2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations

Barrie Sander
Postdoctoral Fellow
School of International Relations
Fundação Getulio Vargas (FGV)
São Paulo, Brazil
barrie.sander@graduateinstitute.ch

Abstract: In an age of cyber insecurity, anxieties about the silence of States concerning the applicability of international law to peacetime cyber operations have been growing. Concerns have focused on the reluctance of States to agree cyber-specific multilateral treaties and to publicly clarify the customary international rules applicable to hostile cyber operations. Taking these concerns as its point of departure, this paper argues for greater specificity in evaluating the silence of States in the cyber context by distinguishing between three distinct types of peacetime security threats: cyber attacks, cyber espionage, and cyber information operations. Cyber attacks and cyber espionage are technical security threats which involve breaking into and targeting information and communications technologies. The primary distinction between the two is in the nature of the payload to be executed; while a cyber attack's payload is destructive, a cyber espionage payload acquires information non-destructively. Cyber information operations are content-based security threats which involve harnessing the power of online information to cognitively target human intelligence. Relying on this typology, this paper highlights how State silences concerning the application of international law to peacetime cyber operations are not uniform, but vary in terms of their targets, scope and rationale depending on the particular security threat under examination. It is suggested that these variations not only reveal an important dimension of the politics of international law, but are also salient to how the silence of States in different cyber contexts may be evaluated. Contrary to the tendency to

automatically cast State silences in a negative light, this paper reveals that silences can perform different and sometimes constructive functions that are yet to be fully acknowledged or appreciated.

Keywords: *State silence, peacetime cyber operations, international law, cyber attacks, cyber espionage, cyber information operations*

1. INTRODUCTION

In an age of cyber insecurity, international lawyers have been grappling with the challenge of identifying the extent to which international law applies to cyber operations.[1] The engagement of international lawyers with this question has evolved over time. Following the notorious cyber attack on Estonia in 2007, international lawyers were initially preoccupied by the prospect of cyber war – a concern reflected in the narrow focus of the first edition of the *Tallinn Manual*, which fastened its gaze on the law governing the use of force (*jus ad bellum*) and the law of armed conflict (*jus in bello*).[2] Over the course of the past decade, however, it has become increasingly apparent that the vast majority of hostile cyber operations neither cross the threshold required to constitute a prohibited use of force nor occur in the context of existing armed conflicts. In line with this realisation, the focus of international lawyers has gradually shifted towards a concern for interpreting the international legal rules applicable to so-called "below the threshold" peacetime cyber operations – an interest reflected in the expanded mandate of the second edition of the *Tallinn Manual*.[3]

Yet, for all the interpretive efforts of international lawyers, recent years have also witnessed growing concerns about the silence of States concerning the applicability of

* The author would like to thank Duncan Hollis, Russell Buchan, Kubo Mačák, Asaf Lubin, and the anonymous reviewers for their comments on earlier drafts of this paper. The author would also like to acknowledge the funding of Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), which enabled this research to be conducted. All errors remain the author's own.

1 Barrie Sander, 'Cyber Insecurity and the Politics of International Law', *ESIL Reflections* (2017).

2 *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013).

3 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP, 2017) (*'Tallinn Manual 2.0'*). On the shift of focus to peacetime cyber operations, see generally, Kubo Mačák, 'From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law', in Henry Rõigas et al. (eds), *Defending the Core* (NATO CCD COE, 2017) 135.

international law to peacetime cyber operations.[4] According to conventional wisdom, this silence has manifested itself in a number of forms.

First, States have appeared resistant to agreeing cyber-specific multilateral treaties, a trend exemplified by the struggle of Microsoft to garner widespread support for its proposed Digital Geneva Convention. *Second*, States have been reluctant to publicly clarify the customary international rules applicable to peacetime cyber operations, a trend recently characterised by Dan Efrony and Yuval Shany as amounting to "a policy of silence and ambiguity" that is designed to preserve high levels of operational flexibility within the cyber domain.[5] This "wait and see" approach to cyber regulation recently came to the fore in the latest round of talks within the UN Group of Governmental Experts (GGE), which failed to agree a consensus report on the voluntary and binding norms applicable to cyber operations.[6] While recent developments – including the Paris Call for Trust and Security in Cyberspace[7] and the adoption of two resolutions by the UN General Assembly's first committee establishing an open-ended working group on cyber norms and a new UN GGE[8] – have demonstrated a willingness to continue the conversation, it remains to be seen how far States are able to achieve consensus beyond vague assertions about the applicability of international law to cyber operations.[9]

4 See, for example, Brian J. Egan, 'International Law and Stability in Cyberspace', (2017) 35 *Berkeley Journal of International Law* 169, 172 ("States' relative silence could lead to unpredictability in the cyber realm"); Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers', (2017) 30 *Leiden Journal of International Law* 877 , 888 ("faced with states' silence, non-state actors have moved into the vacated norm-creating territory previously occupied exclusively by states"); and Dan Efrony and Yuval Shany, 'A Rule Book on The Shelf? *Tallinn Manual 2.0* on Cyber Operations and Subsequent State Practice', (2018) 112 *American Journal of International Law* 583, 648 (arguing that "a significant normative gap exists in relation to the regulation of interstate cyberoperations" because of "the combination of silence and ambiguity in state practice and their reluctance to articulate their official policy in cyberspace"). See, however, Nicholas Tsagourias, 'The Slow Process of Normativizing Cyberspace', (2019) 113 *AJIL Unbound* 71, 73-74 (arguing that the slow pace by which States are "translating overbroad principles of international law into rules and practice and […] translating practice into rules and principles […] is not peculiar to cyberspace" and, as such, "there is no reason to despair").

5 Efrony and Shany, *supra* n.4, 588. See also Fleur Johns, 'War Without Words', (2019) 113 *AJIL Unbound* 67, 68 (observing how, according to Efrony and Shany, "[l]aw flows from language and its advance stalls in the quiet" and "international law's capacity to curtail or condition the exercise of military power, economic might, and tangible or intangible violence in the cyber domain is presumed to depend upon its capacity to saturate the vocabularies of those with means to deploy such power and to do so in visible, recordable ways").

6 'Dispute along cold war lines led to collapse of UN cyberwarfare talks', *The Guardian*, 23 August 2017.

7 Arthur P.B. Laudrain, 'Avoiding a World War Web: The Paris Call for Trust and Security in Cyberspace', *Lawfare*, 4 December 2018.

8 Alex Grigsby, 'The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased', *Council on Foreign Relations*, 15 November 2018.

9 The applicability of international law to cyber operations was famously confirmed by the UN GGE in its 2013 consensus report. A degree of progress was made in the UN GGE's 2015 report, which began to articulate binding international legal norms applicable in cyberspace. See generally, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', U.N.Doc. A/68/98, 24 June 2013; and 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', U.N.Doc. A/70/174, 22 July 2015 ('UN GGE 2015 Report').

