encrypt their data, and demand payment under threat of leaking stolen information.[28]

7. **Wiper operations**: operations where malware is used to erase, corrupt or overwrite data on a computer system or network, rendering it unusable.

- → **Albania attack, July–September 2022:** Iranian State-linked hackers are alleged by Albania and other States to have carried out a destructive cyber operation against Albania's government systems, using malware to disrupt public services. Albania was forced to shut down its government websites, and the Albanian Interior Ministry said police and civic services would need to operate in person.[29] Hackers forced Albanian officials to temporarily shut down the system used to track individuals entering and exiting Albania, meaning that border entry and exit had to take place manually.[30] The cyberattacks also resulted in data being leaked, including the names and addresses of 1000+ undercover police informants, email traffic of the head of intelligence, and the banking information of 30,000+ people[31] as well as bank customer financial records.[32]
- → **GRU operations against Ukrainian government's computer systems, January 2022:** in a US indictment, it is alleged that members of Russia's military intelligence services conspired to use US-based company services to distribute malware known as 'WhisperGate' to dozens of Ukrainian government entities' computer systems and destroy those systems and related data in advance of the Russian invasion of Ukraine.[33]

[25] US Department of Justice, 'North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting US Hospitals and Health Care Providers' (Press Release, 25 July 2024) https://www.justice.gov/archives/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals.
[26] 'Costa Rica declares national emergency amid ransomware attacks' (The Guardian, 12 May 2022) <https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks>.
[27] US Department of Health and Human Services, 'Lessons Learned from the HSE Cyber Attack' (02 March 2022) https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf.
[28] America Cyber Defence Agency, 'Understanding Ransomware Threat Actors: LockBit' (14 June 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
[29] 'Cyberattack blocks Albania's public online services' (AP News, 19 July 2022) https://apnews.com/article/albania-malta-government-and-politics-8847142d6fe3c2de2cf7f31f1784d2ce.
[30] Center for Strategic and International Studies, 'Significant Cyber Incidents' https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[31] A Higgins, 'A NATO Minnow Reels From Cyberattacks Linked in Iran' (The New York Times, 25 February 2023) https://www.nytimes.com/2023/02/25/world/europe/albania-iran-nato-cyberattacks.html.
[32] Ayman Oghanna, 'How Albania Became a Target for Cyberattacks' (Foreign Policy, 25 March 2023) https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.
[33] US Department of Justice, 'Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data' (Press Release, 26 June 2024)

10. To date, States that have been the victim of cyber operations have responded in a number of ways: diplomatic, political and operational. Some engage in private diplomatic démarches; others may employ 'naming and shaming' strategies, ie make public attributions of State or State-backed actors conducting cyber operations. Attribution has political, technical and legal dimensions – political attribution involves ascribing responsibility to a State or State-sponsored entity based on technical information and intelligence; technical attribution involves identifying the source of the cyber operation; and legal attribution involves identifying a State as responsible under the law on State responsibility.[34]

11. Traditionally, public political attributions have been made by Western States: in October 2023, it was reported that the US, Germany, Australia and Japan had made public political attributions of cyber operations in 164 instances.[35] Increasingly, such States have made attributions on a collective basis – for example, the States in the 'Five Eyes' intelligence network (the UK, US, Canada, Australia and New Zealand) often issue statements or advisory reports together.[36] However, in the past year other States have also started to make public attributions; for example, in September 2024, the Chinese Ministry of State Security accused Taiwan of carrying out cyberattacks against targets in Beijing,[37] and in July 2025, Singapore called out a cyber threat group, 'UNC3886', for targeting the country's critical infrastructure.[38] The group is believed to be linked to China.[39]

12. States have also responded to malicious cyber operations through measures of 'retorsion' – legal but unfriendly actions perpetrated by one State upon another in retaliation for a similar act – such as expelling diplomats; severing diplomatic relations; imposing 'cyber sanctions';[40] or disrupting supply chains to deplete resources.[41] As of May 2025, for example, the EU has sanctioned 17 individuals and four entities under its cyber diplomacy framework.[42] States have

https://www.justice.gov/archives/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian.

[34] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 Journal of Conflict and Security Law 229.

[35] 109 attributions by the US, 32 by Germany, 17 by Australia, and 6 by Japan. See Christina Rupp and Alexandra Paulus, Official Public Political Attribution of Cyber Operations: State of Play and Policy Options (Stiftung Neue Verantwortung, October 2023) https://www.interface-eu.org/index.php/publications/official-public-political-attribution-of-cyber-operations.

[36] See, for example, Connor Jones, 'Five Eyes and US finally confirm Russia was behind Ukrainian government, Viasat cyber attacks' (IT Pro., 10 May 2022) https://www.itpro.com/security/cyber-attacks/367634/five-eyes-and-us-governments-confirm-russia-behind-attacks#:~:text=Five%20Eyes%20and%20EU%20intelligence,the%20highest%20level%20of%20confidence. There have been 14 collective public political attributions made since 2017: See Dan Efrony, 'Collective Attribution in Cyberspace: A Rebranded Version does not make it more Effective' (2024) 103 ILS 270, 315.

[37] Ben Read, 'China is using cyber attribution to pressure Taiwan' (Binding Hook, July 2025) https://bindinghook.com/articles-hooked-on-trends/china-is-using-cyber-attribution-to-pressure-taiwan/.

[38] K Shanmugam, 'The Next 10 Years: Securing our Cyberspace and Digital Future' (Cyber Security Agency of Singapore Tenth Anniversary Dinner, 18 July 2025) https://www.mha.gov.sg/mediaroom/speeches/csa-10th-anniversary-dinner-the-next-10-years-securing-our-cyberspace-and-digital-future/.

[39] TxOne networks, 'Unmasking UNC3886: A Sophisticated Cyber Espionage Group Targeting Critical Infrastructure' (29 July 2025) https://www.txone.com/blog/unmasking-unc3886/.

[40] See Iryna Bogdanova and María Vásquez Callo-Müller, 'Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value' (2023) 54(4) VJTL 911. Australia, Canada, the EU, the UK and US have all established cyber sanctions regimes in the last ten years, with increasing use. Between 2017-2020, for example, the Trump administration averaged 57 cyber-related sanctions per year, an increase from an average of 10 per year in the previous Biden administration. See Jason Bartlett and Megan Ophel, 'Sanctions by the Numbers: Spotlight on Cyber Sanctions' (Center for a New American Security, 4 May 2021) https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.

[41] See, for example, Operation Endgame, which disabled the malware that cybercriminals use to infiltrate systems unnoticed before deploying ransomware: Europol, 'Operation ENDGAME strikes again: the ransomware kill chain broken at its source' (23 May 2025) https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source.

[42] See Council of the European Union, 'Cyber-attacks: Council extends sanctions and legal framework' (Press release, 12 May 2025) https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework.

also instituted political processes such as the Counter Ransomware Initiative and Pall Mall process in an attempt to mobilize international action against malicious cyber operations.[43]

13. Diplomacy is an important means of contributing to the peaceful settlement of disputes in the cyber context, but it has its limits. Often the 'naming and shaming' by one State of another simply results in silence or denials on the part of the accused State, leading to a lack of accountability for wrongful behaviour.[44] Cyber diplomacy also faces challenges at the international level. At the UN Open-Ended Working Group on the Security of and in the Use of Information and Communication Technologies (OEWG) in July 2025, some States had pushed for a dedicated thematic group on international law as part of the new UN permanent mechanism for the discussion of Information and Communication Technologies (ICTs), which would have enabled deeper dialogue by States on all topics of international law, including the peaceful settlement of disputes. However, States failed to agree on the inclusion of international law as a thematic group, leading to frustration among many stakeholders, as 'a missed opportunity to advance the discussions on international law and cyber activities'. [45]

14. As well as dealing with disputes through bilateral or multilateral diplomacy, States have the right to take unilateral action against another State in certain circumstances. Under customary international law, a State that is the victim of a violation of international law has the right to take countermeasures in order to induce the perpetrating State to comply with its international obligations.[46] Many States have asserted that the right to take countermeasures applies in the cyber context,[47] and a few States consider that this includes the right to take collective countermeasures.[48] However, the rules on the circumstances in which countermeasures can be used are strict. Countermeasures risk escalating disputes, and some States have criticized their use on the basis that they are prone to abuse.[49]

---

[43] The Counter-Ransomware Initiative was set up by the US to tackle ransomware in 2021 and has over 60 members; see International Counter Ransomware Initiative, 'About Us' https://counter-ransomware.org/aboutus. The Pall Mall Process was launched by the UK and France in February 2024 to tackle proliferation and irresponsible use of commercial cyber intrusion capabilities: see UK Foreign, Commonwealth and Development Office, The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities (28 February 2025) https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

[44] Martha Finnemore and Duncan Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity' (2020) 31(3) EJIL 969.

[45] Kubo Macak, 'A Missed Opportunity: An International Law Perspective on the Final OEWG Report' (EJIL: Talk!, July 2025) https://www.ejiltalk.org/a-missed-opportunity-an-international-law-perspective-on-the-final-oewg-report/.

[46] Countermeasures are actions taken by a State that would normally breach international law but are justified as a response to a prior breach, where their aim is to bring the wrongdoing State into compliance with international law. Rules governing the use and limits of countermeasures are set out in Articles 49-53 of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (2001) YILC vol II (Part Two).

[47] See NATO Cooperative Cyber Defence Centre of Excellence, 'Countermeasures' (International Cyber Law: Interactive Toolkit) https://cyberlaw.ccdcoe.org/wiki/Countermeasures#:~:text=Countermeasures%20are%20measures%2C%20which%20would,force%20and%20must%20be%20proportionate.

[48] i.e. indirectly injured States taking countermeasures against a wrongdoing State to protect a collective legal interest in order to enforce obligations owed to the whole community; see Russell Buchan, 'Collective and Third-Party Countermeasures' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 195 -236.

[49] See Brazil's national position statement advising a cautious approach to countermeasures, both in the cyber context and generally: NATO Cooperative Cyber Defence Centre of Excellence, 'Countermeasures' (International Cyber Law: Interactive Toolkit) https://cyberlaw.ccdcoe.org/wiki/Countermeasures#:~:text=Countermeasures%20are%20measures%2C%20which%20would,force%20and%20must%20be%20proportionate.

15. The means by which States can settle their disputes peacefully are far broader than diplomatic measures, yet other means by which States can settle international disputes – particularly methods that involve courts or tribunals – have received relatively little attention in the cyber context, either by States or scholars. This Brief is timely in considering legal accountability options, as States start to pay more attention to the peaceful settlement of disputes in their official position statements on how they consider international law applies in the cyber context. So far, 13 States and two regional organisations (the EU and AU) have included the topic of peaceful settlement in their national positions on how international law applies in the cyber context,[50] and a number of States have explicitly referred to the potential for cyber cases to come before the ICJ.[51] An important academic study published in 2024 has helped to shine a spotlight on this area,[52] but further analysis and capacity-building is needed.

16. This Brief begins by assessing the options available under international law for settling inter-State cyber disputes. The second section looks at prosecutions of cybercrimes carried out by non-State actors under domestic and international criminal law. The final section provides conclusions and highlights areas in need of further research.

THE OBLIGATION TO SETTLE INTERNATIONAL DISPUTES BY PEACEFUL MEANS

17. Under Article 2(3) of the UN Charter, all UN Member States are required to resolve their disputes only by peaceful means, i.e. not through the use of force. Article 2(3) has crystallised into a customary rule, which has been applied in the decisions of the ICJ, UN General Assembly[53] and UN Security Council resolutions,[54] and reinforced in multilateral and bilateral treaties.[55] For disputes that endanger the maintenance of peace and security, States have a duty to 'seek a solution'.[56] Article 33(1) of the UN Charter sets out a non-exhaustive and non-cumulative list of 'peaceful means' by which States may do so:

> '*negotiation*, *enquiry*, *mediation*, *conciliation*, *arbitration*, *judicial settlement*, *resort to regional agencies or arrangements*, *or other peaceful means of their own choice*'.

18. While not all cyber disputes will endanger the maintenance of peace and security, it is easy to conceive of major inter-State cyber operations with damaging effects on the victim State doing so. The UN Group of Governmental Experts Report of 2021 notes that the misuse of ICTs may harm international peace and security.[57]

---

[50] The content of national and regional positions on the Peaceful Settlement of Disputes in the cyber context are set out in the CCDCOE's CyberLaw Toolkit. See NATO Cooperative Cyber Defence Centre of Excellence, 'Peaceful Settlement of Disputes' (International Cyber Law: Interactive Toolkit) https://cyberlaw.ccdcoe.org/wiki/Peaceful_settlement_of_disputes; see also Thailand Ministry of Foreign Affairs of the Kingdom of Thailand, Thailand's National Position on the Application of International Law to Cyberspace (5 July 2025) https://www.mfa.go.th/en/content/th-s-national-position-on-app-of-il-cyberspace-en; Ministry of Foreign Affairs of the Republic of Korea, National Position of the Republic of Korea on the Application of International Law in Cyberspace (7 July 2025) https://www.mofa.go.kr/viewer/skin/doc.html?fn=20250708095015054.pdf&rs=/viewer/result/202508.

[51] See, for example, the National position of the Netherlands in NATO Cooperative Cyber Defence Centre of Excellence, 'National Position of the Netherlands' (International Cyber Law: Interactive Toolkit, 2019) https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)#Introduction §7.

[52] Nicholas Tsagourias, Russell Buchan and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024).

[53] For example, UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/2625(XXV); UNGA Res 37/10 (15 November 1982) UN Doc A/RES/2625(XXV).

[54] For example, UNSC Res 2171 (21 August 2014) UN Doc S/RES/2171; UNSC Res 2282 (27 April 2016) UN Doc S/RES/2282.

[55] For example, The Constitutive Act of the African Union 2000 art 4(e) on the peaceful resolution of conflicts.

[56] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 33.

[57] See 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.

19. In addition to the means listed above, there are also some special dispute settlement mechanisms that may be relevant to cyber matters specifically. The Budapest Convention on Cybercrime, for example, refers disputes to the European Committee on Crime Problems in the first instance.[58]

20. The ways in which different dispute settlement methods – both diplomatic and adjudicative – might apply in the cyber context is explored below.

A. Non-adjudicative methods of dispute settlement

(i) Negotiation

21. Negotiation usually involves direct conversations between the parties in dispute, without a third party involved. Inter-State diplomacy is a form of negotiation, and to date, this has been the focus of States' responses to malicious cyber operations. The UN Group of Government Experts' Report of 2021 notes that in addition to States' obligations to settle disputes by peaceful means under the UN Charter, States 'could also avail of the full range of diplomatic, legal and other consultative options available to them, as well as voluntary mechanisms and other political commitments that allow for the settlement of disagreements and disputes through consultation and other peaceful means'.[59]

22. Exchanges of views between States at the bilateral, regional and multilateral level can make an important contribution to the peaceful settlement of disputes in the cyber context.[60] In 2015, the UN Group of Government Experts agreed on 11 voluntary cyber norms of responsible State behaviour in the Information, Communication and Technology context, which have helped to build and create a set of expectations among States about what responsible behaviour in cyberspace means in practice.[61] Regional mechanisms, including cyber dialogues within the EU, ASEAN and OAS, can help to promote the peaceful settlement of disputes through enhancing mutual understanding in relation to cybersecurity issues.[62] Some States are also conducting bilateral cyber dialogues.[63]

23. It has also been suggested that there is a role for the UN's International Law Commission as part of negotiations – for example, to prepare the ground for a treaty in relation to cybersecurity, which certain States (particularly Russia, China, Iran, and allies) have advocated for some time. In a statement during the final OEWG session, Iran stated that '[t]he path

[58] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167 art 45.
[59] 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, para 25.
[60] For a detailed discussion on this topic, see Iakovos V Iakovidis, 'The Brave New World of Cyberspace: Do Traditional Diplomatic Tools Apply to Cyber?' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024), pp. 157 – 171.
[61] See, Australian Strategic Policy Institute, The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN (March 2022) https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.
[62] For example, Organization for Security and Co-operation in Europe, 'OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.
[63] For example, the US is engaging in bilateral cyber consultations with several States, including Mexico, Korea, Singapore and Switzerland. See Iakovos V Iakovidis, 'The Brave New World of Cyberspace: Do Traditional Diplomatic Tools Apply to Cyber?' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 158.

towards an ICT-specific applicable international law may need to engage relevant bodies within the UN. The International Law Commission can contribute to these efforts.'[64]

24. However, unlike international adjudication, where all States are equal before the relevant court or tribunal, powerful States have more leverage in international negotiations than less muscular States. Negotiation also relies on political will; some powerful States might not see the point in negotiating with weaker States, and vice versa. Negotiation also depends on diplomatic relations, which may not exist in some cases. For conflicts that are frozen or intractable, negotiation may only exacerbate the dispute or delay its resolution.

