EU CYBER DIRECT

SHADES OF GREY: CYBER INTELLIGENCE AND (INTER)NATIONAL SECURITY

Dennis Broeders and Camino Kavanagh

EU CYBER DIRECT

SHADES OF GREY: CYBER INTELLIGENCE AND (INTER)NATIONAL SECURITY

Dennis Broeders and Camino Kavanagh

October 2023

Suggested citation: Broeders, Dennis & Camino Kavanagh (2023) *Shades of Grey: Cyber Intelligence and (Inter)national Security*. Policy brief, EU Cyber Direct, October 2023.

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Cover image credits: The afflicted modernist /Unsplash
Figure 1 credits: Christian Dietrich, Data Visualisation Designer at EU Institute for Security Studies (EUISS)

Implementing organisations for EU Cyber Direct:

EU Institute for Security Studies
Carnegie Endowment for International Peace
Leiden University

Funded by the European Union

Contents

Executive summary

This paper is about cyber intelligence in the context of national and international security. It is a call for greater attention to cyber-intelligence operations in diplomatic processes relevant to the use of cyberspace/ICTs by states. Under the term 'cyber intelligence', the paper distinguishes 'intelligence operations', i.e. espionage activities or operations conducted via cyber means to support political decision-making, from intelligence-led operations, i.e. covert action such as sabotage, subversion or influence.

The paper acknowledges that despite earlier assumptions, cyberspace is less a war-fighting domain than one in which there is constant competition between intelligence agencies. It highlights the scope, scale and tenacity of many of the intelligence and intelligence-led cyber operations discovered over the past decade, each of which has set new precedents in terms of the number of government institutions, businesses and individuals affected, has caused much consternation, yet has led to little discernible action in terms of discussing, let alone agreeing on, possible legal or normative restraints or limits at the international level.

The paper nonetheless highlights some of the normative actions that are slowly taking place at the national level, or in specialised bodies that shape national-level decisions, to place some restraints on the means and methods used in intelligence and intelligence-led cyber operations. It notes that such action often results more from societal pushback to state activity revealed in significant leaks or breaches than from a pre-emptive effort to ensure that intelligence activity is conducted in accordance with existing rules and principles. Some of these developments are important, particularly where privacy, data protection and broader human rights are concerned. And while some such developments have served to provide a legal base for existing activity, in some instances they have resulted in new or reinforced oversight and accountability mechanisms and privacy guardrails. The paper also highlights the increasingly expansive nature of foreign intelligence/counter-espionage legislation in some jurisdictions, and how this contrasts with the limited restraints placed on the cyber-activity of a given state's own intelligence agencies abroad. It asks whether this expansion of foreign intelligence legislation is resulting from or driving reciprocal action on the part of other states.

Finally, the paper calls for a franker discussion among states on intelligence-led cyber operations and the different types of action (espionage/intelligence collection, covert action) that they consider to fall under that rubric. Such a discussion can start bilaterally or among a small number of states, but at some stage it will need to be broadened. The paper puts forward some suggestions on what such a discussion could focus on.

1. Introduction[1]

Many cyber operations that have come to light in recent years are intelligence operations, in the sense that they entail some form of espionage: the extraction of secret or confidential data from a government, international organisation or a private company. In addition, many of the cyber operations that have been discovered and attributed to foreign intelligence agencies would not be considered classic espionage, i.e. 'intelligence operations', but rather covert operations, since they involve some element of sabotage, subversion or influence, i.e. 'intelligence-led operations'. Intelligence agencies are extremely active in cyber operations below the threshold of armed conflict, and this has not gone unnoticed.[2] In political, diplomatic and policy circles there is a growing awareness that intelligence agencies play a bigger role in cyber operations than most military cyber commands. This recognition is also evident in ongoing academic debates about whether below-the-threshold strategic outcomes in, through and from cyberspace are possible, for example through persistent engagement,[3] or whether such below-the-threshold activity is best understood as 'an intelligence contest'. [4] On the latter, and as noted by one of the experts at the Valencia workshop, there is also the view that intelligence can contribute to strategic stability through better decision making, pre-bunking hostile information operations, and letting off steam: an aspect that is generally neglected in international relations theory.

Elements of this debate are now playing out in policy and practice, including with regard to their perceived influence on cyber-specific institutional arrangements such as the UK's National Cyber Force (NCF). The latter fuses intelligence and military personnel and capabilities in a unified structure to proactively respond to cyber threats both in

[1] The authors would like to thank all the participants in the EU Cyber Direct Research Seminar on 'Cyber Espionage' in Valencia in November 2022 for the discussion and their insights. They are especially grateful to Monica Kaminska, Jon Lindsay, Thorsten Wetzling, Damien van Puyvelde and Nicholas Tsagourias for their thoughtful comments on an earlier version of this paper.

[2] There is an ongoing academic debate on whether we should see cyber conflict in peacetime as an intelligence contest, rather than a military affair. See for a good overview Robert Chesney and Max Smeets (eds, 2023), *Deter, disrupt or deceive: Assessing cyber conflict as an intelligence contest*. Washington, DC: Georgetown University Press.

[3] Joshua Rovner divides those writing on strategic theory into two types: proponents of a more aggressive approach centred on 'agreed competition', and proponents of a more cautious approach whose writings focus on crisis instability, escalation dynamics and security dilemmas. For the former, see in particular Michael Fischerkeller, Richard J. Harknett and Emily O. Goldman (2023), *Cyber persistence theory: Redefining national security in cyberspace*. Oxford: Oxford University Press; Michael P. Fischerkeller (2022), 'A cyber persistence way to norms', *Lawfare*, https://www.lawfaremedia.org/article/cyber-persistence-way-norms. For the latter, Rovner cites Jason Healey (2019), 'Getting the drop in cyberspace', *Lawfare*, https://www.lawfaremedia.org/article/getting-drop-cyberspace; Martin Libicki (2012), *Crisis and escalation in cyberspace*. Santa Monica, CA: Rand Corporation; Ben Buchanan and Ryan Evans (2017), 'The promise and peril of cyber operations', *War on the Rocks*, https://warontherocks.com/2017/02/the-promise-and-peril-of-cyber-operations/; Joshua Rovner (2019), 'Cyber war as an intelligence contest', *War on the Rocks*, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[4] See for instance Michael Poznansky (2021), 'Covert action, espionage, and the intelligence contest in cyberspace', *War on the Rocks*', https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/; Rovner, 'Cyber war as an intelligence contest'; Jon Lindsay, 'Military organizations, intelligence operations, and information technology', in Robert Chesney and Max Smeets (Chairs), 'Policy Roundtable: Cyber competition as an intelligence contest', *Texas National Security Review*, Special Issue, September 2020; Lennart Maschmeyer, 'Subversion, cyber operations, and reverse structural power in world politics', *European Journal of International Relations*, 29(1), 79–103.

peacetime and in conflict, deploying a broad range of intelligence capabilities ranging from espionage to covert action. The NCF's description of operations 'closely aligns with U.S. insights about cyberspace embodied in the defend forward strategy and the operational approach of persistent engagement'.[5] The differences, others argue, lie inter alia in the NCF's 'articulation of a value proposition for cyber operations, while also being cognisant of some of the real limitations of offensive cyber power'.[6] This new UK institutional arrangement is heavy on principles and on committing to legislative and executive oversight, including through the parliament's Intelligence and Security Committee, although, as we discuss below, it is still light on important details. Meanwhile, renewed efforts are being made to clarify the 'cyber competition as an intelligence contest' argument, debating the logic and implications of such a framing and examining it across several areas of cybersecurity policy and in different national contexts.[7]

At the international level, the debate on the actions of intelligence agencies in cyberspace is limited at best. It has received some attention from legal scholars, including in the *Tallinn Manual 2.0*, which discusses peacetime cyber espionage under the heading of 'cyber operations not *per se* regulated by international law'.[8] Moreover, mirroring the treatment of intelligence under international law, intelligence and intelligence-led cyber operations are not generally discussed in international negotiations on the responsible use of ICTs by states. The consensus reports that are the outcome of the UN processes on responsible state behaviour in cyberspace—the UN Group of Governmental Experts (UNGGE) and the UN Open-Ended Working Group (UNOEWG)— reference the military use of ICTs, yet pay scant attention pay to intelligence-led operations. The 2021 reports of both groups marked a slight shift in this regard with their reference to 'a notable increase in ICT-enabled covert information campaigns', yet one has to be creative in identifying adequate response mechanisms in the subsequent sections of said reports. Undoubtedly, many of the elements in the reports can be understood to apply to the actions of any government agency, including signals-intelligence agencies and other relevant structures. Yet, even when politicians and diplomats have publicly decried certain cyber operations conducted by intelligence agencies, such reactions—generally articulated in public outcries or more measured attribution statements—may well identify the harms posed to individuals, the economy and the state, but rarely specify the legal principles or norms that these operations violate or undermine.

---

[5] Michael Fischerkeller, Richard J. Harknett and Emily O. Goldman (2023), 'U.K. National Cyber Force, responsible cyber power, and cyber persistence theory', *Lawfare*, https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory.

[6] Erica D. Lonergan, 'Similarities and differences between the UK and US approaches to cyber operations', in Tim Stevens, Rory Cormac, Erica D. Lonergan, Dan Lomas, Pia Hüsch and Joe Devanny, 'Evaluating the National Cyber Force's "Responsible cyber power in practice"', RUSI, https://rusi.org/explore-our-research/publications/commentary/evaluating-national-cyber-forces-responsible-cyber-power-practice.

[7] Robert Chesney and Max Smeets (eds, 2023), *Deter, disrupt or deceive: Assessing cyber conflict as an intelligence contest*. Washington, DC: Georgetown University Press.

[8] Michael Schmitt (2017), *Tallinn Manual 2.0. On the international law applicable to cyber operations* (2nd edn). Cambridge: Cambridge university Press, 168–73. Interestingly, the other issue covered under this section is 'Non-state actors'.