Beyond the reluctance of States to engage meaningfully in the construction and clarification of the international legal rules applicable to cyber operations, a *third* development has been the growing tendency of States to embrace the language of non-binding voluntary norms to articulate responsible behaviour in cyberspace. This trend has been particularly visible in the work of the UN GGE, whose 2015 report recommended 11 norms for consideration by States.[10] According to Kubo Mačák, the emergence of a parallel track to develop voluntary norms of responsible State behaviour in cyberspace signifies "a trend of moving away from the creation of legal rules of international law in the classical sense".[11] *Finally*, the silence of States concerning international law in the cyber context has also been visible in their growing tendency to publicly attribute hostile cyber operations to other States without making reference to applicable international legal rules. In other words, while States have proven increasingly open to naming the involvement of other States in hostile cyber operations, they have often studiously avoided shaming them through recourse to the language of international law.[12]

While this account of the relationship between States, international law and peacetime cyber operations is not inaccurate, it is nonetheless incomplete. Taking this account as its point of departure, this paper argues for greater specificity in examining the silences of States concerning the relationship between international law and peacetime cyber operations. To this end, this paper distinguishes between *three distinct types of peacetime security threats* that have arisen in the cyber domain: cyber attacks, cyber espionage, and cyber information operations. *Cyber attacks* and *cyber espionage* are technical security threats which involve breaking into and targeting information and communications technologies. The primary distinction between the two is in the nature of the payload to be executed: while a cyber attack's payload is destructive, a cyber espionage payload acquires information non-destructively.[13] In contrast to these technical security threats, *cyber information operations* are content-based security threats which involve harnessing the power of online information to cognitively target human intelligence.[14] Although, in practice, a particular cyber operation may encompass more than one type of security threat, this typology offers a useful lens for examining the silences of States within the cyber domain.

10 UN GGE 2015 Report, supra n.9, para. 13. For commentary, see Eneken Tikk (ed.), *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (UN Office for Disarmament Affairs, 2017). The Global Commission on the Stability of Cyberspace (GCSC) has also been conducting important work on global cybersecurity norms. See, for example, GCSC, 'Call to Protect the Public Core of the Internet', November 2017; GCSC, 'Call to Protect the Electoral Infrastructure', May 2018; and GCSC, 'Norm Package Singapore', November 2018.

11 Mačák, *supra* n.4, 882.

12 Martha Finnemore and Duncan B. Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *SSRN*, 6 March 2019.

13 Herbert Lin, 'Responding to Sub-Threshold Cyber Intrusions: A Fertile Topic for Research and Discussion', (2011) 12 *Georgetown Journal of International Affairs* 127, 129-130.

14 Leonhard Kreuzer, 'Disentangling the cyber security debate', *Völkerrechtsblog*, 20 June 2018.

Relying on the typology, this paper reveals how State silences concerning the application of international law to peacetime cyber operations are not uniform, but vary in terms of their targets, scope, and rationale depending on the particular security threat under examination. In terms of *targets*, silences may pertain to the identification of hostile cyber operations, the existence and contours of international legal rules, issues of attribution, or measures adopted in response to cyber operations. In terms of *scope*, silences may be more prevalent amongst particular groupings of States or concerning the applicability of particular types of international legal norms. In terms of *rationale*, silences may be motivated by a range of concerns, including technical attribution challenges, geopolitical sensitivities, a desire for operational flexibility in cyberspace, or averting the risk of legitimising the repressive practices of other States.

The paper concludes that these variations not only reflect an important dimension of the politics of international law, but are also salient to how State silences in different cyber contexts may be evaluated. Contrary to the tendency to automatically cast State silences in a negative light, this paper reveals that silences can perform different and sometimes constructive functions that are yet to be fully acknowledged or appreciated.

2. PEACETIME CYBER ATTACKS

Peacetime cyber attacks are destructive cyber operations, encompassing acts undertaken by a State – or actors whose conduct is attributable to a State under international law – that uses cyber capabilities to alter, disrupt, degrade or destroy the computer systems or networks of a foreign State, or the information or programs resident in those systems or networks, which fall below the threshold required to constitute a prohibited use of force and occur outside the context of an armed conflict.[15] To the extent that information concerning peacetime cyber attacks has entered the public domain,[16] at least four types of silences are identifiable in the reactions of victim States.

First, victim States have sometimes been silent as to whether a particular incident resulted from an accident or a cyber attack. Kristen Eichensehr has referred to this type of silence as pertaining to the "what" attribution question, which involves determining what caused a particular incident.[17] For instance, when its centrifuges began spinning out control in 2008, it was not immediately apparent to Iran that its nuclear facilities had been subject to a cyber attack by the Stuxnet worm rather than failures of their own internal operating teams.[18]

15 This definition draws on Lin, *supra* n.13, 129.

16 On the limits of available open-source material that reveals both the existence of hostile cyber operations and State responses to them, see Efrony and Shany, *supra* n.4, 594-595 and 631-632.

17 Kristen Eichensehr, 'Cyber Attribution Problems – Not Just Who, But What', *Just Security*, 11 December 2014.

18 David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times*, 1 June 2012.

Second, in other instances, victim States have refrained from taking a public position in response to particular cyber attacks, remaining silent both in terms of whether attacks may be attributed to other States, as well as whether any response measures have been adopted. The series of cyber attacks involving the so-called Shamoon malware offers a clear illustration of this approach.[19] This malware was deployed against a range of Saudi Arabian and Qatari private and public sector targets between 2012 and 2017, resulting in the erasure of data from the hard drives of infected computers and significant network shutdowns. Yet, despite suspicions that the attacks were sponsored by Iran, to date the Shamoon operations have not been publicly attributed by Saudi Arabia or Qatar to any State or State-sponsored group, nor have there been any official non-covert operations in response.[20]

Third, in some contexts, victim States have responded by publicly attributing cyber attacks to other States whilst remaining silent about whether international law is applicable to the situation. A clear example of this approach may be found in the response of the US to the 2014 cyber attack against Sony Pictures Entertainment.[21] Conducted by a hacking group calling itself "Guardians of the Peace", the Sony operation involved, *inter alia*, the deployment of destructive malware which caused tens of millions of dollars of damage to Sony's computer infrastructure. In response, the US publicly attributed the cyber attack to North Korea and imposed a series of sanctions on ten individuals and three entities associated with the North Korean regime. In addition, the shutdown of North Korea's Internet network on Christmas Eve of 2014 is widely believed to have been a covert US response to the Sony hack. Yet, in terms of international law, US Secretary of State John Kerry was only willing to characterise the cyber attack as an operation that demonstrated North Korea's "flagrant disregard for international *norms*",[22] while US President Obama referred to the incident as "an act of cyber vandalism", a phrase without a clear legal connotation.[23]

A similar approach was adopted in response to the WannaCry cyber attack.[24] In 2017, WannaCry affected hundreds of thousands of computers across at least 150 States around the world. The WannaCry malware prevented Microsoft's Windows operating system from booting and encrypted all data stored on affected computers. In October

19 See generally, Efrony and Shany, *supra* n.4, 620-624.

20 Ibid., 623-624.

21 See generally, ibid., 605-609; Clare Sullivan, 'The 2014 Sony Hack and the Role of International Law', (2016) 8 *Journal of National Security Law & Policy* 437; and Michael Schmitt, 'International Law and Cyber Attacks: Sony v. North Korea', *Just Security*, 17 December 2014.