(ii) Good offices and mediation

25. 'Good offices' refers to the influence of a third party to facilitate negotiations without directly participating in them. It typically involves an intermediary discreetly intervening behind the scenes to encourage disputes parties to meet or to resume negotiations. The UN Secretary-General has offered to make available his good offices to contribute to the peaceful settlement of conflict stemming from malicious activity in cyberspace.[65] The Secretary-General's Office for Digital Technologies, set up in January 2025 to support the follow up and implementation of the Global Digital Compact, may be a resource in this context. In mediation, a third party is involved in the facilitation of negotiations, for example by clarifying positions and suggesting solutions.

(iii) Conciliation

26. Like good offices and mediation, conciliation involves a third party (either an individual or a panel) trying to facilitate communication between the parties, though the role of the third party is more formal in conciliation – for example, in the form of an expert panel that holds hearings. Conciliation is a bespoke process that has not been used much in recent years.[66] While proposals made as a result of the process are not necessarily binding, conciliation has led to binding outcomes in some cases, as in the successful conciliation conducted through the Permanent Court of Arbitration (PCA) in *Timor-Leste v Australia*.[67]

27. Conciliation may also provide a framework for dialogue and future agreements. An example from the cyber context is the Organization for Security Cooperation in Europe's (OSCE's) 'Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' of 2016.[68]

(iv) Fact-finding

28. Fact-finding, which involves an independent third party looking into the facts of a dispute, has a long history as a means of settling disputes.[69] Traditionally, fact-finding involved two States

[64] Permanent Mission of the Islamic Republic of Iran to the UN, 'Statement by Mr. Heidar Ali Balouji at the 2nd Substantive Sessions of the OEWG on Security of and in the Use of ICTs on "Applicability of International Law"' (30 March 2022) https://newyork.mfa.ir/portal/product/8786/451/Statement-on-. See also Samantha Besson and others, 'The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?' (ESIL Reflections, 3 July 2018) https://esil-sedi.eu/esil-reflection-the-codification-of-the-international-law-applicable-to-cyber-operations-a-matter-for-the-ilc/.

[65] UN Office for Disarmament Affairs, Securing our Common Future: An Agenda for Disarmament (2018) https://front.un-arm.org/documents/SG+disarmament+agenda_1.pdf 56.

[66] For a discussion of conciliation, including in the cyber context, see Pål Wrange, 'The Obligation to Settle Cyber Disputes Peacefully' Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 256.

[67] Timor Sea Conciliation (Timor-Leste v Australia), Report and recommendations of the Compulsory Conciliation Commission Between Timor-Leste and Australia on the Timor Sea (2018)

[68] Organization for Security and Co-operation in Europe, 'OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (10 March 2016) PC.DEC/1202.

[69] Fact-finding was first introduced by the Hague Convention for the Pacific Settlement of Disputes 1899. For a more detailed discussion of its potential application in the cyber context, see Pål Wrange, 'The Obligation to Settle Disputes Peacefully' in Nicholas

agreeing to set up a commission of inquiry, whose findings of fact would sometimes be binding.[70] More recently, fact-finding commissions have been conducted under the auspices of international organizations. For example, UN fact-finding missions have investigated human rights issues in countries such as Syria, Myanmar and Sudan. The use of international fact-finding missions has increased significantly in the last two decades.[71]

29. Where cyber disputes are heavily factual, with a focus on the source of the operation through technical attribution, rather than a violation of the law, fact-finding may be more appropriate than adjudicative methods that have limited capacities to summon or evaluate evidence.[72] In practice, there are many disagreements between States about cyber activity that States deem 'irresponsible' but not necessarily unlawful. For example, the Solar Winds hack resulted in serious national security and commercial effects due to the establishment of vulnerabilities in the networks of many US government agencies, companies and think tanks. The US imposed sanctions and other measures on Russian nationals and entities, 'to make clear that this behaviour was unacceptable'. Yet whether or not this activity violated international law is a matter of debate.[73]

30. Fact-finding may be particularly suited to cyber disputes since the first step in considering the cyber dispute will be identification of the source of the malicious cyber operations, which will require investigation of the tactics, techniques and procedures of the operation on the basis of technical evidence[74] (technical attribution). By analogy, it is possible to think of attribution disputes involving the investigation of complex facts in the physical context, for example, in relation to the downing of Malaysian Airlines flight MH17,[75] which involved evidence from multiple jurisdictions and the use of experts.

31. Even if they are not able to assist in relation to cyber disputes themselves, some existing organizations may provide useful food for thought in terms of structure and process. For example, Fact-Finding Missions have been established under the Organization for the Prohibition on Chemical Weapons (OPCW). In particular, a Fact-Finding Mission responsible for determining whether toxic chemicals were used as weapons in Syria was established in 2014, based on the general authority of the OPCW Director-General to seek to uphold the object and purpose of the Chemical Weapons Convention. On the basis of the Mission's findings, which are ongoing, the OPCW Investigation and Identification Team collects and analyses evidence that may help to identify the perpetrators of chemical weapons attacks in Syria.[76] In the cybersecurity context, there is no treaty equivalent to the Chemical Weapons Convention, but if a treaty emerges in the future (as has been proposed by certain States for some time),[77] there

Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 260.

[70] As, for example, in the Tiger claim, as agreed by the parties: Sinking of the steamer "Tiger" (Germany and Spain) (9 November 1918). See Larissa J van den Herik, 'An Inquiry into the Role of Commissions of Inquiry in International Law: Navigating the Tensions between Fact-Finding and Application of International Law' (2014) 13(3) CJIL 507.

[71] Max Lesch, 'Contested Facts: The Politics and Practice of International Fact-Finding Missions' (2023) 25(3) ILR 1.

[72] Discussed further below in section B.

[73] See, for example, Michael Schmitt, 'Top Expert Backgrounder: Russia's SolarWinds Operation and International Law' (Just Security, December 2020) https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/; Antonio Coco, Talita Dias, and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) EJIL 1275.

[74] See Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 JCSL 229.

[75] Netherlands Prosecution Service, 'The Criminal Investigation by the Joint Investigation Team (JIT)', https://www.prosecutionservice.nl/topics/mh17-plane-crash/criminal-investigation-jit-mh17.

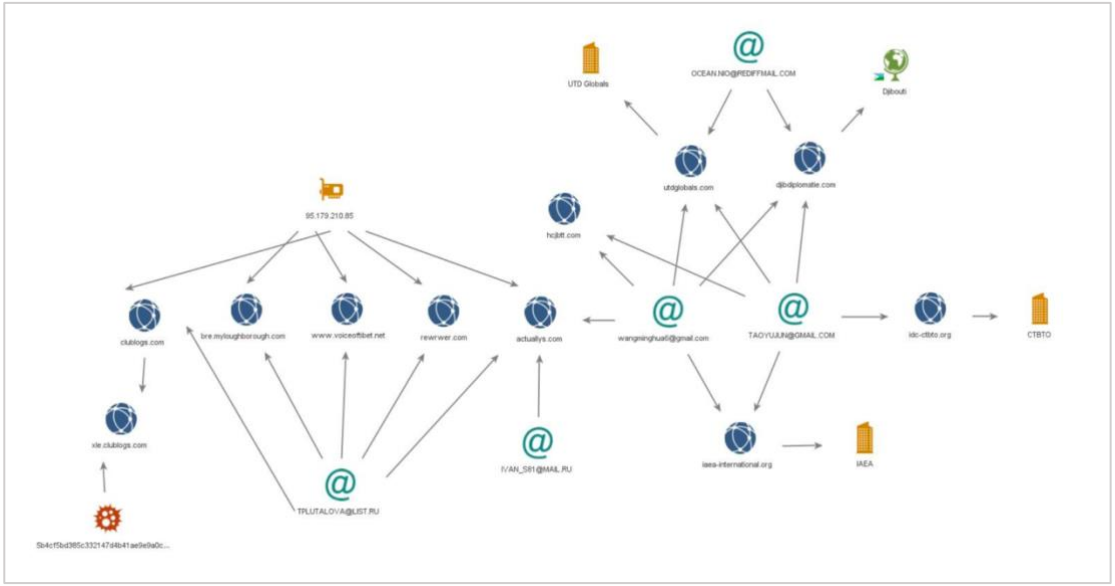
[76] See Organisation for the Prohibition of Criminal Weapons, 'Fact-Finding Mission' https://www.opcw.org/fact-finding-mission. To date, the Fact-Finding mission has issued 21 reports.

[77] See, for example, Statement by the Russian Interagency Delegation at the Tenth Session of the UN Open-Ended Working Group on Security Of and In the Use of ICTs 2021-2025 (New York, 14 February 2025) https://docs-library.unoda.org/Open-

may be opportunities for the establishment of a fact-finding mission under its auspices. Fact-finding may be particularly attractive to victim States that do not have the capabilities to make technical attributions themselves. As more States start to make public political attributions (a trend noted in para 11 above) the potential for formal disputes to develop about the facts of attribution may also increase.

32. However, many States are likely to be sceptical of fact-finding, especially if the cyber intrusion was achieved through means and methods that a victim State or its ally would not want revealed in a courtroom. States may prefer to respond through other means such as naming and shaming, sanctions, or a countermeasure, especially as some international courts do not have procedures for dealing with classified material.

33. Even if States did decide to submit a matter to a fact-finding body, technical attribution of a cyber operation can be challenging because such operations are typically conducted covertly and anonymously, often using techniques that hide the identity of the perpetrator, such as masking tools like VPNs or proxy servers in multiple jurisdictions. The diagram below, showing decoy and non-malicious domains used in malware targeting Uyghur, Tibetan and Taiwanese individuals, illustrates the complexity:



Source: UK National Cyber Security Centre Advisory[78]

34. The ability of States to technically attribute a malicious cyber operation to an individual has improved, including as a result of governments working with the private sector.[79] A fact-finding body would almost certainly need to draw on expert evidence from non-State actors, particularly cybersecurity companies.

Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_OEWG_ICT_security_-__statement_-_international_law_-_ENG.pdf.

[78] UK National Cyber Security Centre and others, BADBAZAAR and MOONSHINE: Technical analysis and mitigation (9 April 2025) https://www.ncsc.gov.uk/files/NCSC-Advisory-BADBAZAAR-and-MOONSHINE-technical-analysis-and-mitigations.pdf.
The Report notes that, 'The mix of masquerading domains and non-malicious domains could suggest the existence of an infrastructure procuring entity used to support the malicious actors' cyber operations.'

[79] See Roy Schondorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 ILS 395.

35. The conclusions of fact-finding bodies facts are not automatically binding; it is for the parties to decide whether to accept them or not. As well as establishing the facts in a case, fact-finding missions may make recommendations and monitor situations. Some fact-finding bodies may also exercise adjudicative functions by identifying violations of international law,[80] as has been the case, for example, with UN Commissions of Inquiry into situations in Burundi,[81] Gaza[82] and Darfur (which also identified perpetrators).[83]

36. The UN Security Council may call upon States to settle their disputes peacefully and recommend an appropriate dispute settlement method,[84] it may investigate a dispute endangering international peace and security by establishing a fact-finding mission,[85] or it may qualify certain malicious cyber operations as a threat to international peace and security under Article 39 of the UN Charter, a prelude to the determination of measures, potentially including the use of force, that can be taken to maintain or restore peace and security.[86] However, the ability of the UN Security Council to act is severely constrained by the use of the veto by the five permanent members.

(v) Proposals for an independent fact-finding and/or attribution mechanism

37. States have engaged in their own fact-finding in order to establish who was responsible for malicious cyber operations. However, as noted above, the particular features of malicious cyber operations make technical attribution challenging, and the ability of States to conduct technical investigation varies. Attribution claims are also often contested by accused States – for example, China contested the US's attribution of the Microsoft Exchange cyber operations to malicious cyber actors affiliated to the Chinese State, claiming that the accusations were unwarranted and 'made up out of thin air',[87] and Iran strongly rejected accusations by Albania that it was responsible for a cyberattack on Albanian government computer systems in 2022.[88]

38. Nor do we have international standards on evidence and proof for technical or political attribution in this context at this time. Some States publish briefs or alerts to encourage increased awareness and build the case for action such as sanctions. For example, the FBI in the US provided a briefing after the destructive attack on Sony pictures, which attributed the operation to North Korea and provided technical detail in support.[89] But while it is generally

---

[80] See Nicholas Tsagourias and Fiona Middleton, 'Fact-Finding and Cyber Attribution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 444.
[81] UN Human Rights Council, 'Detailed Final Report of the Commission of Inquiry on Burundi' (29 September 2017) UN Doc A/HRC/36/CRP.1/REV.1.
[82] As with the Report of the UN Fact Finding Mission on the Gaza Conflict published in 2009: see Emily Alinikoff and Ted Piccone, 'The Goldstone Report: Behind the Uproar' (Brookings Institute, 9 April 2011) https://www.brookings.edu/articles/the-goldstone-report-behind-the-uproar/.
[83] Report of the International Commission of Inquiry on Darfur to the UN Secretary-General (25 January 2005) https://www.legal-tools.org/doc/1480de/pdf/.
[84] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 36.
[85] ibid art 34.
[86] For discussion of this and the role of the UN Security Council in relation to cyber operations more broadly, see Tomohiro Mikanagi, 'The Role of the Security Council in Addressing Malicious Cyber Operations that Threaten International Peace and Security' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024); Talita de Souza Dias, 'Applying Chapters VI and VII of the Charter of the United Nations in the Cyber Context' (United Nations Institute for Disarmament Research, 22 September 2021) https://unidir.org/publication/applying-chapters-vi-and-vii-of-the-charter-of-the-united-nations-in-the-cyber-context/.
[87] See Robert Kolb and Andraz Kastelic, 'Good Faith in the Resolution of Cyber Disputes' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024).
[88] 'Iran rejects involvement in recent Albania cyberattack' (Rudaw, 12 September 2022) https://www.rudaw.net/english/middleeast/iran/120920222.
[89] Federal Bureau of Investigation, 'Update on Sony Investigation' (19 December 2024) https://www.fbi.gov/news/press-releases/update-on-sony-investigation.

understood that an allegation of wrongful behaviour by a State should be substantiated,[90] there is no obligation on States to publicly disclose evidence supporting political attribution claims.[91] However, should a case come to court, a State would be required to provide evidence to support attribution claims – so greater clarity in standards for States in this area would be beneficial.

39. In 2023, the UN Secretary-General recommended 'establishing an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct'.[92] And over the last 10 years, there have been various proposals for an independent fact-finding mechanism to establish the facts underlying attribution claims in the cyber context. As well as helping to resolve disputes around attribution, such a mechanism could facilitate the settlement of a broader dispute of which the cyber attribution dispute may be part, or it may pave the way for a claim before the ICJ or other courts.

40. For example, in 2014, the Atlantic Council proposed a 'Multilateral Cyber Adjudication and Attribution Council' with public and private membership.[93] Under this proposal, if an attribution ruling found against the defendant, the Council would refer cases, alongside its recommendations and evidence, to the UN Security Council, the ICJ, or a 'regional security body'[94] (which presumably includes bodies such as the African Union, ASEAN, European Union or Organisation of American States). In 2017, Microsoft proposed an attribution organisation,[95] alongside the idea of a Digital Geneva Convention.[96] In the same year, the RAND Cooperation proposed a 'Global Cyber Attribution Consortium' that would have the power to formally select cases to be investigated, to collect and assess evidence, to develop specific standards and methodologies, and to attribute and communicate with the relevant parties and through the publication of reports. The Consortium could refer the case to the ICJ or the UN Security Council for further action.[97] Both of these proposals envisaged experts making findings, and a very limited role for participation by States.

41. Various scholars have also mooted the idea of an independent, centralised attribution mechanism. In 2020, Schmitt and Shany proposed an International Attribution Mechanism for Hostile Cyber Operations, which would support States with limited attribution capabilities by providing them with independent access to better intelligence and investigative capacities.[98]

42. None of these proposals have come to fruition. States are unlikely to want to submit evidence, especially classified information such as intelligence, or details of access to computer networks,

[90] For example, the UN Group of Government experts noted in its 2015 report that, 'the accusations of organizing and implementing wrongful acts brought against State should be substantiated': UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174, para 28(f).
[91] This has been affirmed by many States in their national positions in the cyber context, for example, Canada, France, Germany, Israel, the Netherlands, Switzerland, UK and US. See NATO Cooperative Cyber Defence Centre of Excellence, 'Attribution' (International Cyber Law: Interactive Toolkit)
https://cyberlaw.ccdcoe.org/wiki/Attribution#Evidentiary_standards, §3.
[92] UN Secretary General: Our Common Agenda: A New Agenda for Peace (20 July 2023) UN Doc A/77/CRP.1/Add.8.
[93] Jason Healey and others, 'Confidence-building measures in Cyberspace: a Multistakeholder Approach for Stability and Security' (Atlantic Council and the National Defence College, November 2014)
https://www.atlanticcouncil.org/wp-content/uploads/2014/11/Confidence-Building_Measures_in_Cyberspace.pdf 11.
[94] ibid 17. A regional security body in this context presumably includes regional bodies such as the EU, AU, OAS and ASEAN.
[95] Microsoft, An Attribution Organization to Strengthen Trust Online: Policy Paper (2017). This source is not currently available online.
[96] 'The need for a Digital Geneva Convention' (Microsoft, 2017)
https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.
[97] John S Davis II and others, 'Stateless Attribution' (Rand Corporation, June 2017)
https://www.rand.org/pubs/research_reports/RR2081.html.
[98] Yuval Shany and Michael N Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations?' (2020) 96 ILS 196.

to a third party. Cyberspace is also an area in which States have major strategic interests, so they have an interest in retaining control over attributions.[99] There may also be benefits to decentralised attribution, in which multiple actors – including States and non-State actors (such as cybersecurity companies and Computer Emergency Response Teams (CERTs))[100] – cooperate, as the credibility of the assessment may be bolstered when it is depoliticised and endorsed by more than one institution.[101] Cybersecurity experts play a vital role as neutral sources of attribution, both to expose State activity and to provide evidence to support public attributions made by States. There has been some support in the UN for the sharing of good practices on the source of cyber incidents, including the recent establishment of a Points of Contact Directory that encourages CERTS to exchange information on urgent or significant cyber incidents.[102] The CyberPeace Institute (co-funded by Microsoft, Mastercard and Hewlett Foundation), while not a formal attribution mechanism, carries out investigations that can help other actors conducting attribution assessments.[103] Its findings may also be helpful for other quasi-judicial or judicial bodies, as may the findings of private cybersecurity companies such as Mandiant (part of Google) or CrowdStrike.