This lack of attention can be explained by a number of factors, including:

- a general (and increasingly contested) understanding among states that intelligence-gathering activities are permitted, including under international law, regardless of the means and methods involved and the scope, scale and effects of the activity (we don't talk about intelligence), even if there is also a view that certain means and methods may violate international law);[9]
- the reality that we do not always have visibility on the full scope of cyber-related activity that intelligence actors engage in, including where their role and the operations they engage in begin and end (we don't know about intelligence).

Both obfuscations are intentional. Politically, it has made sense for countries not to address the behaviours of intelligence agencies in legal terms, other than in domestic law, although even the latter is relatively recent. Given the secret nature of espionage and intelligence writ large, it is logical that we do not have full visibility on their activities. However, this does make it hard to make meaningful assessments of these activities from a policy or normative perspective. Moreover, if perceptions start to shift and countries start to pay more attention to the cyber activities of intelligence agencies, the previously accepted practice of disregarding these actions in international law and in diplomatic practice may start to be questioned. Reactions to the SolarWinds hack as well as to earlier operations such as NotPetya suggested a shift in this direction. Some national-level developments also suggest that there is greater pressure to ensure alignment of cyber intelligence-related activity with existing legal norms and principles. This is partially evident in the UK government's paper on Responsible Cyber Power as applied to the country's new NCF.[10] We argue that there is a need to discuss cyber-intelligence operations in diplomatic processes: first in smaller, like-minded settings and ultimately at the international level.

In order to discuss the role of cyber intelligence and related legal, normative and governance challenges at the international level, the EU Cyber Direct programme convened a group of experts in November 2022.[11] These experts discussed a number of issues including **definitions and concepts**; the **role and status of cyber-intelligence actors**; the **blurred lines between government and private actors** in cyber intelligence; developments in the field of **international law and cyber espionage**; domestic **accountability and oversight measures**; and possible **policy**

[9] The full legal argument—and debate—is more nuanced, as is set out in Section 4 of this paper.
[10] UK National Cyber Force, 'Responsible cyber power in practice', 4 April 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html.
[11] The experts that attended were: Dennis Broeders (Leiden University), Gary Brown (National Defense University, Washington, DC); Francois Delerue (IE University Madrid); Joe Devanny (King's College London) Monica Kaminska (Leiden University); Camino Kavanagh (King's College London); Jon Lindsay (Georgia Tech); Lennart Maschmeyer (ETH Zürich); Damien van Puyvelde (Leiden University); Nicolas Tsagourias (Sheffield University); Thorsten Wetzling (Stiftung Neue Verantwortung, Berlin); Kim Zetter (independent journalist).

recommendations. The discussions were held under the Chatham House Rule but inform this research paper.

2. Definitions and concepts: what is cyber intelligence?

Main points

- There is no agreed definition of intelligence, and no agreed definition of espionage. The political system and culture of a given country often determine what intelligence is in practice. The same applies to cyber intelligence and cyber espionage.
- The activities of, or the means and methods deployed by, intelligence agencies are often used in lieu of a definition. There is no agreement on where these start and stop (intelligence is what intelligence actors do).
- The limited international debate on intelligence and intelligence-led cyber operations has tended to focus mainly on intelligence operations, i.e. cyber espionage/intelligence collection. That this kind of activity has garnered attention is warranted given the seriousness of many recent cyber-espionage operations that have come to public attention.
- There are persistent debates over whether 'covert action' conducted by cyber means, i.e. intelligence-led operations, should be classified as intelligence activity. Covert cyber operations are generally not addressed at the international level, even though such action is becoming an increasingly common feature of inter-state activity during peacetime.
- The digital age has propelled signals-intelligence agencies to the forefront of intelligence activities. It has also turned intelligence and other such agencies into hunters as well as gatherers of information.
- Secrecy has historically been the defining characteristic of intelligence. This is no longer the case. Regardless of how we describe this situation—the declining half-life of secrets, delayed disclosure, unacknowledged activity—if we can't name it, we can't discuss it. This makes it difficult to have any meaningful progress—legal, normative or otherwise—on addressing the issue.
- The lines between military and civilian roles in intelligence and in active operations are blurring. This can be problematic from an oversight and accountability perspective.
- There are persisting tensions between what countries prohibit foreign agents from doing on their territory and what they do on the territory of others. Cyberspace accentuates these tensions.
- In many instances, it is difficult to differentiate between the intelligence activities of 'democratic' and 'autocratic' countries, since they deploy similar means and methods. Yet the intelligence practices of most countries sit between these

opposing 'democratic' and 'authoritarian 'poles, varying in their international interests, reach and commitment to safeguards.

2.1 What is intelligence?

Any meaningful discussion would have to start with at least some agreement on definitions or terminology, yet this is no easy task. As noted by Lindsay in his discussion on the associated challenges, 'intelligence operations are transgressive by nature: They cross protected boundaries, break established laws (at least those observed by the target), and subvert established systems. Small wonder that intelligence refuses to be contained by a definition.'[12] Also, the fact that states have traditionally regarded intelligence as unconstrained by international law has militated against a precise understanding of what intelligence 'is'. A range of political, cultural, historical and institutional factors make it even more complex to arrive at working definitions of intelligence at the international level. This complexity was borne out, for instance, in efforts to develop a working definition of intelligence in the UN peacekeeping domain. UN member States contributing to the development of the relevant policy submitted such conflicting views of what intelligence is that efforts to reach a common definition were discarded. Instead, a concept –'peacekeeping-intelligence' was devised, and the focus shifted to ironing out the core features of the 'peacekeeping-intelligence' cycle.[13]

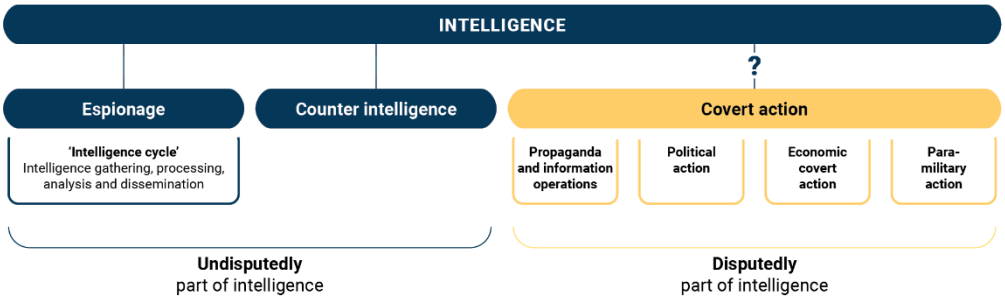
The seminar in Valencia discussed an encompassing range of activities associated with intelligence and espionage, but there was no real consensus on where intelligence begins and where it ends. The main bone of contention in terms of defining intelligence is whether it encompasses covert action or only includes espionage (gathering of protected data and information) and counter-intelligence (see Figure 1).

[12]Jon Lindsay, 'Military organizations, intelligence operations, and information technology', in Chesney and Smeets, 'Policy Roundtable'.

[13] Sarah-Myriam Martin-Brûlle, 'Finding the UN way on peacekeeping-intelligence', International Peace Institute, cited in Nicholas Tsagourias and Camino Kavanagh, 'The use of intelligence in UN peacekeeping operations' in Russell Buchan and Iñaki Navarrete (eds), *Research Handbook on Intelligence and International Law* (Edward Elgar, 2024/forthcoming).

Figure 1

Intelligence and its component activities



A narrower approach focuses on the so-called 'intelligence cycle': the gathering, processing, analysis and dissemination of information to support decision-making by policy-makers.[14] While the basic framework of the intelligence cycle is similar across countries, differences in priorities, resources and political and cultural contexts generally mean that there are differences in how the intelligence cycle is applied in practice. Purists equate this more traditional understanding of espionage with intelligence. There is wide agreement that the core function of intelligence is espionage, explained as consisting of 'the access, on behalf of a state, to information that is held by another state and considered as confidential or strategic, in the military, security, or economic field'.[15] Indeed, secretly gathering information on a target and using that knowledge to advise and reduce uncertainty for decision-makers remain the cornerstones of intelligence.[16] The practice has continued to evolve over the decades. To many countries it now includes economic espionage, as well as 'surveillance programs implemented by intelligence agencies toward individuals [and] company-to-company industrial espionage'.[17] Even though many states consider classic political espionage a normal—and even a lawful—activity in the international domain, the fact that espionage involves the unauthorised extraction of secret or confidential information almost always makes it a violation of the domestic law of the country that is the target of the activity or operation.