22 'Condemning Cyber-Attacks by North Korea', *US Department of State Press Release*, 19 December 2014 (emphasis added).

23 'US may put North Korea back on state terror list after Sony 'cybervandalism'', *The Guardian*, 21 December 2014.

24 See generally, Efrony and Shany, *supra* n.4, 626-628; Michael Schmitt and Sean Fahey, 'WannaCry and the International Law of Cyberspace', *Just Security*, 22 December 2017; Michael J. Adams and Megan Reiss, 'How Should International Law Treat Cyberattacks like WannaCry', *Lawfare*, 22 December 2017; Jack Goldsmith, 'The Strange WannaCry Attribution', *Lawfare*, 21 December 2017; and Kristen Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *Just Security*, 20 December 2017.

2017, the UK publicly attributed the cyber attack to North Korea,[25] an assessment that was endorsed by Microsoft's President and Chief Legal Officer, Brad Smith.[26] In December 2017, US Homeland Security advisor Tom Bossert also publicly attributed WannaCry to North Korea, an assessment that was endorsed by several cybersecurity firms and five other States: the UK, Canada, Japan, Australia, and New Zealand.[27] Again, however, the vocabulary of international law was conspicuous by its absence. Bossert, for example, neglected to mention international law or to identify any particular response measures being taken against North Korea.[28] Similarly, while the UK Foreign Office Minister for Cyber, Lord Ahmad, confirmed that "international law applies online as it does offline", he stopped short of determining whether WannaCry itself violated international law.[29]

Finally, on at least one occasion States have responded to a pattern of hostile cyber operations – some of which amounted to cyber attacks – by publicly attributing them to another State and confirming that the pattern of operations constituted a violation of international law, whilst remaining silent as to which norms of international law in particular were violated. Specifically, in October 2018, the UK and its allies exposed a series of cyber operations conducted by the Russian military intelligence service against political institutions, businesses, media outlets, and an international sports agency.[30] Some of the operations amounted to cyber attacks, including, for example, a destructive cyber operation that targeted the Ukrainian finance, energy, and government sectors but which ultimately spread and affected other European businesses.[31] According to statements released by a number of States, this series of hostile Russian cyber operations violated both international law and non-binding norms of responsible behaviour in cyberspace. The UK's National Cyber Security Centre, for example, condemned the Russian campaign of cyber operations as a "flagrant violation of international law", while UK Foreign Secretary Jeremy Hunt claimed that "this pattern of behaviour demonstrates [Russia's] desire to operate without regard to international law or established norms and to do so with a feeling

25 'British security minister says North Korea was behind WannaCry hack on NHS', *The Independent*, 27 October 2017.

26 'North Korean government behind NHS cyber attack, says Microsoft boss', *ITV News*, 13 October 2017.

27 'Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea', *White House Press Briefings*, 19 December 2017.

28 Ibid.

29 Foreign and Commonwealth Office and Lord Ahmad of Wimbledon, 'Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks', *Press Release*, 19 December 2017.

30 National Cyber Security Centre, 'Reckless campaign of cyber attacks by Russian military intelligence service exposed' *Press Release*, 4 October 2018. For commentary, see generally, Jeffrey Biller and Michael Schmitt, 'Un-caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences', *EJIL: Talk!*, 24 October 2018.

31 National Cyber Security Centre, *supra* n.30.

of impunity and without consequences".[32] Although these statements made clear the UK's position that international law had been violated, they were nonetheless vague in three respects: first, they failed to distinguish between the different cyber operations attributed to Russia – merely noting that "the pattern" of cyber operations was in violation of international law and established norms; second, the statements failed to distinguish which cyber operations violated international law and which merely transgressed voluntary norms of responsible behaviour in cyberspace; and finally, the statements failed to specify which international laws and established norms in particular had been violated.

A range of reasons may explain these different forms of State silence in response to cyber attacks. State reticence to publicly identify, attribute or respond to cyber attacks may simply be a result of insufficient evidence either concerning the existence of an attack or concerning the attribution of the cyber operation to a suspected State. The challenges of attribution in the cyber domain are well documented, requiring *technical* attribution to identify the location and identity of the cyber infrastructure from which an operation originates, *political* attribution to identify the person behind the infrastructure, and *legal* attribution to identify a sufficient legal nexus between the persons behind the operation and a State. The complexity of attribution in the cyber context is compounded by a variety of factors, including the ability for cyber operations to be routed through multiple computer networks in different States and the use of "anti-attribution" mechanisms to hide the provenance of cyber operations.[33]

Even when attribution *is* possible, national security concerns may lead victim States to opt for silence; for example, to prevent their adversaries from finding out that they have been detected or to reduce the risks associated with publicly exposing the victim State's vulnerabilities and technological capabilities. In addition, victim States may have geopolitical interests in remaining silent in the face of a cyber attack, including reducing the risk of escalation or ensuring that ongoing diplomatic efforts with particular States in related issue areas are not negatively affected.[34] A lack of effective response measures may also motivate State silence in this context. As Jack Goldsmith and Stuart Russell explain: "Unless a nation is able to effectively redress a cyber

32 Ibid. For similar statements, see 'Joint statement by Presidents Tusk and Juncker and High Representative Mogherini on Russian cyber attacks', Council of the EU, *Press Release*, 4 October 2018 ("We deplore such actions, which undermine international law and international institutions"); 'Attribution of a Pattern of Malicious Cyber Activity to Russia', Prime Minister of Australia, Minister for Foreign Affairs of Australia, *Media Release*, 4 October 2018 ("contrary to the consensus on international law and norms"); 'Canada identifies malicious cyber-activity by Russia', Global Affairs Canada, 4 October 2018 ("demonstrate a disregard for international law and undermine the rules-based international order"); 'Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW', Ministry of Defence of the Netherlands, 4 October 2018 ("undermine the international rule of law").

33 Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', (2012) 17 *Journal of Conflict & Security Law* 229, 234.

34 Efrony and Shany, *supra* n.4, 632-637.

intrusion, it can be harmful or self-defeating to publicize it, since public knowledge of loss and the failure to respond effectively invite more attacks".[35]

The reluctance of States to confirm whether or how international law applies in the context of particular cyber attacks likely stems from additional factors. In particular, State silence in this context may reflect doubts about the adequacy and adaptability of the international legal framework to the cyber domain. In terms of *adequacy*, the limitations of self-help remedies available to victim States under the law of State responsibility, including the notification and proportionality conditions of countermeasures, may lead some States to conclude that there is little added utility in invoking international law in the cyber domain.[36] In terms of *adaptability*, State silence may reflect a lack of consensus within a particular government or disagreements *between* governments trying to formulate a coordinated response to a particular cyber attack over whether there has been an international legal violation and, if so, which norm of international law has been violated.[37] In the latter regard, it is entirely plausible that States may prefer to adopt a "wait and see" approach before publicly clarifying their international legal position, particularly given the rapidly-changing technological landscape in which cyber attacks are launched.

