State behaviour in cyberspace: normative development and points of contention

Lahmann, H.C.

Zeitschrift für Außen- und Sicherheitspolitik
https://doi.org/10.1007/s12399-023-00939-7

ANALYSE

State Behaviour in Cyberspace: Normative Development and Points of Contention

Henning Lahmann

Received: 20 November 2022 / Accepted: 2 January 2023

Abstract The increasing use of digital technologies in cyberspace in the context of international conflicts has put pressure on the existing legal framework of international law. After progress in terms of norm development and clarification could be achieved through multilateral processes at the United Nations, Russia's invasion of Ukraine cast doubt on the possibility of further breakthroughs. In light of this development, unilateral declarations of legal positions by states will gain further relevance.

Keywords Cyber operations · State sovereignty · Norm finding processes · Customary international law · State practice

Staatliches Verhalten im Cyberspace: Normative Entwicklung und Streitpunkte

Zusammenfassung Die zunehmende Nutzung digitaler Technologien im Cyberraum zum Zweck zwischenstaatlicher Konfliktaustragung hat den geltenden völkerrechtlichen Rechtsrahmen unter Druck gesetzt. Nachdem multilaterale Prozesse auf UN-Ebene wenigstens in Teilbereichen zur Normklärung und -bildung beitragen konnten, stellt Russlands Invasion der Ukraine die Aussicht auf weitergehende Erfolge in Frage. Vor diesem Hintergrund werden unilaterale Erklärungen staatlicher Rechtsauffassung weiter an Bedeutung gewinnen.

Schlüsselwörter Cyberoperationen · Staatensouveränität · Normfindungsprozesse · Völkergewohnheitsrecht · Staatenpraxis

✉ Assistant Prof. Henning Lahmann
Center for Law and Digital Technologies, Leiden University Law School, Steenschuur 25, 2311 ES Leiden, The Netherlands
E-Mail: h.c.lahmann@law.leidenuniv.nl

Published online: 06 February 2023

1 Introduction

Ever since states discovered globally interconnected network technologies as potentially useful tools of statecraft to extend the projection of power to the digital realm, there has been a debate among states and within legal academia as to the international legal implications of such behaviour. Today, the fact that international law – in its entirety, principally – is applicable when a state resorts to adversarial cyber conduct against another state is virtually undisputed. At the same time, how the pertinent rules stemming from the *jus ad bellum*, the *jus in bello*, the customary law on state responsibility, or international human rights law apply and how these legal frameworks actually constrain states in cyberspace very much remains a contested question.

The following remarks briefly lay out the state of the discourse by first describing some of the adversarial cyber operations from the past 15 years that prompted the international community to take the prospect of "cyber warfare" among states seriously enough to contemplate and initiate a number of norm-finding and norm-clarifying processes in various fora. The article then traces how the previously rather unusual phenomenon of unilateral declarations by individual states as to their interpretation of applicable law vis-à-vis cyber conduct has considerably advanced the debate without always sufficiently contributing to creating conditions for consensus (Section 2). On the basis of this overview, the piece zooms in on some of the most relevant points of contention regarding the application and interpretation of central legal concepts to states' cyber operations (Section 3). The concluding section expounds some of the problems of the emerging views not least against the background of Russia's ongoing aggression against Ukraine (Section 4).

2 The Genesis of International Legal Discourse on State Behaviour in Cyberspace

Before it evolved into a general concern deliberated at the highest levels of the United Nations, the project to clarify the application and interpretation of existing international law to state operations in cyberspace was first and foremost an academic endeavour. The ramifications of this chronology continue to reverberate to this very day.

What experts initially sought to call "cyber warfare" first came into focus in 2007, when vital private and public digital infrastructures in Estonia – at that time the most digitally dependent country on earth – came under a wave of sustained distributed denial of service (DDoS) attacks, seriously inhibiting the operations of government, financial, and other services for weeks. The relatively unsophisticated malicious cyber activities came in reaction to the capital city of Tallinn's prior decision to remove a Soviet memorial from its centre. Although Russian authorship or at least intentional toleration by the Kremlin of "patriotic hackers" operating from Russian territory was widely suspected, it could never be conclusively proven. After this first warning that one of the main instruments of economic and financial globalisation might turn into a hazard for digitally transformed societies, it was the discovery of

the "Stuxnet" worm a few years later that really brought home the message that the deployment of code in adversarial computer systems has the potential to inflict considerable physical damage: In a covert operation that lasted for several years, the intelligence services of the United States and Israel had jointly managed to destroy centrifuges in Iranian uranium enrichment facilities by injecting malicious code into the ostensibly hermetically separated internal networks.