Many analysts include 'covert action' as an activity that falls within the realm of intelligence for historical, institutional and practical reasons.[18] Covert action involves 'activities conducted in support of national foreign policy objectives abroad which are

[14] David Gioe, Michael Goodman and Tim Stevens (2020), 'Intelligence in the cyber era: Evolution or revolution?', *Political Science Quarterly*, 135(2), 191–224: 209. The five stages of the intelligence cycle are generally regarded as planning and direction, collection, processing, analysis and production, and dissemination.
[15] François Dubuisson and Agatha Verdebout (2018), 'Espionage in international law', *International Law*, https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0173.xml.
[16] Gioe et al., 'Intelligence in the cyber era', p. 223.
[17] Harriet Moynihan (2019), 'The application of international law to state cyberattacks: Sovereignty and non-intervention', Chatham House, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.
[18] Chesney and Smeets, 'Policy Roundtable'.

planned and executed so the role of the [sponsor] is not apparent or acknowledged publicly…'.[19] The sponsor's involvement is unknown if the operation remains fully covert; if the operation is discovered, the sponsor might retain a degree of plausible deniability. Some scholars have explained the value of covert action from the perspective of escalation management dynamics, in that covert action allows states to compete without fear of retaliation. In the event that rivals discover an operation, the secrecy shrouding it allows for a tacit behind-the-scenes response, thus minimising potential escalation or limiting an ensuing conflict.[20] Others have explained it from the perspective of domestic politics, in that covert action helps reduce audience costs in situations where the action may violate a peremptory norm such as non-intervention.[21]

Even if both espionage and covert action fall under the broader rubric of intelligence, it is important to note, as Poznansky does, that 'they perform qualitatively different functions': the objective of the former is predominantly information acquisition; that of the latter is to have an effect.[22] The lines between these two functions are, however, increasingly blurred, with many operations straddling the intersection of espionage and covert action and pretty much all 'traffic[king] in secrecy and deception'.[23] Lindsay, for instance, includes counter-intelligence, influence operations and covert action as intelligence activities.[24] So too do Cormac, Walton and van Puyvelde, pointing to three broad types of activities as part of covert action, each of which represents an increase in the use of violence: propaganda, political action and paramilitary action, ranging from training insurgent groups to assassination.[25] Zegart maintains that covert activities can be classified in four types: propaganda/information operations; political action; economic covert action; and paramilitary activities.[26]

Academic definitions are clearly not conclusive: whether on the big divide between espionage and covert action or on the specifics of what exactly constitutes covert action. Some argue that all these activities should be taken together, and that intelligence can be simply defined as 'secret statecraft'.[27] Others go even further. For instance, Stout and Warner make the case that 'Intelligence is as intelligence does', i.e. what intelligence

[19] Reagan (1981), cited in Michael Poznansky (2019), 'Feigning compliance: Covert action and international law', *International Studies Quarterly,* 63(1), 72–84: 72. The US Congress makes a clear distinction between covert activities (visible with hidden sponsorship) and clandestine activities in which both cause and effect are invisible. Michael Warner (2019), 'A matter of trust: Covert action revisited', *Studies in Intelligence*, 63(4) (Extracts, December 2019)

[20] Anderson (1998) and Brown (2014), cited in Poznansky, 'Feigning compliance', 72.

[21] Ibid.

[22] Michael Poznansky (2021), 'Covert action, espionage and the intelligence contest in cyberspace', *War on the Rocks*, https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/.

[23] Ibid.

[24] Jon Lindsay (2021), 'Cyber conflict vs. Cyber Command: Hidden dangers in the American military solution to a large-scale intelligence problem', *Intelligence and National Security*, 36(2), 260–78: 262.

[25] Rory Cormac, Calder Walton and Damien van Puyvelde (2022), 'What constitutes successful covert action? Evaluating unacknowledged interventionism in foreign affairs', *Review of International Studies*, 48(1), 111–28.

[26] Amy Zegart (2022), *Spies, lies and algorithms: The history and future of American intelligence*. Princeton, NJ: Princeton University Press, 172.

[27] Lindsay, 'Cyber conflict vs. Cyber Command', 262.

agencies *do* will over time become what intelligence *is*.[28] While there is no consensus in the academic literature on what is 'in' and what is 'out' when it comes to intelligence, it is evident that 'whether covert action is regarded as part of intelligence or as something separate clearly impacts the ethical landscape we are considering'.[29]

2.2 What is cyber intelligence?

The underdefined nature of intelligence is reflected in what is commonly referred to as 'cyber intelligence'. At the core of cyber intelligence is the espionage function, and it goes without saying that the digitisation of the state, society and the economy has supercharged digital espionage. Bulk interception, collection and surveillance are now key features of cyber espionage, as are highly tailored espionage operations such as the OPM and SolarWinds hacks and the Snake implants.[30] The digital age has put signals-intelligence agencies firmly in the lead when it comes to cyber intelligence, while also propelling a shift from what was heretofore a largely passive function to a much more active one.[31] In the words of Bill Black, a former National Security Agency (NSA) deputy director, the digital age required a more proactive approach on the part of signals agencies: 'In order to get through the morass of data, we have become, rather than gatherers of the past, hunters in cyberspace.'[32]

In the cyber domain, intelligence does not stop at espionage. Intelligence agencies conduct operations in the digital domain that clearly resemble aspects of covert action, while stopping short of the highest level of violence, i.e. there are no cyber assassinations (even if targeting is greatly enhanced). Indeed, the internet is not just a natural environment for mass-scale espionage; it is also very well suited to intelligence-led covert operations. This includes information operations (such as disinformation campaigns and elections interference), all kinds of subversive operations (such as hack and leak operations and the political use of ransomware) and sabotage operations (such as Stuxnet and NotPetya). Victim states often respond indignantly to some of these 'intelligence operations', some of which have been the subject of public attribution

[28] Mark Stout and Michael Warner (2018), 'Intelligence is as intelligence does', *Intelligence and National Security*, 33(4), 517–26.
[29] David Omand and Mark Phythian (2018), *Principled spying: The ethics of secret intelligence*. Oxford: Oxford University Press.
[30] For the OPM hack see Dan Efrony and Yuval Shany (2018), 'A rule book on the shelf? Tallinn Manual 2.0 on cyber operations and subsequent state practice', *American Journal of International Law*, 112(4); Joe Devanny, Ciaran Martin and Tim Stevens (2021), 'On the strategic consequences of digital espionage', *Journal of Cyber Policy*, 6(3), 429–50; for the SolarWinds hack see Marcus Willett (2021) Lessons of the SolarWinds Hack, *Survival*, 63(2), 7-26, DOI: 10.1080/00396338.2021.1906001, and Devanny et al., 'On the strategic consequences of digital espionage'; for the Snake malware see Cybersecurity & Infrastructure Security Agency (2023), 'Hunting Russian intelligence 'Snake' malware', https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a.
[31] Jon Lindsay, in Chesney and Smeets, 'Policy Roundtable'.
[32] Cited in Steven Loleski (2019), 'From cold to cyber warriors: The origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers', *Intelligence and National Security*, 34(1), 112–28.

statements, which in turn are often based, at least partially, on information gathered by their own intelligence agencies.[33]

The prominent role of intelligence agencies in cyberspace, and of cyberspace in shaping the activities of intelligence agencies, has influenced the nature and the methods of intelligence work. At least four big changes should be taken into account when discussing ethical, normative and legal boundaries of cyber intelligence.[34] Firstly, the *scale* of intelligence operations has increased dramatically. This includes both traditional espionage and covert action discussed above such as information operations, subversive operations and sabotage. Secondly, the digital age has increased and changed the nature of the *attack surface* for intelligence activities. Increasingly, the private sector and citizens are implicated in cyber-intelligence operations that used to be much more narrowly focused on state actors and assets. Networks, platforms, supply chains, software and hardware are all 'fair game' in cyber-intelligence operations. Thirdly, cyber intelligence carries with it a high degree of *ambiguity*—at the outset it is hard to determine the purpose of a cyber operation (espionage, subversion or sabotage, or an espionage operation prepping the ground for one of the latter two)—which, some argue, is potentially escalatory and/or destabilising.[35] Fourthly, the tools and methods of cyber intelligence have a *trickle-down effect* in terms of cyber insecurity. Zero days, malware, backdoors and exploits are lost, stolen, leaked or discovered in the wild. They are then analysed and become available to other malicious actors—both state and criminal—making companies and individuals everywhere less cybersecure. Taken together, these changes are significant and call into question whether 'cyber intelligence' is best left unaddressed in terms of ongoing diplomatic processes aimed at shaping the normative framework applicable to cyber operations and other uses of ICTs by states.

2.3 The decline of secrecy

Irrespective of the precise demarcations of the activities that are or are not considered to be intelligence or espionage, secrecy is widely considered to be at their core. In this regard, one of the participants at the seminar argued that intelligence is simply 'secret statecraft'. Secrecy obviously makes it harder to define what intelligence agencies are

[33] See for example the official US government attribution of 2016 US election interference to Russia through a joint report of the CIA, FBI and NSA, under the auspices of the Office of the Director of National Intelligence (ODNI), which named the Russian government (the GRU) and non-government operatives (such as the IRA) and stated that 'Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election' (Office of the Director of National Intelligence (2017) *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*., ii; Michael Schmitt (2018) 'Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', *Chicago Journal of International Law* 19 (1): 30–67). The CIA and the FBI made the attribution with a 'high degree of confidence'. The NSA concurred, but only with a 'moderate' degree of confidence (Schmitt 2018, 34).

[34] These four changes are taken from Dennis Broeders (2023), 'Addressing the elephant in the room: Cyber intelligence and international security', inaugural address, Leiden University, 31 March 2023, 7–8. https://scholarlypublications.universiteitleiden.nl/access/item%3A3572086/view

[35] Ben Buchanan (2016), *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford: Oxford University Press.

and do: outsiders have a limited view on what these agencies do, and no reliable way to determine how much or how little they themselves know. However, if secrecy is the defining characteristic of intelligence, then the digital age is increasingly problematic for this form of statecraft. For many reasons—open-source intelligence, hacks and leaks, the increase of private contractors in intelligence, investigative and citizen journalism—intelligence agencies are having a much harder time keeping their activities a secret.[36] The recent so-called Discord Leaks are just the latest in a series of intelligence leaks, even if the motivation for this specific leak is thinner than ever before.[37]

Peter Swire, a member of the commission tasked by President Obama to study the functioning of the US intelligence services, wrote in 2015 that in the digital era, secrets are not likely to remain secrets for as long as they used to. He called this the 'declining half-life of secrets'.[38] Aldrich and Moran have advanced this argument, suggesting that we may be headed for a world in which 'there are no secrets, only delayed disclosures'.[39] Another of the participants in the seminar suggested that intelligence will increasingly be 'unacknowledged' rather than secret. If activities cannot be kept secret, then the next best thing seems to be to refuse to acknowledge involvement. However, this is not without consequences. If the typical practice is to 'neither confirm nor deny' or even to wilfully deny involvement—even when there is strong evidence of state involvement—this has important implications for any diplomatic and legal discussions on the subject. For instance, legal discussions are only possible on the basis of acknowledged facts and responsibilities. Customary law cannot be built on unacknowledged state action: 'secret and covert acts cannot constitute evidence of state practice that forms customary international law or reflects states' interpretations of treaty obligations'.[40] In a world in which plausible deniability is replaced with 'implausible deniability',[41] the activities of intelligence agencies will become even harder to address.