Differences in the technical capabilities of States to reliably attribute hostile cyber operations may also underpin the silence of certain States concerning the applicability and contours of international law in the context of cyber attacks. Evaluating the reasons behind the opposition of certain States to the applicability of countermeasures in the cyber context at the most recent round of UN GGE talks, Michael Schmitt and Liis Vihul point to the operational reality that "some States, such as Cuba, lack the technical wherewithal of more advanced States to reliably attribute hostile cyber operations and therefore will be less able to establish the necessary basis for resorting to […] countermeasures".[38] Similar concerns may conceivably underpin the reticence of certain States to have recourse to international law more generally when responding to cyber attacks.

Finally, State silence concerning which specific international legal norms have been violated by a given cyber attack may also stem from the conflicting internal interests of powerful States concerning how permissive they believe the international legal framework applicable in cyberspace should be. As Kubo Mačák explains, since powerful States are also some of the most vulnerable to hostile cyber operations, such

35 Jack Goldsmith and Stuart Russell, 'Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in its International Relations', *Aegis Series Paper No. 1806* (Hoover Institution, 2018), 13. See similarly, Eichensehr, *supra* n.24 ("[A]nother possibility is that states do agree that WannaCry violated international law, but are making a policy choice not to call North Korea's actions a legal violation in order to avoid creating public expectations about the need for governments to respond").

36 Efrony and Shany, *supra* n.4, 651.

37 Eichensehr, *supra* n.24.

38 Michael Schmitt and Liis Vihul, 'International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms', *Just Security*, 30 June 2017.

States tend to be confronted by a "glass house dilemma" when formulating their legal positions in the cyber domain, torn between an *offensive* desire for permissive rules that leave some operational flexibility for stone-throwing and a *defensive* desire for restrictive rules that protect the glass houses in which they reside.[39] It is this tension that likely explains the vagueness of the UK's legal position concerning the hostile cyber operations conducted by the Russian military intelligence service. While it was in the UK's defensive interests to interpret the applicable law to conclude that Russia's cyber operations violated international law, it was in its offensive interests to remain silent and ambiguous about which specific international legal norms had been violated so as to leave operational leeway for the permissibility of its own hostile cyber operations in the future.[40]

3. PEACETIME CYBER ESPIONAGE

Peacetime cyber espionage is an information-gathering cyber operation, encompassing any act undertaken clandestinely or under false pretences by a State – or actors whose conduct is attributable to a State under international law – that uses cyber capabilities to copy information from closed as opposed to open sources of a foreign State, which falls below the threshold required to constitute a prohibited use of force and occurs outside the context of an armed conflict.[41] Historically, the predominant policy of States with respect to peacetime espionage operations has been one of criminalisation at the domestic level combined with silence as to their legality under international law. In the latter regard, while there is extensive State practice of espionage, which is widely accepted as a core national security function of the State, espionage operations have generally not been accompanied by government statements from which their legality or illegality under international law may be inferred.[42] According to this

39 Kubo Mačák, 'On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law', (2019) 113 *AJIL Unbound* 81, 82-84.

40 In this regard, it is notable that the international legal norm that the UK could most easily have alleged Russia to have violated – sovereignty – had recently been characterised by the UK Attorney General as a general principle from which the UK could not currently extrapolate any "specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention". UK Attorney General, 'Cyber and International Law in the 21st Century', 23 May 2018, available online at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (last accessed 5 January 2019). See similarly, Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber', (2017) 111 *AJIL Unbound* 207, 208 (characterising sovereignty as "a principle of international law that guides state interactions, but is not itself a binding rule that dictates results under international law"). This position seems to be driven by an offensive desire to establish a broad zone of international legal permissibility within cyberspace. See, in this regard, Biller and Schmitt, *supra* n.30 ("because the criteria for engaging in a prohibited intervention or use of force are both demanding and ill-defined, the 'sovereignty is not a rule' position affords other States the flexibility to act in an 'indiscriminate and reckless' manner while claiming to operate within the boundaries of international law").

41 This definition draws on: *Tallinn Manual 2.0*, *supra* n.3, 168; Russell Buchan, *Cyber Espionage and International Law* (Bloomsbury, 2018), Chapter 1; and Asaf Lubin, 'The Liberty to Spy', *Harvard International Law Journal* (forthcoming).

42 Katharina Ziolkowski, 'Peacetime Cyber Espionage – New Tendencies in Public International Law', in Katharina Ziolkowski (ED.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE, 2013) 425, 437-443.

traditional perspective, therefore, acts of espionage have generally been considered to be either permitted on the basis that they are not forbidden by international law, or *prima facie* in violation of general rules of international law but subject to a customary exception that regards those violations as permissible.[43]

With the advent of cyberspace, however, the espionage landscape has evolved. Cyber technologies have improved the efficiency of espionage operations, enabling cheaper, easier, and increasingly remote access to enormous volumes of information.[44] Significantly, the expansive nature of espionage missions in the digital age implicates non-State actors to an unprecedented degree, including, for example, through the bulk collection of personal data as part of State surveillance programmes.[45] The broader scope of cyber espionage operations has also coincided with their increased visibility, whether as a result of leaks, voluntary transparency on the part of States, or simply the heightened detectability of espionage programmes.[46] Responding to this new environment and to growing pressures from corporations, civil society groups, and the general public for greater regulatory constraints, States have begun to be more vocal about the international legal regulation of peacetime espionage operations. To evaluate these new practices, a distinction may usefully be drawn between international legal rules that aim to protect *the rights of States* and those that aim to protect *the rights of individuals*.[47]

Allegations that acts underlying cyber espionage operations violate international legal rules designed to protect *the rights of States* continue to be the exception. For example, in the wake of the 2013 Snowden disclosures concerning the surveillance practices of the US National Security Agency (NSA), the UK Government Communications Headquarters, and their allies, only a small minority of States declared such

43 Iñaki Navarrete and Russell Buchan, 'Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions', *Cornell International Law Journal* (forthcoming) (describing the "mainstream view about espionage" as holding that "while different forms of espionage violate different international legal rules, […] general and consistent practice of States acting out of a sense of legal obligation has carved out customary espionage "exceptions" (or "defenses") to those primary rules of international law"). For further discussion of the legality of traditional espionage, see generally, Ashley Deeks, 'An International Legal Framework for Surveillance', (2015) 55 *Virginia Journal of International Law* 291, 300-319; and Darien Pun, 'Rethinking Espionage in the Modern Era', (2017) *Chicago Journal of International Law* 353, 359-368. For an alternative perspective, elaborating a new and innovative legal framework for articulating the law and practice of interstate peacetime espionage operations, see Lubin, *supra* n.41; and Asaf Lubin, 'Cyber Law and Espionage Law as Communicating Vessels', in Tomáš Minárik et al. (eds), *CyCon X: Maximising Effects* (NATO CCD COE Publications, 2018) 203, 219-224.