43. More recent proposals seek to address some of the challenges discussed above with regard to independent fact-finding. Tsagourias and Middleton outline the features of a treaty-based cyber attribution fact-finding mechanism that could be created by States voluntarily, on an ad hoc basis, in relation to a particular cyber attribution dispute. The treaty, as a constitutive instrument, could set out the fact-finding mechanism's composition, mandate and methodology.[104] Delerue has proposed a mechanism designed for the pre-dispute phase, when the victim State conducts the investigation, collects and assesses evidence, and evaluates possible next steps.[105] He proposes that the mechanism could be created as an international organization open to States, CERTs, NGOs and private cybersecurity companies, and could assess existing evidentiary standards for attribution of cyber operations used in different contexts and propose rules and standards specifically tailored for the international context. The mechanism could serve as a basis for fact-finding missions and could maintain lists of technical, legal and policy experts on which States and other actors could draw. The mechanism could help to connect relevant experts with States requesting assistance. Delerue notes that his proposed mechanism 'could, to a limited extent, play a similar role to the Permanent Court of Arbitration (PCA) outside its adjudication functions'.[106]

(vi) Leveraging existing mechanisms for fact-finding

44. Rather than disputing States having to start from scratch in setting up a fact-finding mechanism, which is resource- and time-intensive, there may be scope to draw on existing institutions to facilitate fact-finding in the cyber context. For example, the PCA itself, with its long history of independent and impartial facilitation of dispute resolution in the international space through fact-finding, inquiries, mediation, conciliation and arbitration, may be well placed to assist on cyber disputes, for example through facilitating the formation of a panel of

[99] Nicholas Tsagourias and Fiona Middleton, 'Fact-Finding and Cyber Attribution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 459.
[100] A CERT consists of a group of cybersecurity experts that prevent, detect and respond to large-scale cyber security incidents.
[101] See Kirsten Eichensehr, 'Decentralized cyberattack attribution' (2019) 113 AJIL Unbound 213.
[102] UN Office for Disarmament Affairs, 'Global Intergovernmental Points of Contact Directory on the Use of Information and Communications Technologies in the Context of International Security' https://poc-ict.unoda.org.
[103] See CyberPeace Institute https://cyberpeaceinstitute.org.
[104] Nicholas Tsagourias and Fiona Middleton, 'Fact-Finding and Cyber Attribution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 464.
[105] Francois Delerue, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) 106 QIL, Zoom-in 5, 19.
[106] ibid 19.

experts (standing or ad hoc) that could opine in this area, with the PCA serving as a registry. There is precedent for the PCA offering a venue for particular branches of international law that benefit from scientific or technical expertise: the PCA provides specialized lists of arbitrators in relation to disputes on the environment and on outer space.[107]

45. There is a spectrum of roles that the PCA might play. At one end would be the establishment of a panel of experts that could examine the facts of what happened in the cyber incident and the source of the cyber operation, i.e. technical attribution. The composition of any such panel would of course be crucial, in order to encourage States to have recourse to the panel. Currently, there is no list of cyber experts to whom a victim State may go in relation to a cyber dispute; as cyber is a technical and complex field, and one in which States are increasingly engaged in offensive operations, there may be value in a standing panel composed of international law and technology experts, ideally security-cleared under national or international procedures. The advantage of a standing panel would be that prior knowledge of the experts involved may help instil confidence in the parties bringing the claim. An ad hoc panel may face the challenge that there is a limited number of experts qualified in this area. To ensure the confidence of the parties in the members of the panel, the parties could have the right to bring challenges in relation to potential conflicts of interests and could have recourse to an appointing authority in the selection of members, if appropriate.[108] Rules catering to classified evidence could also help build confidence for the States appearing before the panel.

46. Such a fact-finding process could either be free-standing or an initial step in a broader dispute settlement process. In any such process, it would be critical to address and resolve the issue of consent to jurisdiction, which remains the fulcrum for adjudicatory dispute settlement in international law, although not necessarily pivotal to fact-finding, inquiry good offices and mediation.

47. Either in parallel, or as part of a separate process, there is also the potential for a panel of experts to advise or assist on rules of procedure in relation to cyber disputes – as the Permanent Court of Arbitration has done, for example, in devising its Optional Rules for Conciliation of Disputes Relating to Natural Resources and the Environment.[109]

Further areas for consideration

48. Another area that might merit the attention of an independent group of experts is the rules on evidence in cyber cases. Expert evidence in cyber cases can be highly technical and complex – involving, for example, IP logs, telemetry reports, and digital forensics. Cyber cases are also likely to involve digital evidence, which raises the issue of how courts should handle the risks of AI-generated, or AI-manipulated, evidence. All courts are grappling with how to modernise in the face of rapid technological innovation; the development of rules that take account of these issues, and identify any relevant best practice, could be helpful for the ICJ and other international courts and tribunals, as and when a cyber-related dispute comes before them.

[107] See PCA, 'Panels of Arbitrators and Experts' www.pca-cpa.org/en/about/panels.
[108] For the relevant procedure, see PCA, 'Appointing Authority' https://pca-cpa.org/en/services/appointing-authority/.
[109] PCA Optional Rules for Conciliation of Disputes Relating to Natural Resources and/or the Environment https://docs.pca-cpa.org/2016/01/Optional-Rules-for-Conciliation-of-Disputes-Relating-to-the-Environment-and_or-Natural-Resources.pdf.

49. More ambitiously, there is scope to explore the possibility of developing common standards for evidence and proof on legal attribution.[110] Currently, questioning the lack of standards used in attribution is a common tactic by States accused of malicious cyber operations. Experts could also consider innovative proposals in this area, for example that there should be new standards for legal attribution in the cyber context,[111] or liability based on tort law and international law principles.[112]

50. Currently, as discussed further below, the application of international law to cyber operations is unsettled, but as understandings in this area mature, and victim States (particularly less powerful States, without attribution capabilities of their own) look for dispute settlement options in relation to cyber activities, the prospects of fact-finding by an independent body may become more compelling.[113] Each of these options represent incremental steps, some of which anticipate potential pathways for cyber dispute settlement some way in the future, but all are ripe for further discussion.

B. Adjudicative methods of dispute settlement

51. Arbitration and judicial settlement involve an independent third party (either an arbitrator or judge) resolving a dispute with a decision that is usually binding on the parties. All States are treated equally before international courts and tribunals,[114] therefore, international adjudication can level the playing field compared with, for example, negotiation discussed above.[115]

52. However, the international adjudication of cyber cases presents significant challenges, including the limited jurisdiction of international courts, and difficulties with fact-finding and evidence, particularly to support technical and legal attribution. It is notable that while some States have sought legal advice on the option of bringing an inter-State claim concerning malicious cyber operations before a court or arbitral tribunal, to date no States have brought such a claim.

53. There are several reasons for this. First, the option of adjudication may be limited in cyber cases, and more generally, the jurisdiction of international courts is contingent on the consent of the parties involved. In practice, many States are reluctant to consent to a third party deciding on the lawfulness of a dispute, and States are especially hesitant to provide such

    consent in advance of an actual dispute arising.[116] So there may be no forum that can hear an inter-State dispute (and even where there is one, there may be limited options to enforce a judgment).

[110] For arguments in favour of this, see Kristen Eichensehr, 'The Law & Politics of Cyberattack Attribution', (UCLA Law Review, 2020) https://www.law.virginia.edu/scholarship/publication/kristen-eichensehr/927871; Francois Delerue, 'Reflections on the Opportunity of an International Attribution and Accountability Mechanism for Cyber Operations' (2024) 106 QIL, Zoom-in 5, 20.
[111] See Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges' (2020) 31(3) EJIL 941, 962-5, where the authors propose adjusting attribution determinants in the cyber context, particularly in relation to Article 8 of the Articles on State Responsibility, so that the lower standards of 'overall control' and 'soft control' apply in certain situations, as well as the inclusion of implicit instructions as an attribution determinant.
[112] See Rebecca Crootof, 'International Cybertorts: Expanding State Accountability in Cyberspace' (2018) 103 CLR 565.
[113] See Nicholas Tsagourias, 'Cyber Attribution Agencies: A Sceptical View' (2024) 106 QIL, Zoom-in 23, 37-8.
[114] In the case of arbitration, this is provided that arbitrator selection is done properly.
[115] At paras 21-24.
[116] See generally, Robert Kolb, Reservations to Optional Declarations Granting Jurisdiction to the International Court of Justice (Edward Elgar Publishing 2024) 116, noting that the number of declarations in relation to the total number of States in the world has steadfastly declined, and that declarations that are made are increasingly accompanied with restrictive reservations, and sometimes withdrawn.

54. Second, specifically in the cyber context, States so far have rarely characterised cyber operations against them as breaches of international law.[117] For example, in its letter to the UN General Assembly and the Security Council about the cyber operations that were allegedly carried out by Iran in Albanian territory, Albania referred to the cyber operations as 'a blatant breach of the norms of responsible peacetime State behaviour in cyberspace', without reference to international law.[118] One of the reasons for this may be that States – at least those who are major cyber powers – may not wish to limit their own operational freedom, so they often describe cyber operations against them as 'malicious' or 'irresponsible' rather than 'unlawful'. If a State does not consider that there has been a violation of international law, or because of self-interest does not want to characterise it as such – preferring to maintain a position of strategic ambiguity – it will not seek to bring the matter before an international court.

55. Third, there is a lack of clarity about how international law applies in the cyber context. Only 15 years ago, there were debates about whether international law applied to cyberspace at all. Since then, States have agreed in the UN and in other international organisations that international law does apply in the cyber context;[119] the real question is *how*. In the last ten years, over 100 States have published their views on this issue (including regional statements by the African Union and European Union). While there are some areas of convergence between States, at least at the general level (the application of the rules on peaceful settlement of disputes being one such area), in other areas (for example, sovereignty and due diligence) there are divergent views about the applicability and contours of international law rules.[120] Given the unsettled state of the law at the current time, there is a lack of predictability as to how a Court would rule on a particular case. Powerful cyber-active States, in particular, are unlikely to want to risk unpredictable judgments in an evolving area with significant policy implications.

56. Still, States' views on the application of customary international law in the cyber context have certainly evolved in the last ten years through the growing numbers of national and common positions. In the context of the UN Open Ended Working Group (OEWG) in July 2025, some States outlined areas of convergence in relation to the application of certain areas of international law to cyberspace.[121] There is also soft law in this area, in the form of the UN norms of responsible State behaviour in cyberspace,[122] as well as the various reports of the UN's Group of Government Experts (GGE) and OEWG, and influential publications such as the Tallinn Manuals on the International Law Applicable to Cyber Operations. As and when States reach greater agreement on the application of international law in the cyber context, the option of

[117] See Nicholas Tsagourias, 'Cyber Disputes as International Legal Disputes', in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 29.
[118] Letter dated 7 September 2022 from the Permanent Representative of Albania to the United Nations addressed to the Secretary-General and the President of the Security Council (9 September 2022) UN Doc A/76/943-S/2022/677.
[119] See Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174; Report of the open-ended working group on security of and in the use of information and communications technologies (8 August 2021) UN Doc A/77/275; Final report of the open-ended working group on security of and in the use of information and communications technologies (1 July 2025) UN Doc A/AC.292/2025/L.1.
[120] See NATO Cooperative Cyber Defence Centre of Excellence, 'International Cyber Law in Practice: Interactive Toolkit' https://cyberlaw.ccdcoe.org/wiki/Main_Page for views of States on how different rules of international law apply in the cyber context.
[121] See Report prepared by 21 States, 'Working Paper on the Application of International Law in the Use of ICTs: Proposed Text Outlining Areas of Convergence for Inclusion in the 2025 Final Report International Law Section' (United Nations Office on Drugs and Crime, 2025) https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_-_Cross-regional_Working_Paper_on_International_Law_-_11_July_2025.pdf.
[122] UN Office for Disarmament Affairs, 'The UN norms of responsible state behaviour in cyberspace' https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

bringing a case may become more attractive. This may be particularly true for non-Western States, which are increasingly bringing cases before international courts.[123] Unlike powerful cyber-active States, many States do not have the capacity to bring domestic indictments, launch retorsions, or take countermeasures in response to cyber operations. Such States are also less exposed to the risk of an international court making a finding that it is unhelpful to their operational freedom to conduct cyber espionage or offensive cyber operations of their own.

(i) Arbitration

57. Arbitration is provided for in a number of bilateral and multilateral treaties as part of the applicable dispute settlement process. This can be through an ad hoc process or through an institution such as the PCA. As of October 2025, the PCA is hearing seven inter-State arbitrations, having previously resolved 52 inter-State disputes through its arbitration facilities.[124] But to date, there has not been a public inter-State arbitration involving malicious cyber operations.[125]

58. International investment agreements typically allow foreign investors to bring international law claims against a host State in the event that the State breaches its treaty obligations, and may provide the basis for a claim in relation to cyber activity on the territory of the host State that harms the interests of investors.[126] However, such claims would be brought by foreign investors rather than States, and therefore are outside the scope of this Brief.

59. There are some advantages to arbitration in the cyber context. Arbitration allows the parties to customise the process by choosing the applicable law; selecting the arbitrators; setting the rules for evidence, discovery and timelines (including expedited timelines, if appropriate); agreeing whether the decision of the arbitrators should be binding and enforceable on the parties; and deciding whether to keep the decision confidential. The process is therefore more flexible than adjudication before a court. Arbitration can cater to large volumes of technical evidence, as it is possible to select arbitrators with relevant technical expertise, and to involve technical experts.[127]

60. Take a scenario in which a State's intelligence agency taps into submarine cables constructed and owned by another State, then interferes with the cables' transmission of data, disrupting internet services in the State owning the cables. The victim State may wish to bring a claim for violation of international law.[128] Article 287 of the United Nations Convention on the Law of the Sea (UNCLOS) provides that States parties may choose, by means of a written declaration, one or more means of settling disputes on the interpretation or application of UNCLOS.[129] Where a

[123] Ignacio De la Rasilla notes that State practice shows a marked increase in participation before the ICJ by non-Western States since 2000, including by Latin American and Caribbean States between 2000-24: See Ignacio De la Rasilla 'Latin America and the Caribbean in the International Court of Justice—An Empirical Quantitative Analysis (2000-24)' (2025) 16(2) Journal of International Dispute Settlement 1.
[124] PCA, 'Cases' https://pca-cpa.org/cases/.
[125] However, as not all inter-State arbitration decisions are made public, it is not possible to know for certain.
[126] For example, if the investor's business suffers huge losses as a result of a ransomware operation on the State's power grid that exploits weak cybersecurity, and the investor alleges that the host State failed to carry out adequate due diligence, such as oversight of the implementation of basic cybersecurity measures, that would have prevented the malicious cyber operation from succeeding.
[127] For example, the PCA's Optional Rules for Arbitrating Disputes between Two States 1992 art 27 provides that 'the arbitral tribunal may appoint one or more experts to report to it, in writing, on specific issues to be determined by the tribunal'.
[128] For discussion of the application of international law to submarine cables to see Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017), Rule 54 and Commentary.
[129] States have the option to bring a claim before an arbitral panel under Annex VII; the ICJ; the International Tribunal on the Law of the Sea; or a special arbitral tribunal constituted in accordance with Annex VIII.

dispute is not covered by a declaration in force, a State Party to the dispute is deemed to have accepted arbitration in accordance with Annex VII of UNCLOS, which provides for a compulsory, five-person panel arbitral procedure, for which the Permanent Court of Arbitration often acts as registry.