2.4 Intelligence cultures

Because intelligence is underdefined and operates under the radar, countries approach and define it differently. These differences often stem from the political system and culture of a given country, i.e. its 'regime type', as well as different legal frameworks with varying standards for governance and accountability of—and cooperation among—

[36] Broeders, 'Addressing the elephant in the room'.
[37] Julian Borger (2023), 'Pentagon leaks linked to young gun enthusiast who worked at military base – report', *The Guardian*, 13 April.
[38] Peter Swire (2015), 'The declining half-life of secrets and the future of signals intelligence', New America Cyber Security Fellows Paper Series no. 1, July. Washington: New America Foundation.
[39] Richard Aldrich and Christopher Moran (2019), '"Delayed disclosure": National security, whistle-blowers and the nature of secrecy', *Political Studies*, 67(2), 291–306.
[40] A.H. Perina (2015), 'Black holes and open secrets: The impact of covert action on international law', *Columbia Journal of Transnational Law*, 53, 507–83: 511.
[41] Rory Cormac and Richard Aldrich (2018), 'Grey is the new black: Covert action and implausible deniability', *International Affairs*, 94(3): 477–94.

intelligence agencies. The US, for instance, has by far the largest number and variety of intelligence agencies: 18 in total.[42] As a rule of thumb, larger countries with geopolitical ambitions tend to have more intelligence capabilities (agencies, workforce, budget and capacities). In terms of the domain and scope of intelligence, the differences between civil and military intelligence and between domestic and foreign intelligence are important. These traditional boundaries are often related to different rules of engagement, procedures and practices, leading to different subcultures.

Traditionally, many countries have special agencies for gathering military intelligence, i.e. 'timely, accurate information useful in the attainment of military objectives'[43] and—in some cases—for covert operations. In the digital age, however, military intelligence agencies are increasingly engaged in carrying out 'peacetime' operations. The cyber activities of Russia's foreign military intelligence agency—commonly known by its previous abbreviation, GRU—are a case in point.

A complicating factor in cyberspace is that due to the technical complexity of the domain of operations, signals-intelligence agencies are often assigned the lead when states start to build up cyber capabilities for both intelligence and military operations. This often means that in cyberspace, the line between military capabilities and intelligence capabilities has become blurred. Here the fact that the US signals agency (the NSA) and the military US Cyber Command are under the same double-hatted director/commander is a case in point. So too is the UK NCF, which co-locates Government Communications Headquarters (GCHQ), the Ministry of Defence and the Secret Intelligence Service.[44] While this blurring is partially explained by the availability of technical expertise and path dependency—and has operational advantages—there are also legal, normative and operational drawbacks. Amy Zegart characterises the situation: 'The good news is that intelligence and warfighting are now much more connected. The bad news is that intelligence and warfighting are now much more connected.'[45]

The difference between domestic and foreign intelligence is important, as most democratic states purport to have severe limitations on the activities that intelligence and security agencies can deploy domestically. Citizens tend to be (constitutionally) much more protected against certain means and methods that are considered acceptable when deployed as part of foreign intelligence operations.[46] However, as evidenced in many of the major revelations of state surveillance practices that have emerged over the years, such safeguards for citizens are not foolproof and are routinely trampled on. Where democratic safeguards do not exist, the distinction between

[42] Zegart, *Spies, lies and algorithms*, 73–4.
[43] Everett Carl Dolman (2000), 'Military intelligence and the problem of legitimacy: Opening the model', *Small Wars & Insurgencies*, 11(1), 26–43.
[44] 'UK National Cyber Force, 'Responsible cyber power in practice'.
[45] Zegart, *Spies, lies and algorithms*, 193.
[46] Where protections from foreign intelligence activities are concerned, as we discuss in Section 4, recent developments such as the Transatlantic Data Privacy Framework are moving in a positive direction.

domestic and foreign intelligence activities is even thinner. For instance, Hatfield argues that in authoritarian states, intelligence agencies function more as 'palace guards', established to protect the regime at all costs, which means that domestic and foreign operations blur and legal oversight is usually missing.[47] The intelligence practices of most countries sit between these opposing 'democratic' and 'authoritarian' poles, varying in their international interests, operational reach and commitment to such safeguards and oversight.

This adds another layer of complexity to the debate about intelligence agencies and their activities in general. The discussion on the behaviour of intelligence agencies is about goals and intentions (the good guys versus the bad guys) as well as the means and methods they employ (lawful/legitimate and unlawful/illegitimate activities). Where methods are concerned, there is wide consensus on the legitimacy of classical espionage, although many countries tend to make a public show of reacting when it is revealed that their allies are spying on them. Where there is less consensus—for instance, in cases that involve a degree of coercion and in which disruptive, undermining and violent methods are deployed—the focus tends to be on the political motives and nature of the regime behind the activity. Legally however, there is no a priori reason to treat them differently. The nature and goals of intelligence agencies and the political system they are embedded in do not formally play a role in the legal assessment of cyber-intelligence operations. But they do play a role for states in (a) politically calling out the activities of the intelligence agencies of other states ('the bad guys') and (b) justifying the role and activities of their own intelligence agencies ('the good guys').[48]

[47] Joseph Hatfield (2022), 'Intelligence under democracy and authoritarianism: A philosophical analysis', *Intelligence and National Security*, 37(6), 903–19.

[48] For a discussion about the tensions between political responses to cyber-intelligence operations conducted against democratic states and the reaction of intelligence agencies of those states—centring on the question of responsible victimhood—see Devanny et al., 'On the strategic consequences of digital espionage'.

3. Public–private interactions and transactions

Main points

- Private actors—telecommunications, technology and cybersecurity companies, non-profits, university labs—are increasingly enmeshed in the world of intelligence and espionage.
- The private sector largely owns and operates the transmission media, digital assets and infrastructure that intelligence agencies rely on for their trade. This creates tensions as well as complicated dependencies.
- These dependencies and an increasingly digitalised world have had important implications for intelligence organisations, including where Human Resources are concerned. The constant wheel of insourcing and outsourcing of technology and skills poses risks to secrecy.
- Depending on the jurisdiction, the role that some companies play in intelligence gathering and analysis can be hard to distinguish from that of intelligence organisations, yet much less oversight is involved.
- Reporting by such companies sometimes informs the investigations and attribution findings of governments.

Private actors have become entangled in the world of intelligence and cyber espionage in manifold ways, their products and services both changing the context in which intelligence agencies operate and shifting the goalposts for the profession itself. Some changes stem from the markets in which intelligence agencies procure their tools, others from the fact that intelligence agencies increasingly operate in the context of a private, corporate world. Various forms of privatisation—procurement, insourcing and outsourcing—as well as other encounters with private actors and (big) technology companies have made intelligence less self-sufficient and more dependent on private actors than was traditionally the case. As private infrastructure, networks and platforms are now key 'hunting grounds' for intelligence agencies and vulnerabilities or flaws in their software and security are the methods to gain access, government relationships with 'Big Tech' are strained, even when they are domiciled in the same country. It is no secret that certain companies sometimes willingly cooperate with intelligence agencies (especially their 'home' agencies), and sometimes resist cooperation. In a structural sense there is not much room to avoid each other in the digital domain, since many of the companies own and operate the very space that intelligence actors operate in, while others, such as cybersecurity companies, share it.

Intelligence in the digital age has been changing. Like many government professions, intelligence has become less of an exclusive 'calling for life'. For various reasons, it has become more open to career change—people moving in and out—and more open to

outsourcing to, and insourcing of, private contractors. In the US, for example, more than a million private contractors hold security clearances, accounting for about a quarter of all cleared personnel.[49] Not all these contractors work in intelligence agencies, but the number gives an indication of the degree to which national security, which includes intelligence, has become a public–private affair in some countries.

In terms of *military* contracting, in many countries, but especially the US and the UK, much of the private contribution can be characterised as 'contracting out'. This is particularly the case with the military–industrial complex that enables R&D and the design, production, delivery and maintenance of military weapons and technology. Indeed, arms development and everything underpinning it is largely a private enterprise, albeit geared to meet military requirements and with controlled access to government contracts. The situation becomes more complicated when defence activities and actual deployment (although not necessarily combat activities) are outsourced to private military and security companies.

As for cyber-*intelligence* private contracting, which does not require much in terms of hardware, it mostly takes the form of 'contracting in'. Given that cyber-intelligence operations tend to be 'hands-on', private sector contractors often work side by side with official intelligence employees. This blurs the line between the public and private sectors and related roles and responsibilities. It also spreads operational knowledge on (cyber-) intelligence operations beyond official intelligence agencies into the private sector. The famous 'revolving door' of the traditional military–industrial complex is also very much part of public–private interactions in the field of cyber intelligence.[50]

This is perhaps most evident in the private market for zero days, exploits and spyware.[51] The classic example is the tight connection between the Israeli military intelligence's cyber Unit 8200 and the many 'cybersecurity firms' that its alumni have set up.[52] The NSO group, the company behind the notorious Pegasus spyware used by many intelligence and law enforcement agencies, is the best-known example, but many more of these revolving doors between intelligence and 'cyber-intelligence vendors' exist. While they are best documented in the cases of Israel, the US and several European countries, there is no reason to assume that this is not common practice elsewhere.[53] The case of spyware

[49] Damien van Puyvelde (2019), *Outsourcing US intelligence: Contractors and government accountability*. Edinburgh: Edinburgh University Press.

[50] Shane Harris (2014), *@War: The rise of the military-internet complex*. Boston: Houghton Mifflin Harcourt; Nicole Perlroth (2022), *This is how they tell me the world ends: The cyber weapons arms race*. London: Bloomsbury.