Since then, an intermittent series of cybersecurity incidents with varying degrees of severity has reinforced the emerging consensus that the rules of international law ought to have a say in framing such conduct. The first initiative to embark on the mission to sketch out the details was the International Group of Experts convened by the NATO Cooperative Cyber Defence Centre of Excellence, which initially compiled a work addressing cyber operations above the threshold of the use of force with a focus on the law of armed conflict. The result was the Tallinn Manual (Schmitt 2013), published in 2013 and followed up four years later by its much more momentous second iteration. The compendium seeks to provide authoritative guidance – albeit explicitly in an academic, advisory capacity – on the status of customary and conventional international law governing cybersecurity incidents. Substantially, it reaches from the law of state responsibility to questions pertaining to sovereignty and the prohibition of intervention to international human rights law (Schmitt 2017). An unmitigated success from the perspective of its drafters, the Manual has since become the most influential treatise on the law of cyber operations, a development that has led to some more questionable consequences that will be considered further below. The process of drafting the Tallinn Manual 3.0, which will consider emerging state practice and public expressions of *opinio juris*, started in 2021.

On a more official footing, two parallel processes at the United Nations, attempting to find points of legal consensus among states, have been going on for over a decade, with mixed and occasionally contradictory results. The first of the two is the UN Group of Governmental Experts (GGE), initially convened in 2004 with the mandate to "study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security". Its most recent report, result of the GGE's sixth iteration whose work had started in 2019, was adopted in May 2021. The most noteworthy feature of its outcome documents is the politically reasonable yet, from a legal perspective, somewhat confounding insistence on the existence of 13 "norms of responsible state behaviour in cyberspace", first laid down in its 2015 report (UN GGE 2015). These norms accompany the explicit acknowledgment that international law applies to the use by states of information and communications technologies in its entirety. The question whether any of the norms in fact reflect existing international legal obligations – and if so, which ones and in what way – has haunted academic discourse ever since.

The second process under the auspices of the UN is the Open-Ended Working Group (OEWG), which was established through a General Assembly resolution in 2019, initiated by the Russian Federation. Originally conceived as a counterweight to the GGE, which was not only by Moscow perceived as overly dominated by Western powers, and partly a direct response to a failure of reaching consensus within the

GGE in 2017, by 2021 the OEWG had begun to overshadow its older sibling in recognition and influence. This was not least due to its explicit inclusiveness: as opposed to the GGE, the group is open to all UN Member States. The UN General Assembly renewed the OEWG's mandate for the period from 2021 to 2025 in a resolution in December 2020.

Perhaps even more so than the existence of two parallel processes at the United Nations to establish a shared understanding of which international rules are applicable to cyber operations, a real innovation is the quite rapidly growing number of unilateral, public declarations by states as to their own interpretation of the law in the field. To my knowledge, no other context of international relations has ever generated a comparable flurry of activity in foreign ministries across the globe, to the extent that these statements have been referred to as a new type of source for the identification of legal rules (Broeders et al. 2022). Starting with Estonia, the Netherlands, and France in 2019, 25 states had expressed official legal positions on the public record by November 2022, either through statements during deliberations at one of the UN processes or, even more remarkably, as standalone declarations providing more or less elaborate interpretations of the relevant law. Irrespective of the academic question whether such documents should count as expressions of *opino juris* or as instances of practice, rarely ever has international diplomacy witnessed such conscious and deliberate legal positioning outside of the context of treaty-making. Of note is, moreover, the expanding global distribution of states that commit to clear standpoints. While the majority of vocal actors still is European and from the wider Global North, over the past two years more states from other regions have positioned themselves, including Brazil, China, Iran, Kazakhstan, Kenya, and Singapore (Cyber Law Toolkit 2022).