44 Ido Kilovaty, 'World Wide Web of Exploitations – The Case of Peacetime Cyber Espionage Operations Under International Law: Towards a Contextual Approach', (2016) *Columbia Science & Technology Law Review* 42, 66-69.

45 Ashley S. Deeks, 'Confronting and Adapting: Intelligence Agencies and International Law', (2016) *Virginia Law Review* 599, 621-623.

46 Ibid., 615-621.

47 Ibid., 631-650. The present analysis of peacetime cyber espionage operations is not intended to be exhaustive – omitting, for example, consideration of the relationship between cyber espionage and diplomatic and consular law, as well as the relationship between economic cyber espionage and the World Trade Organisation. For a comprehensive overview of cyber espionage and international law, see generally, Buchan, *supra* n.41.

programmes to constitute violations of State-focused international legal rules.[48] Most prominently, the Brazilian President at the time, Dilma Rousseff, characterised the NSA surveillance programme as a situation of "disrespect to […] national sovereignty […and] a breach of international law".[49] The Foreign Ministry of Mexico issued a press release condemning US surveillance practices with respect to the Mexican government and president as "unacceptable, unlawful, and contrary to Mexican law as well as international law".[50] Indonesia also claimed that extraterritorial surveillance practices violate international law and the UN Charter,[51] while the Bahamas argued that the NSA's secret interception of virtually every cell phone conversation in the country had led its citizens to question "what these high ideals of territorial integrity, sovereignty and respect for the rule of law actually mean in practice".[52] The Chinese government also declared that the NSA's surveillance practices had "flagrantly breached international laws […and] deserve to be rejected and condemned by the whole world".[53] Yet, not only were these statements small in number compared to the extensive reach of the surveillance programmes revealed by the Snowden leaks, they were also variable and ambiguous in their specificity.[54] In addition, the sincerity of some of these statements is questionable in light of media reports that reveal similar intelligence practices conducted by some of the States that raised these allegations.[55]

In general, therefore, silence concerning the compatibility of peacetime cyber espionage operations with State-focused international legal rules continues to be the prevailing policy of States.[56] To take a prominent example, the US response to the massive data theft from the Office of Personnel Management between 2014 and 2015 has to date been muted. Despite being dubbed "one of the most potentially damaging

48 For additional analysis of these and other statements submitted by States in response to the Snowden disclosures, see Navarrete and Buchan, *supra* n.43. Beyond State reactions to the Snowden leaks, other practices in support of State-focused intentional legal regulation of espionage operations include the International Court of Justice's provisional measures order in the case between Timor-Leste and Australia, which was based on the plausibility that Australia's interception of information belonging to East Timor located on Australian territory violated East Timor's sovereignty, as well as the German Foreign Ministry's indication to the UK that "tapping communications from a diplomatic mission would be a violation of international law". See generally, Deeks, *supra* n.45, 641-645.

49 'Remarks by Dilma Rousseff at the 68th UN General Assembly', *Voltaire Network*, 24 September 2013.

50 'Mexico Slams US Spying on President', *Der Spiegel*, 21 October 2013.

51 Deeks, *supra* n.45, 644.

52 'Bahamas Raises NSA Spy Scandal at OAS Summit', *Curaçao Chronicle*, 5 June 2014.

53 'China demands halt to 'unscrupulous' US cyber-spying', *The Guardian*, 27 May 2014.

54 See, in this regard, *Tallinn Manual 2.0, supra* n.3, 169 (noting that there remains insufficient State practice and *opinio juris* to conclude that customary international law prohibits espionage *per se*).

55 See, for example, 'Brazil Says It Spied on U.S. and Others Inside Its Borders', *The New York Times*, 4 November 2013.

56 In a notable exception, however, Brian Egan, US State Department Legal Adviser, recently confirmed the US legal position that "there is no *per se* prohibition on such activities under customary international law". Egan, *supra* n.4, 174. This type of statement does not, however, offer insight into how the US views the compatibility of the constituent acts of cyber espionage with general rules of international law. See, in this regard, *Tallinn Manual 2.0, supra* n.3, 170 ("While the International Group of Experts agreed that there is no prohibition of espionage per se, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain of the methods employed to conduct cyber espionage are unlawful").

cyber heists in U.S. government history",[57] the only notable public response by a US official has been one of seeming admiration – James Clapper, then-head of the Office of the Director of National Intelligence, remarking that "you have to kind of salute the Chinese for what they did".[58]

By contrast, the compatibility of the acts underlying peacetime cyber espionage operations with *individual-focused* international legal rules has achieved a prominent position on the agenda of the international community. In particular, the question of the compatibility of peacetime cyber espionage practices with international human rights law has been visible in at least three respects.[59]

First, a number of States have responded to disclosures about the espionage practices of other States by alleging violations of international human rights law. The then-President of Brazil, Dilma Rousseff, for example, characterised the NSA's surveillance programme as a "situation of grave violations of human rights and of civil liberties", adding that "[t]he right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country".[60]

Second, States have expressly recognised the dangers posed by surveillance programmes to individual human rights in a series of resolutions adopted by the UN General Assembly and the Human Rights Council concerning the right to privacy in the digital age.[61] In Resolution 68/167 of 2013, for example, the UN General Assembly expressly recognised "the negative impact that surveillance and/or interception of communications, *including extraterritorial surveillance and/or interception of communications*, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights".[62] In the same resolution, the General Assembly called upon all States to review their

57 'Hacks of OPM databases compromised 22.1 million people, federal authorities say', *The Washington Post*, 9 July 2015.

58 'U.S. Intelligence Chief James Clapper Suggests China Behind OPM Breach', *The Wall Street Journal*, 25 June 2015.

59 Deeks, *supra* n.45, 635-641 (also discussing a fourth context, namely constraints placed on State intelligence agencies by each other). In addition to the examples discussed here, another important area of individual-focused norms is data protection law, in particular the EU's General Data Protection Regulation, which indirectly affects espionage activities by regulating the personal data processing practices of private actors like social media companies, which intelligence agencies sometimes compel to release data.

60 'Remarks by Dilma Rousseff at the 68th UN General Assembly', *Voltaire Network*, 24 September 2013. See also, 'China demands halt to 'unscrupulous' US cyber-spying', *The Guardian*, 27 May 2014 (noting how the Chinese government also concluded that the NSA programme "seriously infringed upon […] human rights").