[51] That market has many more failings. It is largely unregulated and untransparent, meaning that it is very unclear who vendors are selling to—even when they say they only sell to 'legitimate' agencies and law enforcement—and whether they are selling certain assets exclusively to one customer or reselling many times over. See Perlroth, *This is how they tell me the world ends*; Lillian Ablon, Martin Libicki and Andrea Golay (2014), *Markets for cybercrime tools and stolen data: Hackers' bazaar*, Santa Monica, CA: Rand Corporation.

[52] Neri Zilber (2018), 'Hackers for hire', *Foreign Policy*, 230 (Fall), 60–4.

[53] See for example Winnona DeSombre, Lars Gjesvik and Johann Ole Willers (2021), 'Surveillance technology at the fair: Proliferation of cyber capabilities in international arms markets', Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

like Pegasus lays bare that the dividing line between 'good' and 'bad' intelligence practices or democratic vs autocratic countries is a very thin one. Intelligence agencies in both regime types procure and use such software and largely employ the same methods—making the political goals as well as the real-life consequences for those surveilled the main difference. Journalist Jamal Khashoggi met a horrific end at the hands of Saudi Arabian security services, most likely enabled by the Pegasus software discovered on his fiancée's phone.[54] In short, the real-life consequences of surveillance matter greatly, making the discussion about means and methods much less straightforward. As intent cannot be regulated, policy-makers often focus on tools and behaviours, sidestepping the difficult legal and ethical questions, although, as we discuss below, this approach is changing in some contexts.

Another important intersection between intelligence agencies and private companies is the relationship that intelligence agencies have with many of the companies that own and operate the internet's infrastructure and backbone. The debate around Huawei is a case in point, but China is hardly the first country that intends to make use of the prominence of national companies in international digital and data infrastructure and hardware components for intelligence purposes. The US, and before that the UK, have also used informal relations as well as the ability to legally commandeer access to networks or data from global companies domiciled in their jurisdiction.[55] Access to subsea and terrestrial cable networks, cable landing stations and large cloud providers gives huge possibilities for espionage, as does access to platforms and messaging services.[56] In the US we have seen willing cooperation between government and private companies as well as tugs of war between companies—with a business model and a public image to protect—and law enforcement and intelligence agencies on the issue of access to data.[57] One of the latest clashes (Apple vs the FBI in the San Bernardino case) has resulted in an increase in end-to-end encryption on many messaging services, making interception of the content of messages much harder (even if access to metadata is still possible). There is competition not just between rival intelligence agencies in getting access to information but also—and increasingly—between intelligence agencies trying to secure—and private companies trying to deny—access to the information held on private platforms and networks.

One last public–private connection in the field of cyber intelligence relates to the role that threat intelligence companies play in discovering and analysing cyber (intelligence) operations, elements of which are sometimes used in official public attributions of those

[54] Miles Kenyon (2021), 'A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show', *Washington Post*, 21 December 2021.
[55] Gordon Corera (2015), *Intercept: The secret history of computers and spies*, London: Weidenfeld & Nicolson.
[56] Camino Kavanagh (2023), 'Wading murky waters: Subsea communications cables and responsible state behaviour', UNIDIR, https://www.unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour.
[57] Bert-Jaap Koops and Eleni Kosta (2018), 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"', *Computer Law & Security Review*, 34(4), 890–900.

operations.[58] Indeed, threat intelligence companies play a significant role in tracking, exposing and naming some of the advanced persistent threats (APTs) that have been active in Western countries. In some cases, they have directly attributed such activity to state actors, although that practice is becoming less common. As noted, these reports often form part of the mix of information supporting the attribution of a cyber operation to a state actor.[59] This kind of reporting is valuable and has been given a lot of attention. At the same time, researchers have also highlighted how it is subject to bias, reporting mostly on 'high-end threats to high-profile victims' among their Western clientele and paying scant attention to other societal harms.[60] Such reporting does, nonetheless, shed light on cyber (intelligence) operations that the intelligence agencies involved would rather have kept quiet. And while these companies' reporting focuses mainly on the activities of agencies that are adversarial to the West, there are other groups such as the Bellingcat collective that claim to be more exhaustive in their reporting. [61] Finally, more recently, China for the first time publicly attributed a cyber operation to the US on the basis of a private company's research report, widening the playing field of what so far had largely been a Western affair.[62]

[58]See for example Florian J. Egloff (2020), 'Contested public attributions of cyber incidents and the role of academia', *Contemporary Security Policy*, 41(1), 55–81.

[59] See relevant discussion in N. Tsagourias and M. Farrell (2020), 'Cyber attribution: Technical and legal approaches and challenges', *European Journal of International Law*, 31(3), 941–67.

[60] Lennart Maschmeyer, Ronald J. Deibert and Jon R. Lindsay (2021), 'A tale of two cybers – How threat reporting by cybersecurity firms systematically underrepresents threats to civil society', *Journal of Information Technology & Politics*, 18(1), 1–20.

[61] Eliot Higgins (2021), *We are Bellingcat: An intelligence agency for the people*. London: Bloomsbury.

[62] Eric Zhang and Rogier Creemers (2023), *The evolution of Chinese perspectives on cyber deterrence and attribution*. Leiden: Leiden Asia Centre.

4. The governance and non-governance of cyber intelligence

4.1 Cyber espionage and international law

Main points

- There is no one universal legal regime governing intelligence or espionage.
- Tolerance thresholds for intelligence-led cyber operations remain high, despite the severity of some of the operations that have come to light.
- There are three principal viewpoints regarding espionage and international law that are largely applicable to cyber-espionage operations: espionage is lawful; espionage is not unlawful per se, but its methods may violate international law, particularly sovereignty; and espionage is prohibited under the general rules of international law as a violation of state sovereignty or as unlawful intervention if it involves an element of coercion.
- The secrecy that surrounds intelligence-led operations in cyberspace makes it difficult to discern consistent state practice or *opinio juris* for the formation of customary international law.
- For the first time, the 2021 UNGGE and OEWG reports refer to certain 'covert' activities affecting domestic political processes, such as information operations, election interference and threats to the healthcare sector. Nonetheless, states are unlikely to use the current UN process to directly address intelligence-led operations other than these sporadic references in the reports.
- Some states have called out intelligence-led operations in some public attribution statements, yet these rarely reference the legal rules or principles that have been breached in the operation.
- New developments such as joint intelligence–military structures may also shed light on how states view international law as applying to intelligence-led operations both in peacetime and in conflict.
- Most normative developments relevant to cyber-related intelligence activities are taking place at the national level and tend to be centred on (i) restricting or prohibiting the foreign intelligence activities of other states on one's territory; and (ii) regulating bulk collection and the use of surveillance technology. The latter is often the result of much advocacy, in turn sparked by revelations of the bulk collection and mass surveillance practices of states.
- National cybersecurity strategies provide important frameworks for deterring, and strengthening resilience against, the intelligence-led operations of other states.

> In addition, a growing number of legislative and regulatory tools (procurement, foreign investment screening, export controls etc.) contribute to strengthening resilience against such operations.

There is no one universal legal regime governing intelligence or espionage. Whereas international humanitarian law provides relative clarity on **espionage** conducted in the context of an armed conflict, peacetime espionage remains a thorny subject among scholars, and reportedly 'not well understood in mainstream international law'.[63] Indeed, an early study of the subject held international law to be 'remarkably oblivious to the peacetime practice of espionage', with 'Leading treatises overlook[ing] espionage altogether or contain[ing] a perfunctory paragraph that defines a spy and describes his hapless fate upon capture'.[64] Conversely, today there is a general view that espionage (and the activities that underpin it) is a lawful practice.

In contrast, **covert action**, which refers to unacknowledged or clandestine activities undertaken by states to influence events or pursue specific objectives in other states, exists in a legal grey area under international law. The acceptability of covert action is debated and lacks consensus among states. More specifically, covert actions that violate key principles of international law, such as interference in another state's domestic affairs or support for armed groups to destabilise a government, are generally regarded as unlawful. And while some covert actions may be deemed justifiable under international law if they serve legitimate self-defence or national security interests (e.g. counterterrorism operations), the legality of such actions will be determined by the specific circumstances and methods employed. In terms of state practice and customary international law, the secretive nature of covert operations means that limited information is available, making it difficult to discern consistent state practice or *opinio juris* for the formation of custom.

Returning to espionage, as noted three principal viewpoints regarding espionage can be discerned from the literature: espionage is lawful; espionage is not unlawful per se, but its methods may violate international law, particularly sovereignty; and espionage is prohibited under the general rules of international law as a violation of state sovereignty or as unlawful intervention if it involves an element of coercion.[65]

To date, commentary on **cyber espionage** and international law generally accord with these viewpoints, with most scholars agreeing that while cyber espionage is not

[63] Duncan French (2019), 'Book review: Russell Buchan, *Cyber espionage and international law*', *Leiden Journal of International Law*, 32(4), 883–5.

[64] Roland J. Stranger (ed., 1962), *Essays on espionage and international Law, with a foreword by Richard Falk*. Columbus: Ohio State University Press.

[65] Russell Buchan (2018), *Cyber espionage and international law*. London: Hart Publishing; A.J. Radsan (2007), 'The unresolved equation of espionage and international law', *Michigan Journal of International Law*, 28(595); Patrick C.R. Terry (2015), 'Absolute friends: US espionage against Germany and public international law', *Revue québécoise de droit international*, 28(2), 173–203; Catherine Lotrionte (2014), 'Countering state-sponsored cyber economic espionage under international law', *North Carolina Journal of International Law*, 40(443); Craig Forcese (2016), 'Confronting and adapting: Intelligence agencies and international law', *Virginia Law Review*, 102, 67–84.

prohibited under international law, its methods may violate international law and, more specifically, the principles of sovereignty and non-intervention. Take, for instance, the *Tallinn Manual* (2.0), which refers to cyber espionage as 'any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather information'.[66] According to its Rule 32, peacetime cyber espionage does not per se violate international law, although 'the method by which it is carried out might do so'.[67] The method may of itself render the espionage operation unlawful or cyber espionage may be just one component of a broader operation that violates international law.[68]

As argued at the research seminar in Valencia, since the practice of cyber espionage is covert, it does not conform with the conclusions of the International Law Committee (ILC) on the formation of customary international law, i.e. the element of contestation and eventual normative crystallisation does not exist. Regarding *opinio juris,* the policy of silence around cyber espionage and states' high tolerance thresholds for the practice mean that when intelligence-led cyber operations are called out, limited reference, if any, is made to the legal rules or principles that have been violated.