Reading some of the documents by Western states in particular, the Tallinn Manual's considerable and persistent influence instantly catches the eye. Although not at all consistently agreeing and at times explicitly rejecting the International Group of Experts' findings, the level of engagement with a work that strictly speaking cannot claim any authority other than academic merit is conspicuous. And especially with regard to certain pivotal legal doctrines – most importantly the legal character and substance of the notion of sovereignty and to a lesser extent the concept of due diligence – the Manual's contribution facilitated interpretations of the law that had previously been virtually inconceivable. The following section surveys the most consequential of these ongoing normative debates.

3 Normative Debates

The various concurrent norm-finding and -clarifying processes have been primarily revolving around the same set of customary and conventional rules, the most important of which are attribution, the prohibition of the use of force, the principles of non-intervention and sovereignty, states' due diligence obligations, the question of unilateral and collective countermeasures, and the application of international humanitarian law to cyber operations. The most contentious issues in connection with these notions will be addressed in turn.

One of the longest-running debates among states and within academic circles revolves around the vexed problem of attribution, which combines technical and legal aspects that are not always distinguished with sufficient analytic clarity (Rid and Buchanan 2015). In many ways, the legal side of the issue is relatively straightforward. To hold a state accountable for a malicious cybersecurity incident, the operation that caused this incident must be attributed. In accordance with the Articles on State Responsibility (ASR), which are not a multilateral treaty but generally taken to more or less reflect customary international law, a state is principally responsible for the conduct of its own organs. Activities carried out by non-state actors, on the other hand, can only be attributed to a state if they are "in fact acting on the instructions of, or under the direction or control of" the state (Art. 8 ASR). While there remain some contentious questions as to the required degree of control, a much bigger issue is not attribution in the legal sense but what in the literature is often still confusingly called "technical attribution". For the rules of the ASR to come into play in the first place, both the system from which the adversarial cyber operation had been launched and the individual executing the operation need to be identified; the former is usually imperative to determine the location of origin, the latter required to assess the actor's status in relation to a state.

Although states have made much progress in their technical abilities to track the source of a malicious cyber operation, and public statements of official attribution are becoming increasingly frequent and confident, given the fundamental principles of computer code and the ways in which the global network infrastructures are set up, pulling off secret activities in cyberspace while retaining at least plausible deniability remains possible for reasonably sophisticated actors. From a legal perspective, when a state seeks to attribute a cybersecurity incident to an adversary – for example in order to justify the imposing of sanctions or other unilateral countermeasures – the attribution problem therefore mainly concerns the question of the degree of evidence necessary for a state to discharge its burden of proof in this respect. Strikingly, while states by and large acknowledge that the legal operation of attribution indeed requires evidence to be legally sound, quite a few have declared that, as formulated for instance by Germany, "there is no general obligation under international law as it currently stands to publicize a decision on attribution and to provide or to submit for public scrutiny detailed evidence on which an attribution is based", and that "[a]ny such publication in a particular case is generally based on political considerations and does not create legal obligations for the State under international law" (Auswärtiges Amt 2021). Perhaps reasonable from a political standpoint and in order to not be legally obliged to disclose intelligence sources and methods, this widespread stance should nonetheless be viewed critically out of considerations for the international rule of law.

As to the substantive rules that govern inter-state cyber conduct, early discussions put a heavy focus on the question of whether and if yes, under what circumstances a cyber operation might cross the threshold to a use of force within the ambit of Art. 2(4) of the UN Charter, arguably the core of the modern international legal order. Since then, however, the debate has lost much of its steam, mainly for two reasons. For one, there now seems to be an emerging consensus holding that the decisive consideration is "whether the activity's scale and effects are comparable to traditional

kinetic operations that rise to the level of the use of force under international law" (Australian Government 2020). Furthermore, with the possible exception of Stuxnet, to date states' cyber activities have generally remained well below this threshold, rarely if ever causing tangible physical damage. The understanding that an actual, highly destructive "cyber war" will probably not take place (Rid 2018) produced a broader shift in the legal discourse on cyber operations, paying more attention to the much more prevalent "low-intensity cyber operations" (Watts 2015) instead of cyber conduct as a form of force.