61 UN General Assembly Resolution 68/167, 18 December 2013, U.N. Doc. A/RES/68/167; UN General Assembly Resolution 69/166, 18 December 2014, U.N. Doc. A/RES/69/166; UN General Assembly Resolution 71/199, 19 December 2016, U.N. Doc. A/RES/71/199; Human Rights Council Resolution 28/16, 26 March 2015, U.N. Doc. A/HRC/RES/28/16; and Human Rights Council Resolution 34/7, 23 March 2017, U.N. Doc. A/HRC/RES/34/7. See generally, Carly Nyst and Tomaso Falchetta, 'The Right to Privacy in the Digital Age', (2017) 9 *Journal of Human Rights Practice* 104.

62 UN General Assembly Resolution 68/167, 18 December 2013, U.N. Doc. A/RES/68/167, Preamble.

procedures, practices, and legislation regarding their surveillance programmes to ensure their compatibility with international human rights law.[63]

Finally, States have begun to be held accountable for their cyber espionage practices through the findings of human rights treaty bodies and litigation. Determining the compatibility of State espionage programmes with international human rights law generally entails answering two questions: first, whether human rights obligations are applicable to extraterritorial surveillance practices; and second, whether human rights obligations have been violated by such practices.

As regards the first question, apart from notable exceptions such as the US and Israel, there is widespread support amongst States that in certain circumstances human rights obligations apply extraterritorially.[64] In this regard, the prevailing view is that the extraterritorial application of human rights obligations requires power or effective control by the State concerned over territory (the spatial model of jurisdiction) or the person affected (the personal model of jurisdiction).[65] Traditionally, this test has been understood to require *physical* control, a condition which is ill-suited to the cyber domain where control over infrastructure and individuals tends to be virtual in nature. Nonetheless, recent indications from human rights experts, treaty bodies, and courts suggest that the "power or effective control" test may be sufficiently malleable to encompass the extraterritorial cyber surveillance practices of States.[66] In this regard, it is notable that the UN Human Rights Committee has concluded that "measures should be taken to ensure that any interference with the right to privacy complies with the principle of legality, proportionality and necessity, *regardless of the nationality or location of the individuals whose communications are under direct surveillance"*.[67] More recently, in the landmark surveillance case, *Big Brother Watch & Others v. the UK*, the European Court of Human Rights (ECtHR) was able to side-step the question of the applicability of the European Convention on Human Rights to extraterritorial surveillance because the UK government decided not to raise a jurisdictional objection on this point. The case offers an example of how the silence of a State can, in certain contexts, enable scrutiny of its practices; the ECtHR was able to proceed "on the

63 Ibid., para. 4(c).

64 Monika Heupel, 'How do States Perceive Extraterritorial Human Rights Obligations? Insights from the Universal Periodic Review', (2018) 40, *Human Rights Quarterly* 52.

65 See, for example, UN Human Rights Committee, 'General Comment 31 – The Nature of the General Legal Obligations Imposed on States Parties to the Covenant', U.N. Doc. CCPR/C/21/Rev1/Add.13, 29 March 2004, para. 10; and *Al-Skeini v. The United Kingdom*, Application No. 55721/07, ECtHR, Judgment, 7 July 2011, paras 133-140.

66 See, in particular, Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law* (2019, *forthcoming*); Vivian Ng and Daragh Murray, Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?, *HRC Essex Blog*, 2 August 2016; and Report of the Office of the UN High Commissioner for Human Rights: The Right to Privacy in the Digital Age, 30 June 2014, U.N. Doc. A/HRC/27/37, para. 34.

67 UN Human Rights Committee, 'Concluding observations on the fourth periodic report of the United States of America', U.N. Doc. CCPR/C/USA/CO/4, 23 April 2014, para. 22 (emphasis added).

assumption that the matters complained of fall within the jurisdictional competence of the United Kingdom".[68]

On the second question, a significant body of case law has developed concerning the compatibility of State surveillance practices with international human rights law, with an emphasis on the right to privacy in particular. The seminal judgment concerning cyber surveillance is the aforementioned case of *Big Brother Watch & Others v. the UK*, in which the ECtHR scrutinised the UK's bulk interception of content and certain metadata relating to so-called "external communications" (i.e. foreign-to-foreign, foreign-to-domestic, and domestic-to-foreign communications), its receipt of US signals intelligence collection, and its compulsion of communication service providers to provide certain metadata on a targeted basis. While space does not permit a thorough examination of the judgment, two aspects were particularly notable.[69] First, the ECtHR effectively normalised the practice of mass surveillance by concluding that "the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation" and characterising bulk interception as "a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime".[70] The judgment's legitimation of mass surveillance programmes – confining its role to determining whether sufficient safeguards have been adopted in their implementation – stands in contrast to sentiments expressed by the Court of Justice of the European Union (CJEU) in the *Schrems* decision of 2015, in which the CJEU stated that "legislation permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life".[71] Second, the ECtHR adjusted in various ways the application of the safeguards it had developed in the context of scrutinising *targeted* surveillance regimes – for example, by dispensing with the requirement for objective evidence of reasonable suspicion in relation to the persons on whom data is being sought – thereby introducing a differentiated approach to the regulation of surveillance that distinguishes between bulk and targeted surveillance practices.[72]

As this analysis indicates, States have generally been far more reticent to discuss the applicability of *State-focused* compared to *individual-focused* norms of international

68 *Big Brother Watch & Others v. The United Kingdom*, Application Nos 58170/13, 62322/14 and 24960/15, ECtHR, Judgment, 13 September 2018, para. 271. The issue was also not addressed in *Centrum För Rättvisa v. Sweden*, Application No. 35252/08, ECtHR, Judgment, 19 June 2018 (a case in which the ECtHR upheld Swedish legislation that authorised the gathering of covert bulk signals intelligence).

69 See generally, Theodore Christakis, 'A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgment', *European Law Blog*, 20 September 2018. For commentary on the similar case of *Centrum För Rättvisa v. Sweden*, see Asaf Lubin, 'Legitimizing Foreign Mass Surveillance in the European Court of Human Rights', *Just Security*, 2 August 2018.

70 *Big Brother Watch & Others, supra* n.68, paras 314 and 386.

71 *Maximilian Schrems v. Data Protection Commissioner*, C-362/14 ECLI:EU:C:2015:650, Court of Justice of the EU, Judgment, 6 October 2015, para. 94.