While most cyber-espionage operations do not fulfil the 'element of coercion' criterion (i.e. a violation of state sovereignty or unlawful intervention), some scholars are of the view that some economic espionage operations involve elements of **non-forcible** coercion, assessing them against the non-intervention prohibition.[69] This is particularly the case where state-sponsored economic espionage is concerned.[70] Other scholars have, however, critiqued the continued narrow focus on such non-forcible coercive cyber-intelligence operations, contrasting it with the limited focus on **forcible** coercive influence. The latter would include covert action such as that aimed at influencing internal political processes, public opinion and national security more generally.[71] States, including the permanent members of the UN Security Council, would likely be reluctant to entertain an open discussion on the international law applicable to such operations, especially in the current environment. Nonetheless, references in the 2021 UNGGE and OEWG reports respectively to 'ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State' and to 'malicious ICT activities against critical infrastructure and critical information infrastructure that undermine trust and confidence in political and electoral processes' may represent a shift in the treatment of such operations at the international level.[72] To date, though, there has been no meaningful follow-up discussion on the measures—legal or otherwise—that states should put in place to respond to such threats, despite their agreement that they

[66] Schmitt, *Tallinn Manual 2.0*.
[67] Ibid.
[68] Ibid., Rule 32, paras 6 and 9.
[69] Lotrionte, 'Countering state-sponsored cyber economic espionage under international law'; Zhixiong Huang and Kubo Mačák (2017), cited in Moynihan, 'The application of international law to state cyberattacks'.
[70] Lotrionte, 'Countering state-sponsored cyber economic espionage under international law'.
[71] French, 'Book review'.
[72] GGE report 2021; OEWG report 2021.

'undermine trust, are potentially escalatory and can threaten international peace and security, as well as pose direct and indirect harm to individuals'.[73]

It may be possible that over time, the growing practice of publishing and exchanging national views on how international law applies to state behaviour in cyberspace will help clarify how some of these operations may violate international law. For now, however, beyond France's earlier mention that cyber-espionage, while not illegal in international law (…) may infringe such law when linked with an internationally wrongful act", [74] states have largely side-stepped the discussion.[75]

Transparency around new developments such as the setting up of joint intelligence–military structures—and commitments to ensuring that the activities of such structures are conducted 'responsibly'— can shed light on how states view international law as applying to cyber espionage and covert operations both in peacetime and in conflict and propel other states to develop their own views. There is likely an expectation that transparency around such structures and the principles guiding their rules of engagement can also serve as a deterrent. We suggest that it is important to also consider whether such acts of transparency are driving reciprocity in the development of capabilities and behaviours by other states, and related response implications.

Finally, exchanges on efforts at national level to put in place relevant legislation and oversight and accountability mechanisms, as per the thrust of some of the norms and confidence-building recommendations outlined in the UN GGE and OEWG reports, can shed light on the actions that states are taking both to advance their own cyber-intelligence posture and capabilities and to protect against those of others. It is worth highlighting some of these developments.

4.2 Domestic law and oversight

Main points

> Most normative developments relevant to cyber intelligence and espionage are emerging at the national level. This is particularly the case with legislation on foreign intelligence, bulk collection and the use of surveillance technology. These are all ex-post legislative/regulatory actions, and generally only come into being after breaches, leaks of such activity and significant public pressure. In some contexts, they may be put in place simply to legitimise existing practice.

[73] GGE report 2021.
[74] 'International Law Applied to Operations in Cyberspace', Ministère des Armées, France (2019).
[75] 'International Law Applied to Operations in Cyberspace', paper shared by France with the Open-ended working group established by resolution 75/240 (2021), based on the 2019 document prepared by the Ministry of the Armed Forces.

- The scope of intelligence-led cyber operations is expanding alongside the number of public and private actors involved in espionage activities.
- The scope of what are considered to be prohibited foreign intelligence activities in national counter-intelligence legislation is also expanding in some contexts.
- In addition to national legislation, other policy and regulatory levers such as foreign investment screening are being leveraged for counter-intelligence and espionage.
- New precedents are being set through the establishment of joint defence/intelligence structures. While their operations will reportedly be conducted in strict adherence to international law and guided by well-established principles such as accountability, it is unclear what this means in practice, whether like-minded countries will do the same and whether it will be met with reciprocal action by non-like-minded states.
- Efforts to regulate mass surveillance/bulk collection in line with key principles of international law are advancing. It is too soon to assess their impact and it is unclear whether they will have a longer-term deterrent effect.
- New measures are being taken (or recommended) in the US and EU to curb the sale and use of surveillance technology. It is too soon to assess their impact and it is unclear whether they will have a longer-term deterrent effect.
- There are reports that US intelligence agencies and law enforcement regularly purchase people's personal data from commercial companies, in lieu of seeking a warrant. Efforts are under way in the form of a bipartisan bill to curb this practice. It is unlikely to pass.

Intelligence and espionage are characterised by an interesting combination of two legal regimes at the domestic level. Some countries have domestic legislation that provides a legal basis for foreign intelligence, espionage and surveillance for their own agencies.[76] At the same time, almost all states have domestic legislation that criminalises the activities of foreign intelligence agencies of other states operating on their territory. In other words, at the domestic level, while states provide legal cover for the work of their own intelligence agencies abroad, they prohibit foreign intelligence agencies from doing the same on their own territory. In some countries, foreign espionage is even a capital offence.

In terms of regulation and oversight of intelligence activities, the differences between countries are vast. There is a growing acceptance among experts that effective oversight

[76] For instance, regarding domestic surveillance, according to the UN Special Rapporteur for Privacy reporting to the Council of Europe in 2018, more than 80 per cent of UN member states do not have a law that protects privacy by adequately and comprehensively regulating the use of domestic surveillance. More recently, the EU Fundamental Rights Agency reported that only five out of 27 EU member states have detailed provisions on general surveillance of communications (bulk surveillance). Of these five, only three provide for binding involvement of an independent body in the authorisation of measures. Presentation by Joseph A. Cannataci, UN Special Rapporteur for Privacy, ICDPPC, Brussels, 2018. For further context, see *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update*, EU Agency for Fundamental Rights, 23 October 2017, p. 9.

and public trust are vital to the operations of intelligence agencies, including when operating through cyberspace. In this regard, 'effective' oversight requires going beyond mere gestural compliance with principles and standards to establish independent bodies with actual access and the necessary technical tools to conduct their work. This, however, is challenging.

In some countries, parliamentary oversight has existed for decades (e.g. the Netherlands and the US). In line with recent calls for transparency and accountability, many countries have only recently started to formally publish legislation that outlines how their intelligence agencies are regulated. For example, in the UK formal acts regulating British security and intelligence agencies were only introduced in 1989 and 1994 respectively,[77] and in the Netherlands the first act regulating domestic and foreign intelligence was passed in 1987.[78] Prior to this, even if certain activities were regulated it was only by secret statute and with limited public scrutiny, other than in the wake of public scandals.

The recent publication by the UK government entitled 'The National Cyber Force: Responsible Cyber Power in Practice' is worthy of note.[79] Lauded by some for its pivot away from a doctrine of strategic deterrence to one of 'cognitive effects', it highlights the key role of intelligence agencies and covert action in 'weakening the ability of the enemy to plan and conduct hostile operations'.[80] Moreover, it purports to operate in 'strict adherence to robust legal and ethical frameworks, including relevant international law', and 'in an accountable and legitimate manner'.[81] This has created some confusion as to what constitutes a robust framework, especially since little detail and context is provided, including with regard to how the relevant operations relate to the UK government's previous public statements on international law, and especially where the interpretation of sovereignty is concerned. As noted by one scholar, if the document triggers similar statements from other states, 'a comparison with states advancing stricter definitions of international law in cyberspace [could help to] put the UK's approach to offensive cyber operations in context'.[82] Others have criticised the document for being heavy on transparency (yes, we deploy all kinds of offensive operations) and principles (yes, we are guided by key principles), but light on detail in terms of which principles and on implementation and domestic accountability. This is particularly notable where 'oversight and authorisation of NCF activity as it operates against foreign state and non-state threats' is concerned. Key issues to look out for moving forward include how the oversight role of the parliament's Intelligence and Security Committee and the 'joint

[77] Omand and Phythian, *Principled spying*, 75.
[78] Willemijn Aerdts (2023), *Diensten met geheimen. Hoe de AIVD en MIVD Nederland veilig houden*. Amsterdam: Ambo-Anthos.
[79] UK National Cyber Force, 'Responsible cyber power in practice'.
[80] Rory Cormac, 'The historical roots of the "doctrine of cognitive effects"', in Stevens et al., 'Evaluating the UK National Cyber Force's "Responsible cyber power in practice"'.
[81] Pia Hüsch, 'The international legal framework of the NCF's cyber operation', in Stevens et al., 'Evaluating the UK National Cyber Force's "Responsible cyber power in practice"'.
[82] Ibid.

accountability' feature involving both the foreign and defence secretaries will play out in practice, especially given persisting challenges bedevilling the oversight body.[83]

4.2.1 Regulating foreign espionage

In many instances countries are updating their laws regarding the actions of foreign intelligence organisations and agents on their territory. As noted, however, this approach is not generally accompanied by measures that restrain the activities of their own intelligence agencies when operating abroad. In some instances, these legislative updates may be reciprocal, reflecting a response to the transparency measures of other states on their intent to deploy cyber operations as a means of deterrence.[84]