61. An argument might be made that Article 101 of UNCLOS, which refers to acts committed against a ship, aircraft, persons or property in a place outside the jurisdiction of any State, is engaged by acts of piracy on subsea cables,[130] and that piracy in this context covers both physical activity (splicing cables to install devices) and cyber activity (listening to and interfering with the transmission of data through the cables). Alternatively, Article 113 mandates States to make it a punishable offence for ships and individuals under their jurisdiction to damage submarine cables, whether intentionally or through negligence. It is unclear if either Article 101 or 113 of UNCLOS could cover cyber as well as physical activity – this is something that could be tested through arbitration. If cyber activity is included within the scope of Article 113, and if the accused State had not made the damaging of cables an offence, an injured State may argue that the accused State has violated its obligations under UNCLOS.[131] Under Article 304 of UNCLOS, remedies provided for under the general law of State responsibility are available to claimants, in addition to any provisions in UNCLOS on responsibility and liability for damage (not applicable on these facts). Remedies under the rules on State responsibility include declaration of a breach; restitution; compensation; and satisfaction.[132]

62. The Tallinn Manual 2.0 provides other examples of how cyber operations may violate UNCLOS. This includes – in the context of a State's territorial waters – cyber activities designed to collect information prejudicial to the security of the coastal State or cyber operations intended to interfere with communication systems or other facilities or installations of the coastal State.[133] An example of the latter occurred in August 2025, when a hacker group known as Lab-Dookhtegan claimed responsibility for a cyber operation on Iran's maritime sector, disabling communications on more than 60 oil tankers and cargo ships.[134]

63. Compliance with inter-State arbitration is difficult to measure because some awards are confidential. Recent empirical work on compliance in 260 Investor State Dispute Settlement cases in which States were in breach of their treaty obligations found that 31% of awards remained unresolved.[135]

(ii) Litigation before the International Court of Justice (ICJ)

64. For inter-State cases, the ICJ is the obvious option for adjudication, as the only international court with general jurisdiction to hear a case on any question of international law involving States.[136] Judicial decisions, as subsidiary means for the determination of rules of law,[137] may

[130] Jacques Hartmann, 'Piracy and Undersea Cables: An Overlooked Interpretation of UNCLOS?' (EJIL:Talk!, 6 March 2025) https://www.ejiltalk.org/piracy-and-undersea-cables-an-overlooked-interpretation-of-unclos/.
[131] For this novel argument, see Jason Petty, 'How Hackers of Submarine Cables May be Held Liable under the Law of the Sea' (2021) 22(1) Chicago Journal of International Law 260 https://cjil.uchicago.edu/print-archive/how-hackers-submarine-cables-may-be-held-liable-under-law-sea.
[132] See ILC, Articles on Responsibility of States for Internationally Wrongful Acts (2001) YILC vol.II (Part Two) arts 34-36.
[133] Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017), Rule 48 and Commentary, para 6.
[134] Safety4Sea, 'Hackers launch cyber attack targeting Iranian fleet' (25 August 2025) https://safety4sea.com/hackers-launch-cyber-attack-targeting-iranian-fleet/.
[135] Nicola Strain and others, 'Compliance politics and international investment disputes: a new dataset' (2024) 27 Journal of International Economic Law 70, 83 (analysing relevant cases up to 31 December 2020).
[136] Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 36(2).
[137] ibid art 38(1).

help to resolve broader questions about the application of a particular treaty, or of customary international law.

65. States have had increasing recourse to the ICJ in recent years: 39 cases (20% of all cases ever brought to the Court) have been filed in the last decade, and nine cases were filed between April 2023 and 2024 alone (four times the annual average of earlier years).[138] Two thirds of all UN Member States are engaged in proceedings before the ICJ at this time, whether as applicants, respondents, interveners or participants in Advisory Opinions.[139] One factor spurring international litigation is that political options for resolving international disputes – such as recourse to the UN Security Council – are increasingly difficult in today's geopolitical climate.

66. At first glance, the ICJ may not appear to be an appropriate forum for accountability for malicious cyber operations, despite its general jurisdiction and expanding docket. There are general challenges, including the limited bases of jurisdiction and the risk of States failing to appear or comply.[140] ICJ judgments are technically only binding on the parties to the dispute.[141] Bringing a case before the ICJ is expensive and requires significant legal expertise, both of which can hinder access to justice, especially for developing States.[142] It is also a slow route to accountability: on average, ICJ cases take 3–5 years from the filing of the application until judgment is delivered.[143] Addressing cyber disputes through political, diplomatic or operational measures is likely to be quicker. A powerful State may prefer the option of negotiation, or to not resolve the dispute at all.

a) Existence of a dispute

67. A number of additional issues may make the Court an unlikely venue for the adjudication of disputes relating to cyber operations. In the first place, the Court would need to decide whether a 'dispute' arises in the context of the case.[144] The ICJ has held that this requires 'a disagreement on a point of law or fact, a conflict of legal views or of interests between two persons', a position which is broadly accepted and has acquired customary law status.[145] It might be argued that where a State that is accused of certain cyber activity contests the facts laid out in a public attribution statement, or denies involvement, that State is disputing that the activity itself can be ascribed to it – a factual dispute. For example, in 2020 the UK accused Russia of hacking labs conducting research into Covid vaccines. The Russian ambassador denied Russia's involvement.[146] If the accusation were also to allege that the cyber activity constitutes a

[138] Alexander Wentker, 'More and more cases on war and genocide are being litigated at the ICJ' (Chatham House, 4 September 2024) https://www.chathamhouse.org/2024/09/more-and-more-cases-war-and-genocide-are-being-litigated-icj.
[139] Philippa Webb, 'Double Waiver of Immunity and Ripple Effects' (3VB/NUS Arbitration Lecture 2024, 14 May 2024) https://3vb.com/wp-content/uploads/2024/06/Double-Waiver-and-Ripple-Effects_website-version_Webb.pdf.
[140] Michael Wood, 'International Dispute Settlement: A Bright or Depressing Future?' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 502.
[141] Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 59.
[142] Although there is a fund to support States appearing before the ICJ, and counsel may work at pro bono or reduced rates for developing countries.
[143] Fiker Institute, 'Reforming the ICJ' (October 2022) https://www.fikerinstitute.org/publications/reforming-the-international-court-of-justice.
[144] Statute of the International Court of Justice (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 36(2).
[145] Mavrommatis Palestine Concessions (Greece v UK) (Objection to the Jurisdiction of the Court) [1924] PCIJ Series A No 3, 19.
[146] Agence France-Presse, 'Russia's Ambassador to UK Denies Coronavirus Vaccine Hacking Claims' (The Guardian, 19 July 2020) https://www.theguardian.com/world/2020/jul/19/russias-ambassador-to-uk-denies-coronavirus-vaccine-hacking-claims.

violation of international law and this aspect of the claim were denied, that could also form the basis of a legal dispute.[147]

68. In practice, however, States often remain silent in the face of statements attributing malicious cyber operations to them, rather than mount a formal legal claim or defence.[148] Should silence on the part of a State be construed as a response, leading to the existence of a dispute?[149] In *Gambia v Myanmar (Preliminary Objections)*, the ICJ stated that it did not require the respondent to expressly oppose the claims of the applicant, and that where the respondent has failed to reply to the applicant's claims, 'it may be inferred from this silence, in certain circumstances, that it rejects those claims and that dispute exists at the time of the application'.[150] While there are various reasons for States to remain silent (for example because they wish to de-escalate, do not have diplomatic relations, or lack a functioning government),[151] the Court's recent case law suggests that if the claim calls for a reply, silence could indeed be construed as a response.[152]

b) Jurisdiction

69. In addition, the Court's jurisdiction is limited in ways that may preclude the submission of many disputes before the Court. There are four ways in which the ICJ can have jurisdiction, as set out in the ICJ Statute.[153] First, States can make an Optional Declaration, in which they accept the compulsory jurisdiction of the Court over particular issues provided for in Article 36(2) of the ICJ Statute. Only 74 States currently have Article 36(2) declarations in force, including only one of the five permanent members of the UN Security Council (the UK, but with reservations). Second, two or more States may reach a special agreement (*compromis*) to submit a dispute to the Court, but this is only used in about 15% of cases and is unlikely to be relevant in the cyber context, where States are conducting malicious operations.[154] Third, one State can bring a case to the ICJ and invite the other to consent to the Court's jurisdiction (*forum prorogatum*),[155] but this has been rarely used.[156] As noted above, it is unlikely that a State accused of carrying out a malicious cyber operation would agree to let a third party decide on its lawfulness.[157] A fourth and more promising basis for jurisdiction in the cyber context is a compromissory clause, ie a clause in a treaty that requires a dispute involving interpretation or application of the treaty to be submitted to a specific court, such as the ICJ. There are over 300 treaties with ICJ

[147] For a detailed analysis of how cyber disputes transform into international legal disputes, using this example and others, see Nicholas Tsagourias, 'Cyber Disputes as International Legal Disputes' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 13-37.
[148] Joseph M Brown and Tanisha M Fazal, '#SorryNotSorry: Why States Neither Confirm Nor Deny Responsibility for Cyber Operations' (2021) 6(4) European Journal of National Security 401.
[149] The ICJ has also held that the existence of a dispute can be inferred 'from the failure of a State to respond to a claim in circumstances where a response is called: see, for example, Application of the Convention on the Elimination of All Forms of Racial Discrimination (Georgia v Russian Federation) (Preliminary Objections) [2011] ICJ Rep 70 [84].
[150] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Gambia v Myanmar) (Preliminary Objections) [2022] ICJ Rep 477 [71].
[151] See Nicholas Tsagourias, 'Cyber Disputes as International Legal Disputes' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 28.
[152] See also Duncan Hollis and Eneken Tikk, 'Peaceful Settlement in International Law' (2022) 57(2) Texas International Law Journal 2, 19.
[153] Statute of the ICJ (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 36(1)-(2); ICJ Rules of Court 1978, art 38(5).
[154] Statute of the ICJ (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 36(2).
[155] ibid art 36(1); International Court of Justice Rules of Court 1978 art 38(5).
[156] There has only been one case since 1951 in which the ICJ's jurisdiction relied on this basis; see Vincent Pouliot, 'Forum prorogatum before the International Court of Justice: the Djibouti v France case' (2008) 3 Hague Justice Journal 28 https://www.haguejusticeportal.net/Docs/HJJ-JJH/Vol_3(3)/Journal%20-%20Pouliot%20-%203.3%20-%20EN.pdf.
[157] However, public rejection of the invitation to participate may count against the accused State reputationally, especially if it has, in its national position on the application of international law to cyberspace or in the UN, affirmed the importance of international law principles in the cyber context.

compromissory clauses,[158] and the scope of some of these may be relevant to disputes about malicious use of ICTs.

70. To invoke the ICJ's jurisdiction on this basis, the first step would be to find a treaty to which the State(s) engaged in the malicious cyber activity are parties. As noted earlier, the data suggests that for those cyber operations that are sponsored by States, a relatively small number of States are responsible.[159] There are certain treaties with compromissory clauses that have many States parties, which may provide a basis for the ICJ's jurisdiction. For example, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Montreal Convention) has 190 States parties and may be relevant in the event of cyber interference in aviation systems, and the Convention on the Elimination of Racial Discrimination has 182 States parties and might be relevant, for example, if cross-border cyber surveillance or disruption specifically targeted a racial or ethnic group.[160] In practice, this avenue – which is examined in a hypothetical case study later on in the Brief – is likely to be the most promising basis for establishing the ICJ's jurisdiction in a cyber case.[161]

c) Evidential challenges

71. Even assuming jurisdiction is established, the ICJ would need to determine that the malicious cyber activity was attributable to the defendant State before turning to the application of the law. This may be an impediment, as the Court has more limited fact-finding powers and abilities than a criminal court. The Statute of the ICJ and the Rules of Court do not require specific standards of proof – the standard used by the Court is flexible and depends on various factors, including the gravity of the case in question.[162]

72. As noted above, States may also be unwilling to disclose intelligence linking the malicious cyber activity to a State due to national security considerations.[163] The ICJ's Rules of Procedure do not have provisions to protect sensitive evidence, unlike those, for example, of the International Criminal Tribunal for the former Yugoslavia (ICTY),[164] the European Court of Human Rights,[165] and some domestic frameworks.[166] And the ICJ has been reluctant to draw inferences from the refusal of a State to produce confidential documents.[167] However, the ICJ does have some

[158] The State of Switzerland and others, Handbook on accepting the jurisdiction of the International Court of Justice (United Nations 2014) https://legal.un.org/avl/pdf/rs/other_resources/Manual%20sobre%20la%20aceptacion%20jurisdiccion%20CIJ-ingles.pdf.
[159] See Council on Foreign Relations, 'Cyber Operations Tracker' https://www.cfr.org/cyber-operations/, discussed at para 8 above.
[160] International Convention on the Elimination of Racial Discrimination (adopted 7 March 1966, entered into force 4 January 1969) 660 UNTS 195 art 22 contains a compromissory clause.
[161] Note, however, that some States may seek to limit their consent to be bound by compromissory clauses through lodging reservations to the treaty.
[162] Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50(2) Texas International Law Journal 240; See also Jinan Bastaki, 'Whose reasonable inference? The ICJ's Advisory Opinion and the threshold for apartheid's mens rea' (EJIL:Talk!, 2024) https://www.ejiltalk.org/whose-reasonable-inference-the-icjs-advisory-opinion-and-the-threshold-for-apartheids-mens-rea/.
[163] See para 32 above.
[164] See International Criminal Tribunal for the former Yugoslavia Rules of Procedure and Evidence 2015, Rules 66C and 68(iv).
[165] See the discussion in para 108 on Rule 44F of the European Court of Human Rights' Rules of Court.
[166] For example, the Classified Information Procedures Act 1980 in the US, which provides for the use of classified evidence, or substitutions of that evidence, in criminal cases, or the Closed Materials Procedure under the Justice and Security Act 2013 used in some judicial proceedings in the UK.
[167] Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50(2) Texas International Law Journal 240, 257, 269, noting that in Corfu Channel and Bosnian Genocide cases the Court declined to draw any inferences from refusal to produce evidence. See Corfu Channel (UK v Albania) (Merits) [1949] ICJ Rep 4; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 43.

powers to protect the identity of witnesses and hear evidence *in camera*, if necessary, as it did in the *Bosnian Genocide* case.[168]

73. States also may not wish to submit evidence obtained through unauthorised intrusions into another State's computer systems, which some States and scholars consider can amount to a violation of international law.[169] There is no express rule in the ICJ Statute providing that evidence obtained through a violation of international law is inadmissible. Instead, the Court assesses the "weight, reliability and value" of the evidence presented in deciding whether the evidence is or should be "eliminate[d] from further consideration".[170] Roscini notes that in the *Corfu Channel* case, the ICJ did not dismiss evidence illegally obtained by the UK in Operation Retail; on the contrary, the Court relied on the evidence in order to determine the place of the accident and the nature of the mines.[171] Nevertheless, States may be reluctant to provide the evidence, and if they do, the manner of obtaining it may aggravate the dispute.[172]

74. Since digital evidence is vulnerable to manipulation, especially with developments in AI, issues surrounding the authenticity of digital evidence are likely to arise. While there is no explicit procedure for challenging the authenticity of evidence, the party producing the digital evidence will have to prove that it is authentic, accurate and complete.[173] The Court may choose to engage technical experts to help test these factors independently. As well as the veracity and reliability of digital evidence in a cyber case, the complexity of the evidence (for example, technical telemetry and malware reports) may bring challenges, raising the question of how much deference the judges should give to experts, and whether there is value in offering opportunities for knowledge exchange or training to judges and Registry officials in this area.

75. However, in principle, all evidence is admissible before the ICJ, including evidence in digital form,[174] and the Court then gives that evidence the probative weight that it considers appropriate.[175] And increasingly, ICJ judges are faced with complex, heavily contested, fact-intensive cases. For example, in the pending *South Africa v. Israel* proceedings, South Africa's memorial alone reportedly comprised approximately 750 pages of textual argument and analysis, supported by over 4,000 pages of exhibits and annexes.[176] Parties can also provide

---

[168] James Devaney, 'Evidence: International Court of Justice' (Max Planck Encyclopaedias of International Law, 2018) https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3430.013.3430/law-mpeipro-e3430?prd=OPIL para 24. See Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 43.

[169] See, for example, Common Position of the African Union on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace (International Cyber Law: Interactive Toolkit, 2024) https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024) para 15, see also Kevin Jon Heller, 'The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace' (OpinioJuris, 5 February 2024) https://opiniojuris.org/2024/02/05/the-african-union-rightly-endorses-pure-sovereignty-in-cyberspace/.

[170] Armed Activities in the Territory of the Congo (DRC/Uganda) (Judgment) [2005] ICJ Rep 168 [59]; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 130 [213].

[171] Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50(2) Texas International Law Journal 240, 271. See Corfu Channel (UK v Albania) (Merits) [1949] ICJ Rep 4.

[172] See Robert Kolb and Andraz Kastelic, 'Good Faith in the Context of the Resolution of Cyber Disputes' in Nicholas Tsagourias, Russell Buchan, and Daniel Franchini (eds), The Peaceful Settlement of Inter-State Cyber Disputes (Bloomsbury Publishing 2024) 59.

[173] Antonio Segura Serrano, 'International Dispute Settlement: Digital Evidence and Online Dispute Resolution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 470.