72 *Big Brother Watch & Others, supra* n.68, paras 303 and 316-320.

law in the context of peacetime cyber espionage operations. A number of reasons likely explain this divergence, including the heightened external pressures exerted by human rights groups and courts on States to conform their espionage practices to individual-focused norms, the unpalatability of States arguing that international human rights law does not apply to espionage practices, and the fact that State agencies surrender less flexibility of action in conceding that individual-focused norms apply to their practices compared to State-focused norms.[73]

4. PEACETIME CYBER INFORMATION OPERATIONS

Peacetime cyber information operations are content-based cyber operations, encompassing any act undertaken clandestinely or under false pretences by a State – or actors whose conduct is attributable to a State under international law – that harnesses information in the cyber domain to influence political sentiment in a foreign State, which falls below the threshold required to constitute a prohibited use of force and occurs outside the context of an armed conflict.[74] Examples of cyber information operations include:[75] *dis*information operations, which involve the spread of "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public";[76] and *mal*information operations, which involve threatening, abusive, discriminatory, harassing or disruptive behaviour that aims to cause harm to a person, organisation or State.[77] With the rise of social media, cyber information operations have become increasingly prevalent in recent years, the most high profile being Russia's cyber information operation on the 2016 US presidential election.[78] Importantly, the targets of information operations are the perceptions of an adversary which reside in the cognitive dimension of the information ecosystem.[79] Since the regulation of cyber information operations embroils States in defining the boundaries of content control

73 Deeks, *supra* n.45, 665-667 (noting that interpreting State-focused norms as strictly applying to espionage activities "would bring to a halt most spying and covert action, as so many of those activities violate other states' territorial integrity and sovereignty, broadly interpreted"). It should be emphasised that the extent to which States have been willing to engage in discussions concerning the application of individual-focused norms to espionage practices has been variable. While States in Europe have proven particularly vocal, other States – such as China, for example – have been relatively silent.

74 This definition draws on Jen Weedon et al., 'Information Operations and Facebook', *Facebook*, 27 April 2017, 4.

75 Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking* (2017), 20 (also distinguishing the further category of "mis-information", namely information that is false but not created with the intention of causing harm).

76 'Communication – Tackling Online Disinformation: A European Approach', European Commission, COM(2018) 236 final, 26 April 2018, 3-4.

77 Chris Tenove et al., *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (2018), 22-25.

78 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, ICA 2017-01D, 6 January 2017. See also, Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, November 2017 (noting that disinformation tactics "played an important role in elections in at least 17 other countries over the past year").

79 Herbert Lin and Jaclyn Kerr, 'On Cyber-Enabled Information/Influence Warfare and Manipulation', *SSRN* (2017), 6.

and freedom of expression, it is perhaps unsurprising that approaches adopted at the international level to date have been highly divergent.

According to what may be termed the digital authoritarian perspective – whose adherents include China, Russia, and other members of the Shanghai Cooperation Organisation (SCO) – cyber information operations encompass a broad category of "information security" threats, including internal dissent and anti-government information disseminated through cyberspace.[80] As Roger Hurwitz explains, adherents to this perspective tend to be motivated by a desire "to control the ideational space that cyber networks afford their populations", based on a characterisation of cyberspace as "a vector for dissident political information and organizing – one not easily suppressed, but easily exploited by external rivals, in particular the United States".[81] In line with this stance, in 2009 the SCO adopted an agreement which defined "information war" in broad terms as "dissemination of information harmful to political, social and economic systems, as well as spiritual, moral and cultural spheres of other States".[82] Towards the end of 2011, a number of SCO members, including China and Russia, submitted to the UN General Assembly a draft International Code of Conduct for Information Security,[83] which they updated in early 2015.[84] The 2011 draft advocated "curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment".[85] As Tim Stevens notes, this provision "has been widely interpreted as a defence of internet censorship and states' rights to prohibit access to materials deemed inimical to their ideologies".[86]

80 Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', *Aegis Paper Series No. 1703* (Hoover Institution, 2017), 3; and Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (CUP, 2018), 54-55.

81 Roger Hurwitz, 'A New Normal? The Cultivation of Global Norms as Part of a Cybersecurity Strategy', in P.A. Yannakogeorgos and A.B. Lowther (eds.), *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (Taylor & Francis, 2014) 233, 238.

82 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security (16 June 2009), unofficial translation available online at: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf (last accessed 5 January 2019).

83 International Code of Conduct for Information Security (2011), Annex to the Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N.Doc. A/66/359 (14 September 2011).

84 International Code of Conduct for Information Security (2015), Annex to the letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N.Doc. A/69/723 (13 January 2015).

85 International Code of Conduct for Information Security (2011), *supra* n.83, para (c). See similarly, Draft International Code of Conduct for Information Security (2015), *supra* n.84, para. 2(3) (advocating for States not to use ICTs "to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability"); and Astana Declaration of the Heads of State of the Shanghai Cooperation Organization, 9 June 2017 ("member states will continue to strengthen practical interaction in countering propaganda and justifications of terrorism, separatism and extremism in the media").

86 Tim Stevens, 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace', (2012) 33 *Contemporary Security Policy* 148, 162.

By contrast, the US and members of the EU have generally refrained from discussing cyber information operations at the multilateral level, rejecting the language of "information security" in favour of a narrower discussion of technical security risks under the banner of "cyber security".[87] The silence of those States at the multilateral level should not, however, be mistaken for a lack of concern for the regulation of cyber information operations at the regional or domestic levels. All States regulate the dissemination of content in their territories, the difference between them being essentially one of degree.[88]

In the EU, for example, illegal content includes incitement to terrorism, xenophobic and racist speech that publicly incites hatred and violence, as well as child sexual abuse.[89] Even the US, which is host to one of the most permissive free speech environments in the world, has federal criminal laws that restrict, for example, child pornography and knowingly providing material support to designated foreign terrorist organizations.[90] These types of *content restriction* laws are often paired with *intermediary liability* laws, which establish the conditions under which intermediaries – including social media platforms – may be held liable for illegal content generated by their users.[91] Germany, for example, recently enacted the Network Enforcement Act (*NetzDG*), which requires major social media platforms with at least two million registered German users to set up an effective and transparent complaints management infrastructure that can ensure illegal content is deleted or blocked within specified timeframes, or risk facing the prospect of penalties of up to €50 million.[92]

Viewed in this light, the reticence of certain States such as the US and members of the EU to discuss the regulation of cyber information operations at the multilateral level is not driven by a disdain for content regulation *per se*, but a fear that an international treaty would serve to legitimise the highly intrusive online censorship practices implemented by digitally authoritarian governments such as China and Russia.[93] Indeed, it is possible that one of the reasons why the Obama administration decided to characterise Russia's information operation on the 2016 US presidential election as merely a "violation of established international *norms* of behavior" was a concern

87 Segal, *supra* n.80, 3; and Maurer, *supra* n.80, 54-55.

88 See similarly, Zhixiong Huang and Kubo Mačák, 'Toward the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches', (2017) 16 *Chinese Journal of International Law* 271, 294.

89 'Communication – Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms', European Commission, COM(2017) 555 final, 28 September 2017, 2.

90 Daphne Keller, 'Internet Platforms: Observations on Speech, Danger, and Money', *Aegis Series Paper No. 1807* (Hoover Institution, 2018), 12.

91 Rebecca MacKinnon et al., *Fostering Freedom Online: The Role of Internet Intermediaries* (UNESCO, 2014), 40-43.

92 See generally, William Echikson and Olivia Knodt, 'Germany's NetzDG: A Key Test for Combatting Online Hate', *Counter-Extremism Project Research Paper No. 2018/09*, November 2018.