The rule of non-intervention prohibits states from interfering by coercive means in internal or external affairs of other states in which these may decide freely. As the International Court of Justice held in its Nicaragua decision in 1986, coercion "forms the very essence of" the prohibition of intervention (International Court of Justice 1986, p. 108). Yet despite decades of practice, no generally accepted definition of the notion has emerged. The legal experts drafting the Tallinn Manual 2.0 identified a rather high threshold, arguing that the cyber conduct in question "must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take)" (Schmitt 2017, pp. 318–319). While some states such as the Netherlands agree with this position (Kingdom of the Netherlands 2019), others, for example Australia (Australian Government 2020) or New Zealand (New Zealand 2020), deem "more subtle and indirect forms of behaviour" sufficient that do not necessarily deploy dictatorial means but merely effectively deprive the target state of control over matters within its *domaine reservé* (Moynihan 2021, p. 403).

Either way, it seems obvious that the requirement of coercion for the rule of the prohibition of intervention to be engaged leaves out a great deal of potentially harmful adversarial cyber activities. In response to this ostensible gap in the law, the Tallinn Manual scholars developed a doctrinal theory of sovereignty that to this day has been exerting an outsized influence on the legal discourse. In fact, it seems safe to say that the whole current shape of the debate would not be conceivable without the experts' seminal contribution. Generally speaking, sovereignty is one of the core principles of international law that, according to the famous Island of Palmas arbitral award, "in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State" (Permanent Court of Arbitration 1928). Although the UN GGE had acknowledged in its 2015 report that "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities" (UN GGE 2015), the Tallinn Manual took the concept a step further by "discovering" in past international practice that sovereignty was not simply a foundational principle of international law but also functions as a standalone rule that may be violated in itself, triggering the international responsibility of the offending state (Schmitt 2017, p. 17).

Despite the experts' contention that this understanding of sovereignty followed from a precise interpretation of existing law and did not in any way amount to a proposal as to its progressive development, the concept had at least never explicitly been framed in this way before. Either way, this "rule of sovereignty" indeed appeared suitable to proscribe malicious state behaviour in cyberspace that did not

reach the thresholds of either force or coercion as long as it amounts to a significant "infringement upon the target State's territorial integrity" or constitutes "an interference with or usurpation of inherently government functions" (Schmitt 2017, p. 20). As this extensive understanding of the protective scope of sovereignty would restrict many forms of malicious state conduct, it is not surprising that in their official statements, a growing number of states have endorsed the Manual's view, among them Austria, the Czech Republic, Finland, France, Germany, Italy, the Netherlands, Norway, Romania, Sweden, but also the Islamic Republic of Iran – often citing the experts' findings verbatim (Cyber Law Toolkit 2022). While other states such as the United States and Israel have been more reluctant, today only the United Kingdom remains steadfast in its rejection of the conception of sovereignty as a primary rule of international law, insisting on its status as a principle (Braverman 2022).

Given these unambiguous declarations of legal positioning, the development clearly points to an emerging general acknowledgment of this very broad understanding of sovereignty in the digital age. As I have argued elsewhere, one obvious yet largely neglected ramification is that it directly plays into the hands of some authoritarian actors, among them the Russian Federation and China. For a long time, these states have been advocating for a strict understanding of sovereignty in cyberspace, primarily to obtain legal arguments that support a repudiation of any type of political meddling in their internal digital policies directed against fundamental rights such as the freedom of expression or freedom of information online, in the service of regime stability. In this light, the attempt to reinterpret the principle of sovereignty as a primary rule is not without a cost, as it enables these authoritarian actors to co-opt the sovereignty discourse to further their interests, a tactic that has already been on display at the UN OEWG (Lahmann 2021).

Closely connected to sovereignty is the question of due diligence. The general idea that from a state's right to exercise authority over persons and entities within the bounds of its own territory it follows that it has a corresponding duty not to allow it to be used for activities that are harmful to other states had been recognised for a long time. As the International Court of Justice famously formulated in its Corfu Channel decision, every state is under an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States" (International Court of Justice 1949, p. 22). Despite persuasive accounts in the literature that such a legal obligation indeed exists and thus naturally extends to states' behaviour in cyberspace (Coco and Souza Dias 2021), there remains some doubt among states as to the legal quality of the concept. Strikingly, while including due diligence in its 2015 report, the UN GGE framed it as a non-mandatory principle instead of a binding rule (UN GGE 2015). A couple of states have nevertheless since acknowledged the compulsory character of due diligence in their national statements. Substantially, due diligence does not imply an obligation to actually successfully prevent malicious cyber activity originating from a state's own territory, as this could only be achieved, if at all, by employing highly problematic means, such as constant monitoring of domestic networks. Instead, there should be certain measures in place, for example laws criminalizing cybercrime, and a state has a duty to do everything feasible to avert transboundary harm once it has actual or constructive knowledge of imminent or ongoing malicious activity.