[174] See ICJ Practice Direction IXbis (31 October 2001) which refers to digital evidence at §2(i).

[175] Antonio Segura Serrano, 'International Dispute Settlement: Digital Evidence and Online Dispute Resolution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 479 lists factors the Court may take into account in assessing probative weight.

[176] Republic of South Africa, 'South Africa Delivers Evidence of Israel Genocide to ICJ' (28 October 2024) https://www.gov.za/news/media-statements/south-africa-delivers-evidence-israel-genocide-icj-28-oct-2024.

evidence through witnesses, experts and expert witnesses. The Court has been making creative use of oral and expert evidence – for example, having recourse to scientific and expert evidence in its Advisory Opinion on Climate Change.[177] The ICJ even met privately with the Intergovernmental Panel on Climate Change in order to better understand climate science.[178] A cybersecurity company such as CrowdStrike, or an intergovernmental organization such as Europol or Interpol, could provide expert evidence to a State, which could pass it on to the Court in its written and oral submissions.

76. Oral evidence played a significant role in the *Whaling in the Antarctic* case, for example, in which the cross-examination of the expert witnesses of Japan and Australia helped the Court to conclude that the special permits granted by Japan for the killing, taking and treatment of whales had not been granted for the purposes of scientific research.[179] In oral submissions in the provisional measures phase of the *South Africa v Israel* case, open source digital evidence was shown to the judges, including satellite imagery and videos of the situation in Gaza.[180]

77. In recent years, the ICJ has also made greater use of its own fact-finding powers, which had not been deployed for many years.[181] The Court is able to appoint independent experts to assist it,[182] which may be helpful in a cyber case involving technical complexities. In the *Caribbean Sea* case, the ICJ appointed two of its own experts to provide technical assistance to the Judges.[183] Factual determinations made by other UN organs, for example in the form of a UN General Assembly resolution or UN report, play an increasingly prominent role in ICJ proceedings.[184] In a cyber case, the various reports of the Group of Government Experts (GGE) and UN Open Ended Working Group (OEWG) provided to the UN General Assembly over the last 20 years may be relevant.

78. The ICJ may also be able to rely on fact-finding by other commissions or courts, as it did in the *Bosnian Genocide* case.[185] The International Criminal Court (ICC) has powers to share information with the ICJ.[186] While no cyber-specific fact-finding body exists, there may be a fact-finding body relevant to the subject matter of the specific claim on which the Court can draw. For example, in *The Gambia v Myanmar*, the findings of the UN Fact-Finding Mission on Myanmar were presented to the ICJ by The Gambia in support of its arguments, including satellite imagery assessed by the Fact-Finding Mission as displaying 'irrefutable documentation

[177] Obligations of States in respect of Climate Change (Advisory Opinion) General List No 187 [2025] ICJ 1.
[178] Intergovernmental Panel on Climate Change, 'Announcement' (25 November 2024) https://www.ipcc.ch/2024/11/25/ipcc-icj/.
[179] Whaling in the Antarctic (Australia v Japan; New Zealand intervening) (Judgment) [2014] ICJ Rep 226 [227].
[180] See Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v Israel) (Verbatim Record) 11 January 2024, 10 am https://www.icj-cij.org/sites/default/files/case-related/192/192-20240111-ora-01-00-bi.pdf (see Adila Hassim at [28] and Blinne Ni Ghrálaigh at [32]-[33].
[181] See James Devaney, 'Evidence: International Court of Justice' (Max Planck Encyclopaedias of International Law, 2018) https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3430.013.3430/law-mpeipro-e3430?prd=OPIL para 69.
[182] Statute of the ICJ (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 50.
[183] Maritime Delimitation in the Caribbean Sea and the Pacific Ocean (Costa Rica v Nicaragua) (Decision to Obtain an Expert: Order of 31 May 2016) [2016] ICJ Rep 235; Maritime Delimitation in the Caribbean Sea and the Pacific Ocean (Costa Rica v Nicaragua) (Appointment of Experts: Order of 16 June 2016) [2016] ICJ Rep 240.
[184] See Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v Israel) (Request for Indication of Provisional Measures: Order of 26 January 2024) [2024] ICJ Rep 11 [14]; Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v. Russian Federation) (Request for Indication of Provisional Measures: Order of 16 March 2022) [2022] ICJ Rep 216 [19]. See also James Devaney, 'Evidence: International Court of Justice' (Max Planck Encyclopaedias of International Law, 2018) https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3430.013.3430/law-mpeipro-e3430?prd=OPIL para 53, citing cases in which the ICJ has relied on the ICTY.
[185] James Devaney (ibid) para 59.
[186] Negotiated Relationship Agreement between the International Criminal Court and the UN 2004 art 5(1)(b)(ii).

of the scale of destruction perpetrated' against the Rohingya, and Facebook posts analysed by the Fact-Finding Mission indicating the extent of the junta's online hate campaign.[187]

79. Viewed over the long term, there is a high level of compliance by States with the ICJ's judgments.[188] The situation is more mixed in the short term: of the 20 final judgments over the past decade, five judgments have been met with full compliance.[189] But if States refuse to participate or comply, this may have an effect on their reputation.

d) Hypothetical cases

80. In light of the issues above, the settlement of cyber disputes before the ICJ seems unlikely at the present time. But is it possible to envisage a future case, where there is the right constellation of parties and facts? Take the example below:

> State A launches a targeted cyber intrusion into the air traffic control systems of State B, intentionally causing critical flight management systems to malfunction and the aircraft to crash, killing the several hundreds of passengers on board. State B attributes the cyber operation to an individual based in State A. A Joint Investigation Team set up by several States to determine responsibility for the downing of the plane, and to collect evidence for accountability, also finds that State A is responsible. State A acknowledges that the individual responsible launched the cyber operation from its territory, but denies any link to the individual and refuses to prosecute or extradite the individual for prosecution by another State. State B alleges that this is a violation of the 1971 Montreal Convention on the Suppression of Unlawful Acts against Civilian Aircraft, to which both States are party.

Photo: istock.com/gorodenkoff

81. cyberattacks. For example, in September 2025, the navigation system of a plane carrying Ursula von der Leyen, the European Commissioner, was disrupted due to suspected Russian interference, according to the European Commission.[190] Disruption of GPS signals for aviation have become frequent in the area around the Baltic States since Russia's full-scale invasion of Ukraine in February 2022; several foreign ministers from Eastern European States have warned that if it continues, an air disaster cannot be ruled out.[191]

[187] Antonio Segura Serrano, 'International Dispute Settlement: Digital Evidence and Online Dispute Resolution' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 483.
[188] Philippa Webb, 'Patience and Perseverance: Time and Compliance with Inter-State Judicial Decisions' in Adrea Gattini and Marco Dimetto (eds), Time and International Adjudication: The Temporal Factor in Proceedings Before International Courts and Tribunals (Brill 2025) §2.1.
[189] ibid §2.2.
[190] Maia Davies and Will Vernon, 'EU chief von der Leyen's plane hit by suspected Russian GPS jamming' (BBC News, 1 September 2025) https://www.bbc.co.uk/news/articles/c9d07z1439zo.
[191] ibid.

82. Article 1(a) of the Montreal Convention provides that any person commits an offence if he unlawfully or intentionally commits acts of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft.[192] State B could argue that the cyber operation was unlawfully and intentionally committed under Article 1 of the Montreal Convention. While cyber acts are not specifically mentioned in the treaty, Article 1 is not limited to physical methods of violence and takes an effects-based approach, rather than focusing on the means.[193] Article 3 of the Convention requires States Parties to make the offences mentioned in Article 1 of the Convention punishable by severe penalties under domestic law when conducted by any person. Both the State of landing and the State of the operator can exercise jurisdiction over these offences.[194] State B could alternatively rely on violation of Article 1(b) of the Convention, which refers to 'any person who destroys an aircraft in service or causes damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight', or Article 1(d), which refers to 'any person who destroys or damages air navigation facilities, or interferes with their operation, if any such act if likely to endanger the safety of aircraft in flight'.

83. Article 14 of the Montreal Convention contains a compromissory clause, which designates the ICJ as the forum for resolving disputes related to the treaty's provisions, if the dispute is not first resolved by negotiation. The 190 States Parties to the Montreal Convention include Russia, China, Iran and North Korea which, as noted above, have reportedly been responsible for the majority of known cyber operations since 2005.[195] The dispute would concern the interpretation and application of that treaty. Assuming, in this scenario, that State A attempted negotiations and State B refused to engage constructively, it may be possible for State B to bring a case before the ICJ.[196]

84. State B, in submitting evidence to the Court that State A was responsible, could point to the findings of the Joint Investigation Team on attribution. On the interpretation of the treaty, State B could submit that acts of violence within the Convention can be committed by cyber means and that the interpretation of the Convention must evolve in light of contemporary realities and technological developments. In the Tallinn Manual 2.0, the International Group of Experts agreed that the term 'weapon' in Article 3 *bis* of the Chicago Convention, which recognises that States must refrain from the use of weapons against civil aircraft in flight, includes cyber weapons.[197] In the *Ukraine and the Netherlands v Russia* case before the European Court of Human Rights, which was a claim alleging that Russia was responsible for systematic human rights violations in Ukraine, including those related to the downing of flight MH17, the Montreal Convention was invoked in relation to an act committed from the ground, recognizing that the Convention can apply to non-traditional attacks on aircraft in flight.[198]

---

[192] Convention for the suppression of unlawful acts against the safety of civil aviation (Montreal Convention) (adopted 23 September 1971, entered into force 26 January 1973) 974 UNTS 177 art 1(1)(a).
[193] Report of the Secretariat on the RSGLEG Study on the Applicability of International Law Air Instruments to Cyber Threats against Civil Aviation, Appendix A, p. 12, noting that 'there is no requirement under the Montreal Convention for the perpetrator to be on board the aircraft, which allows the coverage of remote cyber attacks'.
[194] Convention for the suppression of unlawful acts against the safety of civil aviation (Montreal Convention) (adopted 23 September 1971, entered into force 26 January 1973) 974 UNTS 177 art 5.
[195] See para 8 above.
[196] The ICJ has previously ruled on its jurisdiction to hear claims under the Montreal Convention 1971, in Lockerbie (Libyan Arab Jamahiriya v UK) (Preliminary Objections) [1998] ICJ Rep 9.
[197] Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) Rule 57 Commentary, para 2.
[198] Ukraine and the Netherlands v Russia App nos 43800/14, 8019/16, and 28525/20 (ECHR, 9 July 2025).

85. In terms of remedy, State B could request a declaration from the ICJ that State A breached its obligations under the Montreal Convention through failure to prosecute the individual responsible.[199] State B could seek full reparation, including satisfaction (an apology); compensation for the damage caused by its internationally wrongful acts;[200] guarantees of non-repetition; or any combination of these.[201]

86. Another hypothetical scenario in which a treaty with a compromissory clause may have relevance is in the context of cyber intrusions into diplomatic premises:

Photo: istock.com/World photo

87. Hackers under the direction and control of State A plant malware on the computers of diplomats and staff based in the Embassy of State B, which is located in State A. Using the malware, the hackers launch a ransomware attack on the computers in the Embassy, which prevents State A from being able to conduct diplomatic activities. The hackers also use the cyber operation to steal confidential information from Embassy servers.

On Diplomatic Relations 1961 (VCDR) provides that the premises of the diplomatic mission are inviolable and that the receiving State is under a special duty to protect the premises of the mission against any intrusion or damage. The VCDR may provide a basis for a claim by the sending State (whose Embassy is violated by the unauthorized cyber intrusions) against the receiving State allegedly carrying out the cyber operations.

88. The Optional Protocol to the VCDR concerning the Compulsory Settlement of Disputes 1963 has a compromissory clause in Article I under which States Parties agree that disputes shall be referred to the ICJ.[203] A judgment from the ICJ on how the VCDR applies to cyber intrusions into

[199] ILC, Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001) YILC vol.II (Part Two) art 37, commentary para 6.
[200] ibid art 37.
[201] In some cases, the ICJ has ordered the State to come into compliance 'by means of its own choosing'. See Avena and Other Mexican Nationals (Mexico v United States of America) (Merits) [2004] ICJ Rep 72 [153(9)].
[202] Tom Chivers, 'Kremlin-backed hackers target foreign embassies in Moscow' (Semafor, 1 August 2025) https://www.semafor.com/article/08/01/2025/kremlin-backed-hackers-target-foreign-embassies-in-moscow.
[203] Optional Protocol to the Vienna Convention on Diplomatic Relations concerning the Compulsory Settlement of Disputes (adopted 24 April 1963, entered into force 19 March 1967) 596 UNTS 487.

diplomatic premises could be of interest to many States, since all diplomatic missions are vulnerable to such intrusions. However, while the VCDR has 193 States Parties, the Optional Protocol only has 70 parties, limiting it as a basis for establishing the Court's jurisdiction.

(iii) ICJ Advisory Opinion

89. If contentious proceedings before the Court are not an option, or as the pre-cursor to inter-State contentious proceedings, States may decide to seek an advisory opinion from the ICJ to clarify specified legal questions related to cyber operations under international law. Article 65 of the ICJ Statute allows the ICJ to give advisory opinions on any legal question. As noted above, while many States have now opined on how international law applies in the cyber context, States rarely characterise specific cyber incidents as violations of international law.[204] This gap between *opinio iuris* and concrete State practice reflects both legal uncertainty and political sensitivities.

90. The use of national statements to express States' views in this area raises questions about whether the views offered are creating, intentionally or not, a form of *lex specialis* of international law tailored to the cyber context.[205] And if not, what normative implications do these emerging positions have for the interpretation and application of existing international law rules? On issues such as sovereignty and due diligence, positions taken by the majority of States with a published position appear to be diverging from the views of some experts outside the cyber context. For example, some general international lawyers argue that under international law, sovereignty is not a rule and that, as a result, a violation of sovereignty is not necessarily an internationally wrongful act.[206] However, in the cyber context, the majority of States that have opined on this question have stated that sovereignty is a rule, and several draw on the case law of the ICJ to support their reasoning, for example the case of *Costa Rica v Nicaragua*.[207] The ICJ's views on this issue could provide clarification, especially as the Court has engaged with the question of sovereignty many times before and has confirmed that political dimensions of cases do not prevent the exercise of its functions.[208] The views of the Court on the significance of national positions on international law and cyberspace may also be helpful.

91. While ICJ advisory opinions are non-binding, they can be 'an authoritative statement of international law on the questions with which it deals'.[209] In order for the Court to provide an advisory opinion, the UN General Assembly, Security Council or one of 16 specialised UN agencies would need to make a written request to the ICJ, including an exact statement of the question on which the opinion is sought, and any relevant documents that might clarify the

---

[204] See para 54, above.
[205] In international law, lex specialis means that more specific rules will prevail over general rules.
[206] Jack Kenny, Sovereignty and Its Relation to Primary Rules of International Law (British Institute of International and Comparative Law, July 2025) https://www.biicl.org/publications/sovereignty-and-its-relation-to-primary-rules-of-international-law.
[207] Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica) (Judgment) [2015] ICJ Rep 665 [97]–[99], in which the ICJ held that the presence of Nicaragua's military personnel in the territory under Costa Rica's sovereignty amounted to a violation of Costa Rica's territorial sovereignty.
[208] In Alleged Violations of the 1955 Treaty of Amity, Economic Relations, and Consular Rights (Islamic Republic of Iran v United States of America) (Preliminary Objections) [2021] ICJ Rep 9 [55]-[56], the Court affirmed that the fact that a dispute arose in a particular political context did not mean that the Court should decline to resolve the legal questions at issue between the parties, nor that the dispute did not relate to the interpretation or application of the Treaty of Amity.
[209] Dispute Concerning Delimitation of the Maritime Boundary Between Mauritius and Maldives in the Indian Ocean (Mauritius/Maldives) (Preliminary Objections) (2021) ITLOS List of Cases No 28. Massimo Lando, 'Binding Advisory Opinions' in Russell Buchan, Daniel Franchini, and Nicholas Tsagourias (eds), The Changing Character of International Dispute Settlement: Challenges and Prospects (CUP 2023) 115, notes that this reasoning could have significant implications for the exercise of advisory jurisdiction by international courts and tribunals.

question. The Court is quite strict in ensuring that the requesting agency has competence to request an advisory opinion in the area in question.[210] In the cyber context, the obvious body to make the request would be the UN General Assembly, which has been active on cyber issues.

92. In the UN General Assembly, a majority of States present and voting would suffice (in practice, this could mean only 90 votes, factoring in absentee rates and abstentions).[211] The Registrar notifies all States of the request, and the Court invites States and international organizations likely to provide relevant information to submit written statements and potentially make oral statements.[212] Each participant is usually allowed to file a written statement followed by written comments on the other written statements. In the oral submissions, each participant takes the floor only once for a short time (30–45 minutes). In the ICJ's advisory opinion on climate change, for example, 91 written statements were filed by both States and international organizations,[213] and 96 States and 11 organizations made oral submissions.