93 See, for example, 'Statement by the Delegation of the United States', *Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-Seventh Session of the United Nations General Assembly*, 2 November 2012, available online here: https://perma.cc/3C7Q-DUDP ("we cannot support approaches proposed in the draft Code of Conduct for Information Security that would only legitimize repressive state practices").

that alleging a violation of international law might serve to lend legitimacy to Russia's efforts to significantly restrict freedom of expression, including, for example, the practices of human rights NGOs and other civil society groups.[94]

5. CONCLUSION

This paper has sought to demonstrate the explanatory value of distinguishing between cyber attacks, cyber espionage, and cyber information operations when examining the silences of States concerning the relationship between international law and peacetime cyber operations. Three insights emerge from the analysis.

First, this paper has illuminated the different *targets* of State silences. States may be silent as to the attribution of a cyber operation to another State or the measures taken in response to a particular operation. State silences may also pertain to the *existential* questions of whether or not particular rules fall within the corpus of international law or whether or not specific norms of international law are applicable to particular cyber operations – for example, determining the applicability of international human rights obligations to extraterritorial espionage practices. And finally, State silences may also concern the *expository* question of *the meaning* to be assigned to applicable norms of international law in the cyber context – whether provisions of a treaty or norms of customary international law.[95]

Second, this paper has revealed how the *scope* of State silences can vary depending on the security threat under examination. For some peacetime cyber operations, States have been silent about the applicability of a specific subset of international legal norms and more vocal about others. In the context of cyber espionage operations, for example, States have generally been silent about the applicability of *State-focused* norms of international law compared to their greater openness to discuss *individual-focused* norms of international law such as international human rights law. For other peacetime cyber operations, the spread of silence across different States concerning the applicability of international law in the cyber domain has been uneven. In the context of cyber information operations, for example, digitally authoritarian States have actively sought to legitimize their intrusive censorship practices through the

94 White House, 'Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment', *Press Release*, 29 December 2016. See, in this regard, Beatrice Walton, 'Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law', (2017) 126 *Yale Law Journal* 1460, 1513 ("[H]olding states responsible for too many cyber [operations] might encourage states to impose draconian restrictions on internet use. […] And broadening the concept of intervention or sovereignty could result in severe problems for NGOs and other supporters of human rights who engage in what might be called low-level coercive activity").

95 On *existential* and *expository* functions of interpretation, see generally, Duncan B. Hollis, 'The Existential Function of Interpretation in International Law', in Andrea Bianchi et al. (eds), *Interpretation in International Law* (OUP, 2015) 78, 79 ("international law's interpretative process can thus be likened to an iceberg – a rule's meaning arrived at by an interpreter is not simply a function of the method and technique employed (the visible tip) but rests on an array of earlier choices about whether the rule 'exists' to be interpreted in the first place (the iceberg's hidden, critical mass)").

adoption of new multilateral treaties, whereas members of the EU and the US have tended to confine their governance of online content to the regional or domestic levels through the adoption of a mixture of legal and non-legal regulatory measures.

Finally, this paper has revealed some of the possible *rationales* that may underpin the silences of States concerning the applicability and meaning of international law in the cyber domain. These include technical difficulties and geopolitical sensitivities regarding the attribution of peacetime cyber operations to other States, preferences regarding the desired degree of international legal permissibility within cyberspace, a desire to uphold particular values such as freedom of expression rather than risk legitimising intrusive censorship practices, and inclinations towards a "wait and see" approach to the applicability and contours of international law in the context of a fast-changing technological landscape.

Bearing in mind these insights, the significance of the typology outlined in this paper is threefold.

First, by revealing the variable targets, scope, and rationales behind State silences concerning the international law applicable to peacetime cyber operations, the typology reveals an important dimension of the politics that is "part and parcel of international law's structural DNA".[96] As Nicholas Tsagourias explains: "whether states will claim that a violation of international law occurred and take countermeasures depends on many factors, primarily political ones. There is no automaticity as far as the application and enforcement of international law is concerned because states are at the same time law creators, interpreters, and enforcers".[97]

Second, the typology is also salient to the extent that it cautions against the tendency to refer to State silences in uniform terms and to automatically cast such silences in a negative light. Amongst international lawyers, there is often a propensity to fetishise the value of international law, underpinned by an unspoken faith in the transformative potential of law to create order and stability.[98] Yet, as Umut Özsu points out, "the legal form has often underwritten and legitimated precisely the substantive injustice and inequality it is nominally designed to counter".[99] By identifying the distinct targets, scope, and rationales of State silences, this paper has sought to demonstrate that, in certain contexts, a policy of silence may be constructive – for example, to enable the scrutiny of extraterritorial surveillance practices or to prioritise the value of freedom of expression over the potential legitimation of invasive censorship practices. In practice, whether a policy of State silence is deemed appropriate will always be contingent on

96 Tsagourias, *supra* n.4, 74. See also, Sander, supra n.1.
97 Ibid.
98 Jean d'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought', (2016) 21 *Journal of Conflict & Security Law* 575.
99 Umut Özsu, 'Against Legal Fetishism (Part Two)', *Legal Form*, 3 November 2017.

the type of security threat to which the policy relates, the international legal norms in question, and the observational viewpoint from which the policy is evaluated.

Finally, the typology also sets the foundations for future research examining the legal significance of State silences for the development of international law applicable to different types of peacetime cyber operations. Avenues for future exploration in this context include explaining how State silences may be relied upon to make inferences about the scope and content of international legal obligations,[100] as well as examining how State actions, reactions, accusations, initiatives, and the like – which are silent as to their international legal implications – may over time inform the scope and content of international legal rules applicable to peacetime cyber operations.[101]

100 See, for example, International Law Commission, 'Identification of Customary International Law: Text of the Draft Conclusions as Adopted by the Drafting Committee on Second Reading', U.N.Doc. A/CN/4/L.908, 17 March 2018, Conclusion 10(3) ("Failure to react over time to a practice may serve as evidence of acceptance as law (*opinio juris*), provided that States were in a position to react and the circumstances called for some reaction"). On different approaches to silence in international law in general, see Helen Quane, 'Silence in International Law', (2014) 84 *British Yearbook of International Law* 240; and Roland Tricot and Barrie Sander, 'Recent Developments: The Broader Consequences of the International Court of Justice's Advisory Opinion on the Unilateral Declaration of Independence in Respect of Kosovo', (2011) *Columbia Journal of Transnational Law* 321, 330-336.

101 See, for example, Mačák, *supra* n.4, 894 (arguing that the articulation of non-binding voluntary norms in cyberspace may be viewed "as an intermediate stage on the way towards the generation of cyber 'hard law'"); and Hollis and Finnemore, *supra* n.12, 11-12 (arguing that cyber accusations by States concerning State or State-sponsored hostile cyber operations which are silent as to their international legal implications, may serve as early evidence of State practice from which *opinio juris* may emerge over time).