Further controversial subjects worthy of note concern the issue of collective countermeasures and some legal concepts of international humanitarian law. There is little doubt that a state has the right to respond to malicious cyber activity by imposing countermeasures, that is acts that would otherwise be unlawful under international law, provided attribution of the activity to the state against which the measures are directed is successful and the injured state can prove that the latter bears responsibility. A different and more controversial question is whether a third state may engage in countermeasures of its own with the aim of assisting the injured state. Since the President of Estonia came out in favour of that position at a conference speech in 2019, arguing that "[i]nternational security and the rules-based international order have long benefitted from collective efforts to stop the violations" (Kaljulaid 2019), the matter has gained some traction in academic debates. Among states, New Zealand has cautiously endorsed Estonia's view in light of "the potential asymmetry between malicious and victim states" (New Zealand 2020), with which the United Kingdom generally seems to agree (Braverman 2022), while both France and Canada have rejected the concept due to a lack of uniform state practice in this regard, which would be necessary for the formation of a customary rule (Government of Canada 2022).

Finally, states' cyber activities pose additional and unique challenges to the application of international humanitarian law, that is the customary and conventional rules applicable to situations of international or non-international armed conflict. Given that some of the existing rules have their origin in debates surrounding 19th century warfare, it should come as no surprise that the emergence and adoption by states of digital technologies in their armed forces does not always lead to a frictionless adaptation of the legal frameworks. Some of the persisting discussions concern the notion of "attack" under international humanitarian law and whether and under what conditions cyber operations qualify as such, which is highly relevant insofar as the principal rules on targeting with the objective to protect civilians and other non-military persons and objects are contingent on the existence of an attack in this sense. Another ongoing debate, which is partly based on notional misconceptions (Geiss and Lahmann 2021), revolves around the question whether data can be considered an "object" for the purposes of the law, as only civilian objects are covered by the prohibition of attacks (Mačák 2015).

4 Challenges and Outlook

This brief analysis has attempted to provide an overview of the most important contentious legal issues as to the application of international law to cyberspace. Apart from these more narrowly framed doctrinal matters, more general concerns remain. For one, the early and purportedly comprehensive contribution of the International Group of Experts that drafted the first two iterations of the Tallinn Manual shaped the entire subsequent legal discourse to a degree that raises questions of its formal position and legitimacy within a larger nexus of "state-academic lawmaking" (Hughes and Shereshevsky 2022). What is more, the Manual's initial emphasis on the use of force framed the subject matter of state activities "in cyberspace" in mil-

itary terms from the beginning. That the militarisation of the cyber norms discourse is so firmly entrenched today is at least partly attributable to this original decision.

At the same time, Russia's renewed aggression against Ukraine since February 2022 has cast doubt on some received wisdom regarding the future significance of cyber tools within the context of traditional armed conflict. Although the jury is still out as to the actual quality and impact of Russian cyber operations to pursue its war objectives in Ukraine (Willett 2022; Greenberg 2022), a sober assessment of the role of cyber operations will likely entail a re-evaluation of the way in which states think about the applicable rules of international law as well. One intriguing but so far largely unaddressed question that has come up since the onset of the invasion is the precise interpretation of due diligence: considering the activities of Ukraine's "IT Army", which comprises many volunteer hackers that engage in offensive cyber activities against Russia from the territory of third countries, do the latter have any positive legal obligations to try to prevent them from doing so, or can their persistent inactivity perhaps be justified in light of the larger context that these adversarial acts are embedded in? Is it true that "the West is now throwing overboard the legal and normative interpretations it has championed in cyberspace over the past decade for the sake of politically supporting Ukraine" (Soesanto 2022), or should we instead rather advance a more nuanced understanding of those norms?