[210] For example, the ICJ refused the request of the World Health Organization Assembly for an advisory opinion on the legality of the use of nuclear weapons, while granting the request from the UN General Assembly: Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion) [1996] ICJ Rep 66.
[211] See US State Department, Report to Congress on Voting Practices of UN Members for 2022 (March 2023) 7, noting the average absentee rate of 10% in 2022 and abstention rate of 11%.
[212] Evelyne Lagrange and Karim Oellers-Frahm, 'Article 96' in Bruno Simma and others (eds), The Charter of the United Nations: A Commentary (4th edn, OUP 2024).
[213] ICJ, 'Obligations of States in respect of Climate Change (Request for Advisory Opinion) ICJ Press release 2024/31 (12 April 2024) https://www.icj-cij.org/sites/default/files/case-related/187/187-20240412-pre-01-00-en.pdf.

Photo of proceedings before the ICJ. Source: <https://www.icj-cij.org/multimedia-cases>

93. In the climate context, criticisms of a lack of progress have led some States and civil society groups to adopt a legal strategy of requesting advisory opinions from international courts (the ICJ, International Tribunal on the Law of the Sea, the Inter-American Court of Human Rights, and the African Court of Human and Peoples' Rights). These requests seek to obtain legal clarity that has not been achieved through conferences of the parties or other forums for discussion. It is possible that frustration at the lack of progress at the UN on the application of international law to cyberspace may push some States to adopt similar strategies.

94. A coalition of States could support a draft resolution prepared by a State or group of States, noting the importance of clarifying the scope of legal obligations governing State behaviour in cyberspace in order to promote responsible conduct and prevent conflict. For example, a request might seek an opinion on the obligations of States under international law with respect to cyber operations conducted against other States, including operations that may impact the sovereignty, territorial integrity, or political independence of a State, or that may constitute intervention in the internal affairs of a State. The request might also ask for an opinion on the legal consequences under international law for a State that engages in, knowingly allows, or fails to prevent malicious cyber activities originating from its territory that cause significant harm to another State or its nationals.

95. Advisory opinions also, however, present some challenges. The ICJ has the discretion to decline to give an opinion,[214] although in all 30 Advisory Opinions given so far, it has not done so, and the Court has determined that political motives behind a request or the political nature of the question (among other things) are not compelling reasons for it to decline a request. Advisory Opinions are usually focused on questions of law rather than facts,[215] so are not a substitute for contentious proceedings, although they may clarify some legal points. Finally, some may argue that since States, as the primary makers of international law, are still in the process of determining how the law applies in the cyber context – with some States yet to publicise their views in this area[216]– an opinion in this area could be premature and give rise to questions of the legitimacy of the Court to rule on these issues at this stage.

(iv) Regional human rights mechanisms

96. A victim State may also be able to bring a case against another State before one of the three regional human rights courts – the European Court of Human Rights, Inter-American Court of Human Rights and African Court of Human and Peoples Rights – alleging that malicious cyber operations violate international human rights law. So far, no inter-State cases have been brought in relation to malicious cyber activity. But all three courts permit inter-State applications and all three have heard or are in the process of hearing inter-State cases. Drawing on the hypothetical air traffic control scenario discussed above in relation to a case before the ICJ, it is possible to conceive of a claim based on violation of the right to life for the killing of those on board the plane, as well as anyone killed on the ground. If the State carrying out the malicious cyber operation refused to investigate the incident, the claim could be based on both the negative duty to respect life and failure of the positive duty to investigate.

[214] Statute of the ICJ (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI art 65(1).
[215] As noted above (at para 30), fact-finding on attribution will be a crucial first step in cyber disputes. However, the ICJ did conduct some fact-finding in Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136.
[216] For example, many States in Latin America, the Middle East, and Asia have not yet made their views known.

97. The Inter-American system and African system have seen very few inter-State cases.[217] By contrast, there has been a considerable rise in the number of inter-State cases before the European Court of Human Rights, with 15 inter-State disputes currently pending before the Court.[218] This section therefore focuses on a claim before that court.

98. The procedure for an inter-State claim before the European Court of Human Rights is that the victim State lodges an application with a statement of acts and alleged violations of the European Convention of Human Rights; the case is then communicated to the respondent State, which is invited to submit written observations, and the claimant State has the right to reply. In complex and important cases, the Court will hold oral hearings. Usually, it is necessary for claimants to have exhausted domestic remedies before bringing a claim, but in inter-State cases, the Court sometimes disposes of this requirement (for example, where systemic administrative issues appear to curtail Convention rights, as in the case of *Georgia v Russia*, 2014, in which the Court found real obstacles to the effectiveness and accessibility of remedies on the part of Georgian nationals).[219] Claims must be brought within six months of the final domestic decision, where relevant.[220]

99. It is possible for States and international organisations to join the case as third parties. In the recent case of *Ukraine and Netherlands v Russia* – which concerned, *inter alia*, the shooting down of flight MH17 in July 2014 – 20 States and several international organizations joined. The Court can take into account the findings of international fact-finding bodies, such as those under the auspices of the UN.

a) Jurisdiction

100. One of the hurdles to bringing a human rights claim in relation to cyber activity is establishing that the respondent State had jurisdiction over the activities in question, under Article 1 of the Convention, because such activity is often carried out remotely. A State's jurisdiction for the purposes of its obligations under the Convention is primarily territorial.[221] The issue of extraterritorial jurisdiction is controversial among States. Human rights courts and treaty bodies have generally interpreted the notion of State jurisdiction in two ways – as State control over a territory in which the victim of the human rights violation is located (the spatial model) or as State authority, power or control over the victim directly, exercised by one of the State's agents (the personal model).[222] For example, the European Court of Human Rights held, in *Ukraine and Netherlands v Russia*, that military attacks such as shelling are forms of authority and control over the individuals affected by them (the personal model).[223] In the same case, the Court held that State jurisdiction was established in relation to the shooting down of flight MH17 in 2014, because the plane fell in an area under Russian control (the spatial model).[224]

---

[217] The Inter-American Commission of Human Rights has heard two cases; the African Commission, three; and the African Court only one. See Jorge Contesse, 'Inter-States Disputes under the Inter-American Human Rights System' (2024) 13(1) IHRL 74; Frans Viljoen, 'Inter-State Complaints under the African Human Rights System: a Breeze of Change?' (2024) 13(1) IHRL 96.
[218] European Court of Human Rights, 'Inter-State applications' https://www.echr.coe.int/inter-state-applications.
[219] Georgia v Russia (I) App no 12355/07 (ECHR, 31 July 2014) [125].
[220] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221 arts 34-35 (on rules on admissibility of cases).
[221] Banković v Belgium App no 52207/99 (ECHR, 12 December 2001) [67]; Ukraine and the Netherlands v Russia App nos 43800/14, 8019/16, and 28525/20 (ECHR, 9 July 2025) [553].
[222] See Marko Milanovic, 'Surveillance and Cyber Operations' in Mark Gibney and others (eds), The Routledge Handbook on Extraterritorial Human Rights Obligations (Routledge 2022).
[223] See Marko Milanovic, 'The European Court's Merits Judgment in Ukraine and the Netherlands v. Russia: As Good as It Gets (Almost)' (EJIL:Talk!, 2025) https://www.ejiltalk.org/the-european-courts-merits-judgment-in-ukraine-and-the-netherlands-v-russia-as-good-as-it-gets-almost/.
[224] Ukraine and the Netherlands v Russia App nos 43800/14, 8019/16, and 28525/20 (ECHR, 9 July 2025)

101. There is no developed jurisprudence of the Court on how the concept of jurisdiction should be applied in relation to cyber operations, with the exception of some cases dealing with surveillance. In *Wieder and Guarnieri v UK*, the Court held that the interception, storing or processing of data of any individual that implicates their right to privacy will be within the jurisdictional scope of the Convention if such surveillance activities are conducted on the State's own territory, even if the individual concerned is located outside it.[225] This has significant implications, as the principle could apply to any processing of information acquired by a State, even if the interception itself took place abroad.[226]

102. The Court's jurisprudence on jurisdiction in the non-cyber context is so varied that it is difficult to draw reliable conclusions about how the Court will approach this in the future in the cyber context; a range of options are available. At the more expansive end of the spectrum, it is possible that a court may find that the State must comply with its human rights obligations whenever it exercises power or control over a source of harm to individuals (the so-called 'functional' approach to jurisdiction, which some human rights bodies have applied in certain contexts).[227] Alternatively, a court might find that the State must comply with its negative obligations to respect human rights whenever it is able to interfere with the exercise of its rights. On this approach, any cyber operation that adversely affected human rights, for example, a State hacking a computer without consent, would be within the ambit of human rights treaties.[228] Human rights courts and bodies have not gone this far yet, but as there has generally been a trend towards a broader understanding of jurisdiction, both by the European Court of Human Rights and by other human rights bodies, it is likely that at least some cyber operations will be covered.

b) Attribution

103. The claimant State will also have to demonstrate that the malicious cyber activity was attributable to the respondent State, and that the cyber activity caused the violation in question. In the *Ukraine and Netherlands v Russia* case, the European Court of Human Rights held that acts and omissions of the Russian military were acts of Russian State organs attributable to Russia.[229] In terms of the link between the activities and the Russian military, the Court was able to draw on findings of fact from the Joint Investigation Team into the downing of MH17, which was led by the Netherlands with cooperation from a number of other States.[230]

104. Where there has been no prior investigation by a fact-finding body, Article 38 of the Convention and the Court's Investigative Rules allow the Court to gather facts jointly with the parties, including holding in-person fact-finding hearings in Strasbourg or conducting on-the-spot missions. Indeed, it is the norm for the Court to hold fact-finding hearings in inter-State cases, which have proved crucial in some cases.[231]

---

[702]-[706].

[225] Wieder and Guarnieri v UK App nos 64371/16 and 64407/17 (ECHR, 12 December 2023).

[226] See Marko Milanovic, 'Wieder and Guarnieri v UK: A Justifiably Expansive Approach' (EJIL Talk!, 21 March 2024).

[227] This approach is reflected in: UNHRC, 'General Comment 36' (3 September 2019) UN Doc CCPR/C/GC/36 para 63; Inter-American Court of Human Rights, The Environment and Human Rights (Advisory Opinion) (2017) OC-23/17 [101]-[102].

[228] See Marko Milanovic, 'Surveillance and Cyber operations' in Mark Gibney and others (eds), The Routledge Handbook on Extraterritorial Human Rights Obligations (Routledge 2022) 6.

[229] Ukraine and the Netherlands v Russia App nos 43800/14, 8019/16, and 28525/20 (ECHR, 9 July 2025) [362]-[363].

[230] The Team consisted of the Netherlands, Australia, Malaysia, Belgium and Ukraine.

[231] Philip Leach, Costas Paraskeva, and Gordana Uzelec, 'Human Rights Fact-Finding: The European Court of Human Rights at a Crossroads' (2017) 28(1) NQHR 41.

105. As well as any findings of fact by domestic courts (which are less likely to be relevant in inter-State cases), the Court may also be able to draw on any attribution findings made public by governments (collectively or otherwise) or cybersecurity companies. This would be useful, as the Court itself has limited institutional experience in evaluating complex digital forensic reports. Fact-finding measures are also costly and rely heavily on State cooperation, which may be limited in cyber disputes, given the likely involvement of classified materials.

106. However, the Court has been prepared to take a robust approach to fact-finding and evidence in some recent cases. For example, in *Carter v Russia*, the Court primarily conducted the fact-finding itself, and applied Article 8 of the International Law Commission's Articles on State Responsibility to attribute the conduct of the assassins of Alexander Litvinenko to Russia, finding that they were under the direction and control of the Russian authorities.[232] In reaching its judgment, the Court was able to draw on the findings of a judge-led UK inquiry into the assassination. The Court drew adverse inferences from the fact that Russia had failed to make "any serious attempt either to elucidate the facts or to counter the findings arrived at by the United Kingdom authorities",[233] and found that Russia had the burden to establish that the assassins were not under Russian control – especially since the information was exclusively in Russia's possession and the assassins were on its territory.[234]

107. It is possible that the Court would make similar inferences in future cyber cases where the malicious cyber activity is alleged to emanate from the respondent State's territory. This is especially the case since States have agreed that there is an expectation that States should not knowingly allow their territory to be used for internationally wrongful acts using Information and Communication Technologies.[235] Indeed, many States consider this to be a binding obligation of due diligence, as well as a voluntary norm of responsible behaviour.[236]

c) Evidence

108. No types of evidence are *per se* inadmissible before the European Court of Human Rights: the Court is free to evaluate any information presented to it, which includes illegally obtained evidence and hearsay.[237] The Rules of Court allow the Court to limit public access to documents on public interest grounds.[238] Rule 44F also gives the parties to a case access to a special procedure regarding secret evidence, under which (if the Court deems it appropriate, having reviewed the documents in question) the evidence is available only to the Court and not to the other party.[239]

d) Overall assessment

[232] Carter v UK App no 20914/07 (ECHR, 28 February 2022) [72].
[233] ibid [167].
[234] For a discussion of the case, see Marko Milanovic, 'European Court finds Russia Assassinated Alexander Litvinenko' (EJIL Talk!, 23 September 2021) https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.
[235] Australian Strategic Policy Institute, The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN (March 2022) https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf norm (c).
[236] See Cyberlaw Toolkit, 'Due Diligence' https://cyberlaw.ccdcoe.org/wiki/Due_diligence#:~:text=Due%20diligence%20entails%20that%20%E2%80%9Cit,in%20cyberspace%20falling%20under%20their.
[237] Corina Heri, 'Evidence: European Court of Human Rights' (Max Planck Encyclopaedias of International Law, 2018) https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3431.013.3431/law-mpeipro-e3431.
[238] European Court of Human Rights Rules of Court 2025, Rule 33.
[239] Corina Heri, 'Evidence: European Court of Human Rights' (Max Planck Encyclopaedias of International Law, 2018) https://opil.ouplaw.com/display/10.1093/law-mpeipro/e3431.013.3431/law-mpeipro-e3431.

109. There are limitations to State accountability before the European Court of Human Rights for malicious cyber operations because the State accused would need to be one of the 46 parties to the European Convention on Human Rights in order for the Court to have jurisdiction. In the *Ukraine and Netherlands v Russia* case, the Court was competent to deal with the case because a former Member State of the Council of Europe remains responsible for alleged violations of the Convention during the period when it was a party.[240] As such, the Court is only able to deal with facts that arose before 16 September 2022, when Russia ceased to be a party to the Convention.[241] Nevertheless, where there is jurisdiction, there may be fertile ground for inter-State cases in relation to the failure by one State to take steps to protect individuals within the applicant State's jurisdiction from cyber harms originating from the respondent State (whether those harms are carried out by State or non-State actors).

110. Other bodies, including UN human rights treaty bodies, are able to hear human rights cases between States. For example, the UN Committee om the Elimination of Racial Discrimination has recently heard three inter-State cases.[242] The ICJ can also examine, and make decisions about, obligations in human rights treaties. For example, in the ICJ case of *Armenia v Azerbaijan*, both sides have raised claims of hate speech and disinformation by the other (among other claims) under the UN Convention on the Elimination of All Forms of Racial Discrimination.[243] So there are a number of ways in which a State could bring a cyber-related inter-State human rights challenge. As with the ICJ, human rights courts can also issue advisory opinions.

111. Inter-State cases can take many years, and while the Council of Europe's Committee of Ministers oversees the implementation of judgments from the European Court of Human Rights, compliance records are mixed, with 44% of leading judgments from the past decade unimplemented.[244] Russia, in particular, had a poor level of compliance in recent years, and pursuant to Russian domestic law, will not implement judgments rendered by the European Court of Human Rights after 15 March 2022.[245]

112. Regional human rights mechanisms are likely to be more fruitful as an avenue for individuals (as opposed to States) to bring claims about State cyber activity that may infringe their human rights. For example, following a cyber intrusion into the Bulgarian National Revenue Agency, one of the 6 million affected individuals brought a claim against the agency before the Court of Justice of the EU for damages.[246] And in *Bradshaw v UK*, a group of individuals brought a case before the European Court of Human Rights challenging the UK's refusal to hold an

[240] European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 UNTS 221 art 58.
[241] Committee of Ministers, 'Consequences of the aggression of the Russian Federation against Ukraine' (2022) CM/Del/Dec(2022) 1428ter/2.3.
[242] See Jan Eiken and David Keane, 'Towards an Amicable Solution: the Inter-State Communications Procedure under ICERD' (2022) 21(2) The Law and Practice of International Courts and Tribunals 302, arguing for the potential of this mechanism as a global contentious human rights jurisdiction.
[243] Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Azerbaijan v Armenia) (Preliminary Objections) General List No 181 [2024] ICJ 1.
[244] European Implementation Network, Justice Delayed and Justice Denied: Report on the Non-Implementation of European Judgments and the Rule of Law (September 2024) https://www.einnetwork.org/blog-five/2024/9/20/justice-delayed-and-justice-denied-report-on-the-non-implementation-of-european-judgments-and-the-rule-of-law.
[245] See Law No. 180 (14 June 2022) <https://www.garant.ru/products/ipo/prime/doc/404720359/>; Law No. 183. (14 June 2022) https://www.garant.ru/products/ipo/prime/doc/404720365/#131.
[246] Simmons & Simmons, 'Important CJEU ruling on Cyber attack damages' (23 February 2024) https://www.simmons-simmons.com/en/publications/clsyp71bs00huu5mcaxmtns8x/important-cjeu-ruling-on-cyber-attack-damages.

investigation into alleged Russian interference into UK elections.[247] There have also been challenges to States' use of bulk surveillance systems by individuals invoking the right to privacy (Article 8 ECHR),[248] as well as cases brought by individuals before domestic courts.[249] In addition to the inter-State case of *Netherlands and Ukraine v Russia* regarding the downing of flight MH17, there is also a linked case pending by over 500 relatives of MH17 victims.[250]

PROSECUTION OF MALICIOUS CYBER ACTIVITY

A. Multistakeholder Partnerships and Evidential Pathways

113. As noted above, nearly half of cybersecurity incidents remain unattributed to any State.[251] Of course, some malicious cyber activity is carried out by individual hackers without links to a State. But increasingly, certain States use criminal networks as proxies for their cyber operations to give them plausible deniability when confronted in either diplomatic or intelligence channels. For example, Google's Threat Analysis Group has reported that actors backed by the Russian-government have targeted users in Ukraine with destructive cyber operations, including spear-phishing (fraudulent emails seeking to gain confidential information from users),[252] and the ransomware ecosystem increasingly sees States supporting criminal gangs whose activities align with States' objectives.[253] Some States deliberately create enough critical distance to ensure the activity of these proxies is not easily attributed to them. Ransomware is the greatest cyber threat to the UK, but as the National Crime Agency has observed, in most instances, 'links to [a] State extend only to tolerance of their activities'[254] – at a minimum, such tolerance might include allowing the individuals concerned to operate with impunity on the State's territory, while turning a blind eye.