China, for one, recently expanded the scope of its already expansive anti-espionage law to explicitly include covert action. It broadened the scope of what constitutes acts of espionage to include not just the activities of espionage organisations and agents, but also those 'carried out, instigated or funded by foreign institutions, organizations and individuals other than espionage organizations and their representatives, or in which domestic institutions, organizations or individuals collude to steal, pry into, purchase or illegally provide state secrets, intelligence and other documents, data, materials or items related to national security and interests'.[85] The expanded law also defines acts of espionage as 'network attacks, intrusions, obstructions, control or disruptions targeting state organs, units involved with secrets, or critical information infrastructure'.[86] These developments, which clearly cover both espionage and covert action, have given rise to much consternation, including among both foreign and Chinese researchers and businesses who are concerned that such a broad-brush approach to foreign espionage activities would place them at risk. This concern is compounded by the fact that the law allows Chinese authorities to impose exit bans on anyone under investigation, if deemed a national security risk once they leave the country.[87]

In addition to specific anti-espionage legislation, some countries are using other policy, legislative and regulatory levers such as foreign investment screening to protect against the threat of foreign espionage, including when digital hardware and networks can be leveraged for such purposes or when they are conducted via cyber means. The related storms (or rather tornadoes) that gathered around Huawei and 5G are a case in point. More recently, espionage risks (both traditional and cyber-related) are influencing

[83] On such challenges, see for example Andrew Defty (2019), 'Coming in from the cold: Bringing the Intelligence and Security Committee into parliament', *Intelligence and National Security*, 34(1), 22–37.
[84] See Fischerkeller et al., *Cyber persistence theory* . See also Ryan Tate (2022), 'Transparent cyber deterrence', *Joint Force Quarterly*, 107, October.
[85]'Counter-espionage law of the P.R.C.' (2023 edn), *China Law Translate*, https://www.chinalawtranslate.com/en/counter-espionage-law-2023/.
[86] Ibid.
[87] Nadya Yeh (2023), 'Should you be frightened by China's revision to the anti-espionage law?', *The China Project*, https://thechinaproject.com/2023/05/02/should-you-be-frightened-by-chinas-revision-to-the-anti-espionage-law/.

decision-making processes relevant to ensuring or denying access to critical elements of the ICT ecosystem such as subsea cable infrastructure and components, which are highly vulnerable to espionage. This is evidenced, for instance, in decisions taken by the US Federal Communications Commission (FCC) to deny subsea cable licences when a system aims to directly connect the US with certain jurisdictions (e.g. China, Hong Kong, Russia, Cuba) due to the direct and indirect counter-intelligence threats that such connections pose to the US.[88] Other countries have taken or are considering similar measures, including in response to revelations or concerns of similar activity conducted by US and UK signals intelligence agencies.[89]

4.2.2 Mass surveillance/bulk collection

Domestic legislation relevant to intelligence and cyber espionage has advanced most where curbing the mass surveillance/bulk collection practices of states is concerned. The practice came under public scrutiny in 2013 due to data protection, privacy and other rights-related concerns provoked by the Snowden leaks and the role played by signals-intelligence agencies such as the NSA and GCHQ, reports of which continue to emerge. Such practices fuelled much debate and have led to legislative and regulatory reforms in many countries, including Germany, France, the Netherlands, Norway, the UK and the US, as well as more transparency in the legislative processes themselves.[90] In some cases, such processes have been critiqued for simply legalising existing surveillance practices—whitewashing them, so to speak — so as to provide a 'wrapper of democratic accountability and safeguarding' to practices that in many instances really only came to light through disclosures or the relevant legislative processes.[91] As noted by some experts, though, in many cases the situation is much more nuanced, as well as more complex. Recent developments in Germany provide an example of the many good and bad aspects and the missed opportunities of such reforms.[92] In other cases, the jury is still out on whether surveillance powers can be curtailed, the ongoing discussion in the

[88] Kavanagh, 'Wading murky waters'. The DoJ statement on the US–Cuba connection provides a good insight into concerns of the US government, contradictory as they may be. It notes that directly connecting such a cable, whereby a Cuban state-owned company would have exclusive use of the cable, control over its Cuban landing station and remote access to traffic on it, could advance the Cuban government's intelligence objectives by giving direct access to US persons' communications and sensitive data traversing the cable. Concerns regarding the rerouting of traffic other than that flowing between Cuba and the US were also raised.

[89] Kavanagh, 'Wading murky waters'. See discussion on 'reactive routing' decisions, p. 23.

[90] D. Broeders, S. Boeke and I. Georgieva (2019), 'Foreign intelligence in the digital age: Navigating a state of "unpeace"', The Hague Program for Cyber Norms Policy Brief, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3493612.

[91] Natasha Lomas (2022), 'OECD adopts declaration on trusted government access to private sector data', *Tech Crunch*, 15 December. See also Ilina Georgieva (2020), 'The power of norms meets normative power: On the international cyber norm of bulk collection, the normative power of intelligence agencies and how they meet', in Dennis Broeders and Bibi van den Berg (eds), *Governing cyberspace: Behavior, power, and diplomacy*, 227–42. Lanham, MD: Rowman and Littlefield.

[92] Kilian Vieth-Ditlmann and Thorsten Wetzling (2021), 'Caught in the act? An analysis of Germany's new SigInt Reform', *Stiftung Neue Verantwortung* Human Rights, Big Data and Technology Project, https://www.stiftung-nv.de/de/publikation/caught-act-analysis-germanys-new-sigint-reform.

US on the future of US surveillance powers under Section 702 of the Foreign Intelligence Surveillance Act (FISA) being a case in point.[93]

Where surveillance technology is concerned, in many countries tensions remain between public sentiment about government use of spyware on the one hand, and what intelligence agencies and their overseers view as necessary and part of 'normal' international relations on the other.[94] The fact that intelligence agencies of supposedly democratic countries continue to buy and use the same products as regimes that are considered autocratic does not help.[95] Despite renewed efforts to tame these secret markets, challenges remain, including with regard to determining the targets of these efforts. For instance, in 2021 the US placed the NSO group on a Department of Commerce blacklist for 'engaging in activities that are contrary to [its] national security or foreign policy interests'.[96] That measure was evidently found wanting, as since then, the White House has issued an executive order prohibiting the use by the US government of commercial spyware that poses risks to national security. [97] Despite these measures, some government agencies still seem to be procuring spyware from blocked vendors.[98]

The EU, too, has sought to regulate or even ban spyware and spyware companies, but vendors make use of national differences in the implementation of export controls to establish themselves in the EU. Reports of European intelligence and law enforcement agencies using their products continue to make the news.[99] Aware of the threats associated with such practices, in 2022 the European Parliament established a Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Spyware (PEGA). Its report confirms that spyware has been used in the EU context 'to monitor, intimidate and discredit opponents, journalists and civil society', calling out 'systemic issues in Poland and Hungary' and raising 'concerns over its use in Greece and Spain'.[100] The report calls for illicit spyware practices 'to cease immediately', recommending stronger regulation to prevent abuse, including EU rules on its use by law enforcement, a common legal definition of the use of national security as grounds for surveillance, strengthened intelligence cooperation, oversight cooperation and common standards. It also calls for the establishment of a dedicated independent research institute—an EU Tech Lab—with powers to investigate surveillance and provide legal, technological and forensics support,

[93] *New York Times*, 'What to know about Section 702, the post-9/11 surveillance law', 27 February 2023.
[94] Devanny et al., 'On the strategic consequences of digital espionage'.
[95] The work of groups such as Citizen Lab has been key to shedding light on some of these practices. See: Citizen Lab Research, https://citizenlab.ca/category/research/
[96] 'Commerce adds NSO Group and other foreign companies to entity list for malicious cyber activities', United States Department of Commerce, 3 November 2021.
[97] 'Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security', Washington, DC: The White House, 27 March 2023.
[98] 'Opinion: The White House's new executive order on spyware is needed', *Washington Post*, 8 April 2023.
[99] Steven Feldstein and Brian (Chun Hey) Kot, 'Why does the global spyware industry continue to thrive? Trends, explanations, and responses', Carnegie Endowment for International Peace, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.
[100] European Parliament, 'Spyware: MEPs sound alarm on threat to democracy and demand reforms', 8 May 2023.

and for 'new laws to regulate the discovery, sharing, resolution and exploitation of vulnerabilities'.[101]

Other challenges exist, such as the use of commercial data sets. For instance, in the US, where there has been limited progress on comprehensive privacy reform, a declassified report by the Office of the Director of National Intelligence recently revealed that intelligence and law enforcement agencies have been purchasing troves of data on Americans from commercial data brokers.[102] This is reportedly 'the same type' of information that the US Supreme Court sought to shield against warrantless searches and seizures.[103] While acknowledging the intelligence value of commercially available information (CAI), the report raises concerns about privacy and civil liberties, particularly since 'it is less strictly regulated than other forms of information acquired by the [intelligence community]'. The panel established to study the problem made several recommendations, including the establishment of a multi-layered process through which the intelligence community can catalogue, as feasible, the CAI it requires. They also include developing a set of standards and procedures for CAI; governing and requiring regular re-evaluation of acquisition and use decisions, including as to the use of CAI; and as part of the latter or complementary to it, developing more precise guidance to identify and protect sensitive CAI that implicates privacy and civil liberties concerns.[104]

Following publication of the report, a bipartisan proposal was submitted to amend a defence bill—the National Defense Authorization Act (NDAA), currently under scrutiny in the House of Representatives. The aim of the amendment is to abolish the government practice of buying information on Americans that is otherwise attainable only with a warrant. Critics suggest that it is unlikely that the amendment will pass, as it is in practice 'implausible' since the CAI would still be available for purchase to non-US entities, and because it would render the NDAA process 'controversial'.[105] Others are more balanced, noting that even if the amendment is not included in the NDAA, a discussion on American citizens' data privacy will eventually have to happen.[106] Meanwhile in Europe, similar issues relevant to commercially and publicly available information have arisen. Current practices are non-compelled, in that the entity providing the intelligence service with access to the data is not obliged by law to do so; this distinguishes the practices from

[101] Ibid.