114. Where the behaviour can be attributed to an individual, States may be able to use domestic criminal law to hold the individuals responsible to account by bringing prosecutions for cybercrime offences. As well as providing accountability for these crimes, effective investigation and prosecution of cybercrime may have a deterrent effect. Over the last 25 years, States have agreed to criminalise different types of malicious cyber behaviour and used international law to strengthen standards on exchange of evidence and international cooperation. The 80 States Parties to the Budapest Convention on Cybercrime are obligated to criminalise specific cyber activities such as illegal access to a computer system, data

[247] Bradshaw and others v United Kingdom App no. 15653/22 (ECHR, 22 July 2025). The applicants claimed that the UK was in violation of the right to free elections under Article 1 of Protocol 3 of the ECHR; the Court held that the UK was not in violation as it had fulfilled its positive obligations to protect democratic processes.
[248] For example, Big Brother Watch and others v United Kingdom App nos 58170//13, 62322/14, and 24960/15 (ECHR, 25 May 2021). The applicants claimed that the UK was in violation of Article 8 ECHR (right to respect for private and family life) and Article 10 ECHR (right to freedom of expression).
[249] Accountability for malicious cyber operations by non-State actors will be the subject of a subsequent Policy Brief by the Oxford Institute of Technology and Justice.
[250] European Court of Human Rights, 'Q&A – Ukraine and the Netherlands v Russia' (Press Unit, 9 July 2025) https://www.echr.coe.int/documents/d/echr/press-q-a-ukraine-netherlands-russia-eng.
[251] International Society of Automation (ISA) Global Cybersecurity Alliance, 'Defending Against State-Sponsored Cyberattacks in 2025' https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025; see also para 8 above.
[252] Shane Huntley, 'For of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape' (Google Threat Analysis Group, 16 February 2023) https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.
[253] Aleksandar Milenkoski and others, Ransomware's New Masters: How States are Hijacking Cybercrime (Pharos Series: Report No 3, April 2025) https://virtual-routes.org/wp-content/uploads/2025/04/Virtual-Routes-Pharos-Report-Series-No.-3.pdf .
[254] National Crime Agency, 'Cybercrime' https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime.

interference and system interference.[255] They are also under an obligation to cooperate with each other in investigating and prosecuting acts criminalised by the Budapest Convention.[256] Like the Budapest Convention, the UN Cybercrime Convention obliges States Parties to criminalise certain computer-related activity and to cooperate in the investigation and prosecution of these crimes. The Convention was signed in 2024 but is not yet in force; civil society organisations and tech companies have voiced concerns about the breadth of its terms and inadequate human rights safeguards.[257]

115. Sector-specific laws may also be relevant. For example, as noted above, the Montreal Convention of 1971 requires States Parties to make the offences mentioned in Article 1 of the Convention punishable by severe penalties under domestic law when conducted by any person. Certain nuclear treaties, which contain compromissory clauses, criminalise activities affecting nuclear facilities or materials, including use or damage by digital means.[258]

116. Prosecutions should be seen as part of a broader strategy for tackling malicious cyber activity, with States employing a combination of strategies to deter and disrupt such activity, including diplomacy, intelligence, sanctions and legal action. This includes international cyber diplomacy policy initiatives such as the Counter Ransomware Initiative and Pall Mall process and collaborative action on attribution, sanctions and disruption tactics.[259] For example, Operation Cronos, an international law enforcement taskforce led by UK's National Crime Agency and the FBI and consisting of eleven International Counter Ransomware Initiative Member States,[260] successfully executed an international disruption campaign in 2024, taking control of the website and services of LockBit, a very powerful cybercrime group. Two LockBit operatives were arrested, in coordination with Europol, and three international arrest warrants and five indictments have also been issued by the French and US judicial authorities.[261] The UK, US and Australia also sanctioned a senior leader of LockBit.[262] This multi-agency coordinated approach is illustrated in the following graphic.

[255] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167 arts 2-5. States Parties that have ratified the Convention include the US, UK, Ukraine, Australia, Japan and Canada, as well as many States in the EU, Latin America and Africa.
[256] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167 arts 23-25.
[257] See, for example, Deborah Brown, 'New UN Cybercrime Treaty Primed for Abuse' (Human Rights Watch, December 2024) https://www.hrw.org/news/2024/12/30/new-un-cybercrime-treaty-primed-abuse.
[258] See Talita Dias, Joyce Hakmeh, and Marion Messmer, 'Cybersecurity of the civil nuclear sector: Threat landscape and international legal protections in peacetime and conflict' (Chatham House, July 2024) 19 https://www.chathamhouse.org/sites/default/files/2024-07/2024-07-02-cybersecurity-civil-nuclear-sector-dias-et-al_0.pdf. For example, the Convention on Physical Protection of Nuclear Material has a compromissory clause in Article 17(2) which requires recourse to the ICJ or arbitration if negotiation does not succeed as a means of settling the dispute; the International Convention for the Suppression of Acts of Nuclear Terrorism has a compromissory clause in Article 23(1), which requires the parties to settle disputes through negotiation and then arbitration if negotiation fails.
[259] Louise Marie Hurel and Gareth Mott, 'Rethinking Cyber Deterrence in a Multipolar World' (RUSI, August 2025) https://www.rusi.org/explore-our-research/publications/emerging-insights/rethinking-cyber-deterrence-multipolar-world.
[260] The US, UK, France, Japan, Swiz, Canada, Australia, Sweden, Netherlands, Finland and Germany, with the support of Ukraine, Finland, Poland and New Zealand.
[261] Europol, 'Law enforcement disrupts world's biggest ransomware operation' (February 2024) https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.
[262] UK Government, 'UK and allies sanction prolific cyber hacker' (7 May 2024) https://www.gov.uk/government/news/uk-and-allies-sanction-prolific-cyber-hacker.

Source: Europol

117. Similarly, in Operation Serengeti 2.0, coordinated by Interpol, public–private partnerships led to 1,209 cybercriminals being arrested and around $97 million recovered.[263] Civil laws have also played a part in disruption operations by the private sector and law enforcement agencies. For example, the US Department of Justice used civil forfeiture laws and technical capabilities to follow bitcoin trails and seize back ransom paid in the Colonial Pipeline incident, in which a ransomware attack took down the operations of a major US oil pipeline system.[264] The Department of Justice also obtained court authorisation to gain access to ransomware networks and swipe decryption keys, disrupting a botnet that targeted more than 200,000 consumer devices worldwide.[265]

118. There are challenges for investigators and prosecutors to obtain evidence from other jurisdictions because the mutual legal assistance system for the exchange of evidence between States is notoriously slow and bureaucratic. But new routes are opening up, including the possibility for States to make requests for evidence directly to technology companies, facilitated by a number of recently adopted international instruments, including executive agreements under the US Cloud Act;[266] the EU e-Evidence framework (which will come into force in August 2026); and the Second Additional Protocol to the Budapest Convention.[267] An e-evidence agreement between the EU and US, on which negotiations have been ongoing, would also facilitate cyber investigations.[268]

---

[263] Sean Doyle and Natalia Umansky, 'Cybercrime is borderless. This global bust shows how law enforcement can be too' (World Economic Forum, 27 August 2025) https://www.weforum.org/stories/2025/08/cybercrime-global-collaboration/#:~:text=In%20August%202025%2C%20as%20part,blockchain%20transactions%20to%20generate%20cryptocurrency.

[264] US Department of Justice, 'Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside' (Press Release, 7 June 2021) https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[265] US Department of Justice, 'Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers' (Press Release, 18 September 2024) https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state.

[266] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime 2019; Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime 2021.

[267] Second Additional Protocol to the Cybercrime Convention on enhanced cooperation and disclosure of electronic evidence (not yet in force) CETS No 224.

[268] Kenneth Propp, 'Navigating Towards an EU-US Agreement on Electronic Evidence' (Lawfare, 7 December 2023) https://www.crossborderdataforum.org/lawfare-navigating-toward-an-eu-u-s-agreement-on-electronic-evidence/.

119. International cybercrime investigations have also been strengthened by growing cooperation between national authorities and the private sector. Most governments have set up Computer Emergency Response Teams (CERTs), which consist of State and/or non-State experts, to trace cyber operations and identify perpetrators. Microsoft's Digital Crimes Unit carries out tracing, attribution and advanced threat intelligence, and provides reports on malicious cyber activities, for example in Ukraine. Cybersecurity firms have also helped governments to trace chains of proxy servers and to expose and respond to major malicious cyber operations. The US Cybersecurity and Infrastructure Security Agency set up the Joint Cyber Defense Collaborative in 2022, which includes major tech firms such as Amazon, Google, and Microsoft as well as cybersecurity firms such as CrowdStrike and FireEye. The Cybercrime Atlas Initiative, which was launched in 2023 with the support of Fortinet, Banco, Santander, Microsoft and PayPal, is developing a comprehensive picture of the cybercrime landscape that includes details of criminal operations, shared infrastructure and networks to help law enforcement and government agencies take down cybercriminals and their infrastructure globally.[269] The Initiative currently has 23 private sector organizations and individual contributors. Europol's EC3 Cybercrime Team and Microsoft recently announced a partnership to embed Microsoft investigators into EC3 to support investigations.[270] This growing international and public–private cooperation has led to an increasing number of arrests, indictments and prosecutions of malicious cyber activity.[271]

B. US prosecution of malicious cyber activity

120. Over the last ten years, the US has issued indictments against Russian, Chinese, Iranian and North Korean actors for malicious cyber operations against the US or other States. For example, in the 2024 case of *US v Stigal and Others*, the defendants were Russian GRU officers working in the military intelligence unit of the Russian government accused of hacking into 'computers associated with the Ukrainian government and entities associated with the governments of countries that provided support to the Ukrainian government in resisting Russia's invasion of Ukraine'.[272] While the indictments were issued against individuals rather than the State, the State of nationality is implicated, as the indictments make clear that the individuals were working for the State concerned when carrying out the malicious cyber activity (for example, in the case of *US v Stigal*, the GRU is Russia's military intelligence agency, and an organ of the Russian State). Between 2013 and 2016, the Obama administration issued 28 indictments against malicious actors from Russia, China, Iran and North Korea. Between 2017 and 2020, the Trump administration increased the number of indictments to 106.[273]

121. The US has resources to bring these prosecutions, which many States do not, due to a combined investigation and prosecution taskforce which includes the Department of Justice (DoJ) and Federal Bureau of Investigation (FBI) and that involves prosecutors at an early stage and draws on specialised technology units. The US has also received support from allies – the

[269] Derek Manky, 'Cybercrime Atlas: An Effective Approach to Collaboration in Cybersecurity' (Fortinet, 25 October 2024) https://www.fortinet.com/blog/industry-trends/cybercrime-atlas-an-effective-approach-to-collaboration-in-cybersecurity.
[270] Brad Smith, 'Microsoft launches new European Security Program' (Microsoft, 4 June 2025) https://blogs.microsoft.com/on-the-issues/2025/06/04/microsoft-launches-new-european-security-program/.
[271] See, for example, 'Ransomware Countermeasures Tracker' (Virtual Routes) https://virtual-routes.org/ransomware-countermeasures-tracker/.
[272] United States v. Stigal and Others (District Court of Maryland, 07 August 2024) Criminal No. LKG-24-06.
[273] One well-known example is the arrest warrant issued against Park Jin Hyok, a North Korea citizen, for his involvement in the WannaCry 2.0 Ransomware and Sony Hack. See US Department of Justice, 'North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions' (Press Release, 6 September 2018) https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

Stigal case involved the FBI and 12 other partners, representing governments of nine countries, as part of 'Operation Toy Soldier'.[274] Most of the major tech companies are based in the US, which makes it easier for the government to seek evidence from them.

122. These indictments have been called 'speaking indictments' because one of their principal purposes is to show that the US is prepared to make a public attribution of the cyber activity to specific perpetrators and is able to back up the claim by submitting evidence to prove it in court. Such indictments send a public message to States that sponsor malicious cyber activity on their territory but refuse to extradite the individuals concerned, and may have a deterrent effect. The indictments also provide education and awareness for the public and private sector, to assist them in recognising the risks and the need to strengthen cybersecurity.

123. In bringing these indictments, the US has been creative in its assertion of prescriptive jurisdiction, as in many of the cases, the malicious cyber activity took place outside the US with effects in other States. For example, in the *Stigal* case referred to above, the primary victims were the government of Ukraine and Ukrainian citizens. However, that indictment also notes that the conspirators probed websites hosted by protected computers and unassigned servers maintained by a US government agency located in Maryland,[275] so jurisdiction in that case may derive from passive personality (on the basis that the victims included a US national) or the protective principle (on the basis that the cyber activity threatens the security or vital interests of the US).[276] In any event, the Computer Fraud and Abuse Act, the domestic law used in these cases, has broad reach, allowing the US to bring a criminal action against an individual who 'damages' not only a computer in the US but also 'a computer located outside the US that is used in a matter that affects interstate or foreign commerce or communications of the US'.[277]

124. Relatedly, the potential for litigation against States or their officials in US courts has been enhanced by the US Supreme Court's expansion of the understanding of personal jurisdiction in the context of the commercial activities.[278] In practice, this means that unlike in cases involving private foreign defendants, there is no separate 'minimum contacts' inquiry for foreign States or public or private entities acting on their behalf as long as a relevant exception applies and service has been properly effected.

125. A potential challenge for States wishing to bring prosecutions is, however, that individuals acting on behalf of the State may be protected from prosecution under the principle of State immunity. Under international law, State officials committing acts in their actual or apparent official capacity on the territory of another State are usually immune from any form of criminal process (known as functional immunity or immunity *ratione materiae*). The scope of functional immunity under international law, including in relation to the immunity of State officials from foreign criminal jurisdiction, is complex and under discussion by States in the International Law

[274] US Department of Justice, 'Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government' (Press Release, 5 September 2024) https://www.justice.gov/archives/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government#:~:text=In%20an%20indictment%20unsealed%20today,intrusion%20and%20wire%20fraud%20conspiracy.
[275] United States v. Stigal and Others (District Court of Maryland, 07 August 2024) Criminal No. LKG-24-06 [22], [24], [42].
[276] The jurisdictional basis is not addressed explicitly in the indictment itself.
[277] This language was added by the Patriot Act of 2021 and has been construed by US courts as an express grant of extraterritorial jurisdiction.
[278] Claire DeLelle and others, 'US Supreme Court Holds that FSIA Does Not Require Proof of "Minimum Contacts" for a US Court to Exercise Personal Jurisdiction Over a Foreign State' (White & Case, 12 June 2025) https://www.whitecase.com/insight-alert/us-supreme-court-holds-fsia-does-not-require-proof-minimum-contacts-us-court-exercise.

Commission.[279] It is possible that individuals who carry out cyber operations and are acting in their official capacity may seek to invoke (or have their State invoke) functional immunity, although in the proceedings relating to the US indictments discussed above, US courts have not so far considered functional immunity to be a barrier,[280] without giving any reasoning for this position (in the *Stigal* case, for example, the jurisdictional basis is not explicitly stated, nor is immunity discussed). Courts in Germany and Slovenia have also disregarded functional immunity when hearing criminal cases against government officials, without stating why.[281] Therefore State practice in this area is still obscure.

126. Although prosecutions have been possible in US courts, few of these indictments have resulted in the arrest of the individuals concerned, because they are located outside the jurisdiction of the US, in States that are not prepared to extradite. However, in some cases prosecutions have been successful, including where individuals indicted have travelled outside their home State and been arrested by the authorities in a State that was prepared to hand them to the US. For example, in 2024, Evgenii Ptitsyn, a Russian national alleged to have coordinated the sale, distribution and operation of Phobos ransomware as part of an international hacking and extortion conspiracy, was extradited from South Korea to stand trial in the US. He is charged with a 13-count indictment of wire fraud conspiracy, conspiracy to commit computer fraud and abuse, four counts of international damage to protected computers, and four counts of extortion in relation to hacking, and his trial is ongoing.[282] In any event, the indictment strategy has broader benefits – for example, arrest warrants or convictions *in absentia* may limit the travel of the individuals.

127. While these cases are against individuals rather than a State, the actions of the individuals concerned are usually linked to a State (no case has yet been brought against individuals without links to a State). Many States currently lack the capacity to bring prosecutions, but there are efforts to improve this. The UN's Office on Drugs and Crime (UNDOC) runs global training programmes for law enforcement officers and criminal justice practitioners on the investigation of cybercrime, digital evidence, digital forensics and litigation techniques.[283] Eurojust, the European Judicial Training Network and the Cybercrime Programme Office of the Council of Europe all provide training on the prosecution of cybercrime.

Intersections between the peaceful settlement of disputes and prosecution of cybercrime

128. There are various intersections between accountability tools for individual criminal activity discussed above, and the rules on State responsibility for malicious activity in cyberspace, discussed earlier in relation to the peaceful settlement of disputes. Some States and scholars argue that the exercise of domestic court jurisdiction for the suppression of cybercrime forms

[279] 'Analytical Guide to the Work of the International Law Commission: Immunity of State officials from foreign criminal jurisdiction' https://legal.un.org/ilc/guide/4_2.shtml.
[280] See Marko Milanovic, 'Two Case Studies of Clandestine Operations, Attribution and Functional Immunity for Ordinary Crimes' (EJIL:Talk!, 2024) https://www.ejiltalk.org/two-case-studies-of-clandestine-operations-attribution-and-functional-immunity-for-ordinary-crimes/.
[281] ibid.
[282] US Department of Justice, 'Phobos Ransomware Administrator Extradited from South Korea to Face Cybercrime Charges' (Press Release, 18 November 2024) https://www.justice.gov/archives/opa/pr/phobos-ransomware-administrator-extradited-south-korea-face-cybercrime-charges.
[283] United Nations Office on Drugs and Crime, Global Programme on Cybercrime: Training Catalogue (2024) https://www.unodc.org/documents/Cybercrime/Web_Global_Program_on_Cybercrime_Training_Catalog.pdf?v=3.6.

part of a State's due diligence obligations under international law.[284] Whether or not 'due diligence' in the cyber context constitutes an obligation (as asserted in Rule 6 of Tallinn 2.0 and elsewhere) or a voluntary expectation (as asserted by others)[285] is debated, as are the contours of due diligence requirements in the cyber context. Regardless of the position, specific human rights obligations often imply due diligence requirements to prevent, halt and remedy harms in cyberspace, which may include providing civil remedies and criminal provisions to facilitate effective investigations and prosecutions of cyber-related violations.[286] For these reasons, as well as policy imperatives, it is important that States put in place the legislative, executive and judicial infrastructure to combat malicious cyber activities on their territory.[287]

129. There is also an intersection between investigations into cybercrime and State sovereignty. For example, if State A's investigation into ransomware in State B involves State A's officials remotely accessing data in State B without State B's consent, some States would consider that to amount to a violation of sovereignty. But what is permitted in this area is unclear and would benefit from further discussion.

130. Finally, it is possible that in due course we may see disputes between States over cybercrime in international courts. The Budapest Convention provides that the parties may settle disputes before an arbitral tribunal or the ICJ,[288] while the UN Cybercrime Convention provides that disputes that cannot be settled through negotiation shall be submitted to arbitration, and if that is not possible within six months, States may refer the dispute to the ICJ.[289]

C. Accountability for cyber-enabled international crimes

131. In some circumstances, it may also be possible to hold individuals that inflict serious harm by cyber means responsible under international criminal law. There are some situations in which cyber activity is so serious that it qualifies as an international crime (ie a war crime, crime against humanity, genocide or aggression).[290] These crimes may be committed purely by cyber means or carried out as part of a wider set of acts, for example, to coordinate, facilitate or otherwise support physical action in an armed conflict. A statement from the UK government recently noted that in March 2022, Russia 'conducted online reconnaissance to help target missile strikes against Mariupol - including the strike that destroyed the Mariupol theatre where hundreds of civilians, including children, were murdered'.[291] This strike on a civilian shelter, which was clearly marked with 'Children' on the roof, has been alleged to be war crime by several human rights groups.[292]

[284] For example, Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 European Journal of International Law 771.
[285] For example, Jack Kenny, 'Cyber Operations and the Statute of Due Diligence Obligations in International Law' (2023) 73 ICLQ 135.
[286] See Antonio Coco and Talita de Souza Dias, 'Cyber Due Diligence: A Patchwork of Protective Obligations in International Law' (2021) 32 EJIL 771.
[287] ibid.
[288] Budapest Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) 2296 UNTS 167 art 45.
[289] United Nations Convention against Cybercrime (not yet in force), adopted in United Nations General Assembly Resolution 79/243 (31 December 2024) UN Doc A/RES/79/243 art 63.
[290] The core international crimes are genocide, crimes against humanity, war crimes and aggression.
[291] UK Government, 'UK sanctions Russian spies at the heart of Putin's malicious regime' (Press Release, 18 July 2025) https://www.gov.uk/government/news/uk-sanctions-russian-spies-at-the-heart-of-putins-malicious-regime.
[292] See, for example, Shashank Purdey, 'ECCHR assessment claims Russia attack on Mariupol Theatre was a war crime' (Jurist news, 16 March 2024) https://www.jurist.org/news/2024/03/ecchr-assessment-claims-russia-attack-on-mariupol-theater-was-a-war-crime/.

132. Until recently, accountability for individuals who inflict serious harm by cyber means had received little attention, but today there is growing recognition of the role that international criminal law can play in holding such individuals responsible.[293] The Office of the Prosecutor of the ICC has recently published a Draft Policy on Cyber-Enabled Crimes under the Rome Statute,[294] the final version of which is due to be published in late 2025. The proposed policy indicates that the OTP intends to investigate and prosecute cyber-enabled crimes under the Rome Statute of the ICC in the same way as crimes committed by physical or other means. Under the Rome Statute, individual criminal responsibility may arise through individual commission of the crime in question and also through joint commission; commission through others; and/or instigating, assisting in, facilitating or aiding or abetting the commission or attempted commission by cyber means.[295] Commanders and other superiors may be criminally liable for cyber operations that qualify as international crimes and that were conducted by their subordinates.[296]

133. The Office of the Prosecutor's draft policy highlights that cyber-enabled crimes under the Statute will be varied, ranging from sophisticated malware attacks to incitement to genocide. The Human Rights Center at UC Berkeley has made confidential communications to the ICC alleging the commission of cyber-enabled international crimes in the situations of Ukraine (including in relation to cyberattacks on power grids that are alleged to be war crimes)[297] and Mali (including in relation to the spreading of images of atrocities – for example, of people being killed, maimed or mutilated – on Telegram by affiliates of the Wagner group that is alleged to constitute crimes against humanity through causing severe mental harm).[298]

134. Returning to the scenario of a malicious cyber operation on air traffic controls that leads to the downing of a civilian aircraft resulting in hundreds of deaths, it is possible that this could amount to a crime against humanity. A crime against humanity is committed if the act is part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack.[299] Crimes against humanity can be committed in times of peace as well as in war, and the list of crimes against humanity in Article 7 of the Rome Statute includes murder and extermination. The Office of the Prosecutor's Draft Policy notes that 'large-scale killing perpetrated by cyber means, such as the hacking of airplane navigation systems or air traffic control, which results in plane crashes and many victims, could count as extermination'.[300] The Office of the Prosecutor also cites a State launching cyber operations to hack the navigational systems of aircraft, thereby causing death, injury or physical damage, as an example of the use of force and the crime of aggression.[301] If the cyber operation was carried out as part of an armed conflict, it could amount to the war crime of intentionally directing attacks against the

[293] Permanent Mission of Liechtenstein to the United Nations, Council of Advisers Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare (International Law Association, August 2021) https://www.ila-americanbranch.org/wp-content/uploads/2022/10/The-Council-of-Advisers-Report-on-the-Application-of-the-ICC-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.
[294] Office of the Prosecutor, Draft Policy on Cyber-Enabled Crimes under the Rome Statute (6 March 2025) https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf.
[295] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 art 25(3).
[296] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 art 28.
[297] Lindsay Freeman, 'Russian cyberattacks need an international criminal court response' (Center for European Policy Analysis, 19 July 2022) https://cepa.org/article/russian-cyberattacks-need-an-international-criminal-court-response/.
[298] Monika Pronczuk and Sam Mednick: 'A confidential brief urges the ICC to investigate Wagner's promotion of atrocities in West Africa' (Berkeley Human Rights Center, 22 June 2025) https://humanrights.berkeley.edu/hrc-in-the-news/a-confidential-brief-urges-the-icc-to-investigate-wagners-promotion-of-atrocities-in-west-africa/.
[299] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 art 7(1).
[300] Office of the Prosecutor, Draft Policy on Cyber-Enabled Crimes under the Rome Statute (6 March 2025) https://www.icc-cpi.int/sites/default/files/2025-03/250306-OTP-Policy-on-Cyber-Enabled-Crimes-for-public-consultation.pdf 16, para 57.
[301] ibid 21, para 74.

civilian population as such or against individual civilians not taking direct part in hostilities, or the war crime of intentionally directing attacks against civilian objects. [302]

135. Besides the ICC, States can prosecute individuals for their involvement in cyber-enabled international crimes under universal jurisdiction (the prosecution of crimes regardless of where they were committed, and regardless of the nationality of the perpetrator or victim) or other bases of jurisdiction, where available.[303] But in practice, only a limited number of States have 'true' universal jurisdiction (ie allowing for jurisdiction even where the criminal conduct and its perpetrators and victims have no connection to the State whatsoever), and even fewer use such laws to prosecute perpetrators in their courts.[304]

136. However, there is an interesting direction of travel towards joint investigations of international crimes, ie two or more investigative, prosecutorial or judicial bodies coordinating on common lines of inquiry or working alongside each other in specific operations.[305] This includes a Joint Investigation Team supporting investigations into crimes against migrants and refugees in Libya and a Joint Investigation Team established in relation to Ukraine, which involves the national prosecution authorities of several countries with support from the ICC's Office of the Prosecutor; Eurojust; Europol; the Core International Crimes Evidence Database; and the International Centre for the Prosecution of the Crime of Aggression against Ukraine.

[302] Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1 July 2002) 2187 UNTS 3 art 8(2)(b)(i) ; art 8(2)(b)(ii).
[303] See Clooney Foundation for Justice, 'Justice Beyond Borders' https://justicebeyondborders.com/world.
[304] Clooney Foundation for Justice and REDRESS, Global Britain, Global Justice: Strengthening Accountability for International Crimes in England and Wales (October 2023) https://redress.org/publication/global-britain-global-justice-strengthening-accountability-for-international-crimes-in-england-and-wales/.
[305] See Office of the Prosecutor, Policy on Complementarity and Cooperation (April 2024) https://www.icc-cpi.int/sites/default/files/2024-04/2024-comp-policy-eng.pdf paras 102-112.

CONCLUSION

137. When a dispute arises from State-to-State cyber activities, the parties concerned should work together to identify means and mechanisms that can be used to help resolve their dispute peacefully. What those means are will depend on the facts in each case and will be subject to the choice and discretion of States. This Policy Brief has shown that there are various factors that may militate against States settling cyber disputes in public or through court proceedings in some contexts. Nevertheless, recourse to courts can be part of the menu of options for States to seek accountability – both in terms of State responsibility and individual liability – for malicious cyber activity.

138. This Brief has shown how existing treaties on a variety of different subject matters can be relevant to malicious cyber activity and potentially provide the basis for a claim. More broadly, the Brief has shown that international law – whether the Rome Statute, Montreal Convention or the Vienna Convention on Diplomatic Relations – is capable of adapting to the modern era and may be used to hold perpetrators to account for malicious cyber operations as well as physical activity. Increasingly, we are likely to see cases involving a combination of both types of activity.

139. Different dispute settlement options (adjudicative and diplomatic) need not operate in silos – they can be fluid, or used in parallel, depending on what the specific dispute requires. Fact-finding may be a valuable precursor to litigation in the cyber context, as well as an end in itself. Seeking an advisory opinion or judgment from the ICJ is rarely an end in itself but a step in a broader political process that offers the victorious State leverage in negotiations. Prosecutions may take place alongside public attribution and the imposition of sanctions. Non-conventional means of dispute settlement, such as strengthening cooperation (for example, through the UN Points of Contact Directory), coalition-building (for example, cooperation between intergovernmental organisations such as Europol, Interpol and Eurojust) and technical and capacity-building, can substitute for or complement more traditional means of settling disputes.

140. Where there is sufficient evidence to establish State responsibility for malicious cyber activity that amounts to a violation of international law and there is a relevant treaty with a compromissory clause, that may provide a route for bringing a case before an international court or tribunal. Alternatively, it may be possible to found a claim on a violation of customary international law or international human rights law. While the unsettled state of key aspects of the law may be a hurdle, as discussions between States evolve, the prospects for adjudication increase.

141. Momentum and avenues for prosecution of both cybercrime and cyber-enabled international crimes are growing, and important strides are being made in technical attribution, especially through public–private partnerships. Where it is possible to establish the identity of the individual who carried out the cyber activity through technical attribution, but not possible to connect that individual with a State for the purposes of establishing State responsibility, criminal prosecution of the individual under criminal law may be the best or only route to accountability. This is also the case where the malicious cyber activity can be linked to a State but it is difficult to establish that the activity in question is a violation of international law.

142. In order to maximize legal accountability for State-to-State malicious cyber operations, more work is needed in several areas, which will be a focus of the Oxford Institute of Technology and Justice in the future:[306]

- **Clarification of how the peaceful settlement of disputes applies in the cyber context.** The Oxford Institute of Technology and Justice has submitted comments to the forthcoming Tallinn 3.0 on the International Law Applicable to Cyber Operations on this topic and will continue to contribute to discussions on this issue, including in relation to accountability for attacks conducted by or against private actors.

- **Promoting capacity-building for States in this area,** in particular on existing legal accountability mechanisms under international law and clarification of how these can be used effectively in the cyber context. The Oxford Institute of Technology and Justice will develop a roadmap to legal accountability in the cyber context, and plans to contribute to discussions conducted under the auspices of the United Nations' cyber process.

- **Assessment of options related to reform or creation of inter-State dispute settlement mechanisms for malicious cyber operations**, including whether there is scope for a standing panel to hear claims in this area; whether there is potential for clarification on standards of evidence and proof in relation to attribution of cyber activity; and the role of non-State actors in legal accountability mechanisms.

- **Strengthening the work of multistakeholder alliances on accountability for malicious cyber operations**. Building on contributions in 2025 at the International Conference on Cyber Conflict (CyCon) and the Internet Governance Forum, the Oxford Institute of Technology and Justice will collaborate with the Oxford Process on International Law Protections in Cyberspace and others to promote multistakeholder discussion on accountability in the cyber context, including on how States can responsibly build capacity to prosecute cybercrime.

- **Offering investigators, prosecutors and judges opportunities for knowledge-exchange and training** in relation to the handling of cases involving malicious cyber activity and the handling and analysis of complex technical and digital evidence. The Oxford Institute of Technology and Justice will collaborate with partners to facilitate this work, for example through convening peer-to-peer discussions and masterclasses.

- **Analysis of the role of AI in accountability for malicious cyber operations,** including the potential for AI-powered tools to contribute to the prosecution of cybercrime, and a forthcoming contribution to a textbook on the role of AI in the management of digital evidence in cases before international criminal tribunals. The Oxford Institute of Technology and Justice will assess the potential for AI to be leveraged for investigations, evidence handling and establishing attribution, while also identifying the risks and ways in which they can be mitigated.

[306] This work falls under the Institute's Accountability pillar and will be complemented by work on legal accountability options for non-State actors.

Acknowledgments

The authors would like to thank Daisy Peterson for her valuable assistance with research and editing, and Anna Harris, Ruth Collier and Douglas McFarlane for their help with editing and publishing this Policy Brief. The authors are also very grateful to Marko Milanovic, Shehzad Charania, Russell Buchan, Talita Dias, Tsvetelina van Benthem and Bogdana Cherniavska for their helpful comments. This Brief also draws on confidential conversations with policymakers, practitioners, and scholars, some of whom prefer not to be identified. We thank them for their valuable insights.

THE INSTITUTE IS HONOURED TO HAVE RECEIVED INAUGURAL MULTI-YEAR FUNDING FROM MICROSOFT TO LAUNCH ITS WORK.