[102] Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information, 'Report to the Director of National Intelligence, January 2022 (approved for release June 2023)', https://www.congress.gov/118/meeting/house/116192/documents/HHRG-118-JU00-20230712-SD011.pdf. For additional background, see Anne Toomey McKenna (2023), 'Why US agencies buy personal info and what it means in the age of AI', *Military Times*, https://www.militarytimes.com/opinion/2023/06/29/why-us-agencies-buy-personal-info-and-what-it-means-in-the-age-of-ai/.

[103] Dell Cameron (2023), 'US spies are buying Americans' private data. Congress has a new chance to stop it', *Wired*, https://www.wired.com/story/ndaa-2023-davidson-jacobs-fourth-amendment/?utm_source=pocket_saves.

[104] ODNI Senior Advisory Group Panel on Commercially Available Information, 'Report to the Director of National Intelligence, January 2022 (approved for release June 2023)'.

[105] See CyberLawPodcast, Episode 467 (00:43:40), https://www.lawfaremedia.org/article/the-cyberlaw-podcast-district-judge-s-injunction-sets-off-fireworks.

[106] Ibid.

data acquired by other means for which there are legal restrictions and robust authorisation and oversight procedures.[107] Experts suggest that this is likely the region's next frontier for intelligence reform.[108] It is also likely that new technological developments such as large language models and generative artificial intelligence, which some analysts suggest are poised to 'revolutionise intelligence and risks analysis', will exacerbate some of these existing challenges and introduce new ones.[109]

Regional or specialised bodies are also influencing how oversight and accountability for cyber intelligence/espionage is considered at the national level. For instance, the Court of Justice of the European Union (CJEU) and the European Court of Human Rights have played an important oversight and accountability role where the mass surveillance/ bulk collection practices of states are concerned, leading to the codification of core criteria such as necessity and proportionality in member states' national laws.[110] Nonetheless, differences in levels of legal protections for data privacy and discrepancies between how citizens and foreigners are treated under the surveillance regimes of different jurisdictions pose challenges.

For its part, the OECD has managed to broaden a decades-long discussion on privacy and transborder flows of personal data stemming from bulk collection issues.[111] Adopted by some 38 OECD countries and the EU, its 'Declaration on Government Access to Private Sector Data' proposes seven principles (legal basis, legitimate aims, approvals, data handling, transparency, oversight and redress), which purportedly reflect 'commonalities' drawn from the existing laws and practices of signatory states, and aim to 'increase[e] clarity about how government [law enforcement and security] agencies can access data'.[112] The impact of this non-binding Declaration is evidently still unclear and is also contingent on the outcome of other negotiations on cross-border data flows such as the EU–US Data Privacy Framework (DPF). Regarding the latter, recently a US executive order committing to an overhaul of foreign intelligence agencies' access to personal data and creation of a new redress system for EU citizens cleared the path for the DPF negotiations to be concluded.[113] This executive order imposes necessity and proportionality limits on

[107] See Thorsten Wetzling and Charlotte Dietrich (2022), *Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?*', Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/snv_commercially_available_data.pdf.pdf.

[108] Ibid.

[109] Rafal Rohozinski (2023), 'AI is poised to revolutionize intelligence and risk analysis', Centre for International Governance Innovation (CIGI), https://www.cigionline.org/articles/ai-is-poised-to-revolutionize-intelligence-and-risk-analysis/.

[110] E. Kosta (2017), 'Surveilling masses and unveiling human rights—Uneasy choices for the Strasbourg Court', inaugural address. Tilburg Law School Research Paper, https://ssrn.com/abstract=3167723

[111] Lomas, 'OECD adopts declaration on trusted government access to private sector data'. The prior data flows arrangement between the EU and the US—Privacy Shield—was invalidated by the CJEU in 2020 due to protections that were deemed 'not up the required legal standard of "essential equivalence" with EU law'. See CJEU Press Release, 'The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield', 16 July 2020, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[112] OECD (2023), 'Declaration on government access to personal data held by private sector entities', https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487.

[113] 'Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework', Washington, DC: The White House, 22 October 2022.

signal intelligence activities, first by mandating them explicitly, then by explaining the mandate and finally by prescribing oversight mechanisms to verify that intelligence agencies are following the rules.[114] Although political agreement on the new DPF was reached in 2023, it had taken more than a year of negotiations to flesh out the details of the DPF agreement to ensure that the solutions agreed 'specifically address the requirements set by the [European] court as regards the need for limitations and safeguards for access to data by U.S. intelligence agencies in line with the principles of necessity and proportionality and the need to ensure effective redress for EU individuals'. Critics continue to argue, however, that the agreed Framework 'still paper[s] over the same fundamental legal conflict between EU privacy rights and U.S. surveillance powers', noting that it potentially faces 'the same assessment of inadequacy once EU judges get to scrutinize the detail'.[115]

[114] However, many analysts suspect that the Biden Executive Order will not solve the adequacy problem in the long run and expect that there will be a Schrems III court case before the ECJ that will result in striking down of the EU–US DPF. See for example William Alan Reinsch (2022), 'Privacy—Heading for Schrems III?', CSIS, https://www.csis.org/analysis/privacy-heading-schrems-iii.
[115] Ibid. See also Natasha Lomas, 'Europe adopts US data adequacy decision', *TechCrunch*, 10 July 2023.

5. An opportunity for discussing intelligence-led cyber operations in diplomacy?

The use of ICTs by states continues to be a focus of discussions and negotiations at the international level, many of them pertaining to international law and norms applicable to certain behaviours. While these processes do not specifically focus on intelligence activities, they are nonetheless relevant. At the UN, they include work under way within the UN First Committee on International Security and Disarmament, the OEWG on ICTs and international security, and the different GGEs that came before it. It also includes work taking place within specialised bodies such as the Human Rights Council or instruments such as the UN Special Rapporteurs. Beyond the UN, regional groupings such as the EU or specialised bodies such as the OECD also deal with issues of relevance.

In most instances, intelligence operations involving elements of coercion are not being addressed in international fora, despite being the main type of below-the-threshold cyber-activity that states continue to engage in, alongside collection and counter-intelligence. The 2021 UNGGE and OEWG ventured into an initial discussion on some such operations. By discussing information operations, election interference, threats to the healthcare sector and automated cyberattacks, the delegates indirectly touched on the activities of intelligence agencies in cyberspace. It is however unlikely that a meaningful discussion on the measures applicable to such operations will happen in the current process.

In response to revelations of—or growing concerns about—cyber-intelligence activity, some actions are being taken at national level. In some instances, these actions are framing thinking on how new structures should operate (responsible cyber power), on where stronger regulation is required (mass surveillance/bulk collection, the sale and use of commercial surveillance technology), and on what is acceptable behaviour by other countries on one's own territory (foreign intelligence).

Given the increasing role that intelligence and cyber-espionage operations play in statecraft, we argue that it is time for a more structured conversation among policy-makers and diplomats within and between countries not just on the rules and principles that govern cyber-intelligence activities, but also on how emerging technologies such as artificial intelligence will impact the field. We suggest that informal formats such as Track 1.5 and Track 2 dialogues can play an important role in advancing these and other such discussions.[116] The latter could include initial exchanges between like-minded countries on:

- Terminology, demarcations and threats;
- how international law and the framework for responsible state behaviour apply to intelligence-led cyber operations, based on specific case studies;
- the rules and principles governing the operations of joint intelligence–military cyber-force structures such as the UK National Cyber Force in peacetime and in conflict, and reciprocal behaviour-and norm-shaping implications;
- relationship between the rule of law, intelligence contests and strategic stability
- tensions, trade-offs and reciprocity in foreign intelligence legislation;
- the technical, policy and legal implications of LLMs and generative AI for intelligence in general, and cyber espionage in particular.

[116] On this topic and examples of other such track dialogues and their value, see Camino Kavanagh, Madeline Carr and Nils Berglund (2021) *Quiet Conversations: Observations from a decade of practice in cyber-related track 1.5 and track 2 diplomacy*, EU Institute for Security Studies. Digital Dialogue Series. November 2021, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/Nh3fdYmX/quiet-conversations-16-11-21.pdf

About the authors

Dennis Broeders is Full Professor of Global Security and Technology at the Instituteof Security and Global Affairs (ISGA) of Leiden University, the Netherlands. He is the Senior Fellow of The Hague Program on International Cyber Security and project coordinator at the EU Cyber Direct Program. His research and teaching broadly focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance. He is the author of the book The public Core of the Internet (2015). He served as a member of the Dutch delegation to the UN Group of Governmental Experts on international information security and the Open Ended Working Group (2019-2021) as an academic advisor. Before joining Leiden University he was professor of Technology and Society at Erasmus University Rotterdam and senior researcher and project coordinator at the Netherlands Scientific Council for Government Policy, a think tank within the Dutch Prime Minister's office.

Dr. Camino Kavanagh is a visiting Senior Fellow with the Dept. of War Studies, King's College London and non-resident scholar with the Carnegie Endowment for International Peace. Her current research focuses on international politics, conflict and technology as well as emerging issues relevant to critical subsea infrastructure. She frequently lectures on these same topics.

Amongst others, Camino is currently a Senior Digital Advisor to the UN Department of Political Affairs' Policy and Mediation Division. She served as advisor/rapporteur to the 2019-2021 and the 2016-2017 UN negotiating processes (UNGGE and UNOEWG) on cyber/ICT and international security. Over the past decade she has also advised and consulted with the UN Secretary-General's office, the UN Office of Disarmament Affairs (UNODA), the UN Institute for Disarmament Research (UNIDIR), the OSCE, the OAS as well as government departments and agencies on issues pertaining to digital technologies and national/international security, conflict and diplomacy. She participates in a number track 1.5 and track 2 initiatives on these same issues.

Prior to this, Camino spent over a decade working in conflict and post-conflict contexts, including with UN peacekeeping operations and political missions.

About EU Cyber Direct

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