An international treaty to govern state behaviour in cyberspace is not forthcoming. For the immediate future, the most relevant formal forum for the indispensable processes of norm finding and clarification is therefore set to be the UN OEWG. In the aftermath of Russia's war in Ukraine, however, further polarisation among participants should be expected, with possibly another complete breakdown of proceedings; tangible progress is even more in doubt than before. This development implies that state practice and official declarations of legal positioning will likely only gain in significance. In this context, there are pressing questions as to the implications of significant divergences between stated *opinio juris* and (covert) conduct (Perina 2015), which has recently been pointed out by the example of France (Kenny 2021), and of the legal salience of the continuing silence of the majority of states (Hollis and Sander 2022), in particular among those from the Global South. Despite seemingly impressive normative development over the past one and a half decades, the law on cyber conduct is still in its infancy.

Funding Open access funding provided by Leiden University.

References

Australian Government (2020). Annex B: Australia's position on how international law applies to state conduct in cyberspace. https://www.internationalcybertech.gov.au/our-work/annexes/annex-b. Accessed 15 Dec 2022.

Auswärtiges Amt (2021). On the application of international law in cyberspace: position paper. https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf. Accessed 15 Dec 2022.

Braverman, S. (2022, 19 May). International law future frontiers. https://www.gov.uk/government/speeches/international-law-in-future-frontiers. Accessed 20 Nov 2022.

Broeders, D., Busser, E. de, Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand? *Journal of Cyber Policy*, *7*(1), 97–135.

Coco, A., & Souza Dias, T. de (2021). 'Cyber due diligence': a patchwork of protective obligations in international law. *European Journal of International Law*, *32*(3), 771–806.

Cyber Law Toolkit (2022). National positions. https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions. Accessed 20 Nov 2022.

Geiss, R., & Lahmann, H. (2021). Protection of data in armed conflict. *International Law Studies*, *97*, 556–572.

Government of Canada (2022). International law applicable in cyberspace. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng. Accessed 20 Nov 2022.

Greenberg, A. (2022, 10 Nov). Russia's new cyberwarfare in Ukraine is fast, dirty, and relentless. https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/. Accessed 20 Nov 2022.

Hollis, D. B., & Sander, B. (2022). International law and cyberspace: what does state silence say? https://papers.ssrn.com/abstract=4201718. Accessed 20 Nov 2022.

Hughes, D., & Shereshevsky, Y. (2022). State-academic lawmaking. https://papers.ssrn.com/abstract=4210484. Accessed 20 Nov 2022.

International Court of Justice (1949). Corfu channel case, judgment of April 9th, 1949. https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf. Accessed 4 Jan 2023.

International Court of Justice (1986). Case concerning military and paramilitary activities in and against Nicaragua. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf. Accessed 4 Jan 2023.

Kaljulaid, K. (2019, 29 May). International law and cyberspace. https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon. Accessed 20 Nov 2022.

Kenny, J. (2021, 12 Mar). France, cyber operations and sovereignty: the 'purist' approach to sovereignty and contradictory state practice. https://www.lawfareblog.com/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice. Accessed 20 Nov 2022.

Kingdom of the Netherlands (2019). Appendix: International Law in Cyberspace. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace. Accessed 4 Jan 2023.

Lahmann, H. (2021). On the politics and ideologies of the sovereignty discourse in cyberspace. *Duke Journal of Comparative & International Law*, *32*(1), 61–107.

Mačák, K. (2015). Military objectives 2.0: the case for interpreting computer data as objects under international humanitarian law. *Israel Law Review*, *48*(1), 55–80.

Moynihan, H. (2021). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394–410.

New Zealand (2020). The application of international law to state activity in cyberspace. https://dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace. Accessed 4 Jan 2023.

Perina, A. H. (2015). Black holes and open secrets: the impact of covert action on international law. *Columbia Journal of Transnational Law*, *53*(3), 507–583.

Permanent Court of Arbitration (1928). Reports of international arbitral awards. Island of Palmas (Netherlands, USA). https://legal.un.org/riaa/cases/vol_II/829-871.pdf. Accessed 4 Jan 2023.

Rid, T. (2018). Cyber war will not take place. *European Review of International Studies, 5*(1), 131–134.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37.

Schmitt, M. N. (ed.). (2013). *Tallinn Manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Schmitt, M. N. (ed.) (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press.

Soesanto, S. (2022). The IT army of Ukraine: structure, tasking, and eco-system. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf. Accessed 20 Nov 2022.

UN GGE (2015). Group of governmental experts on developments in the field of information and telecommunciations in the context of international security: note / by the Secretary-General. https://digitallibrary.un.org/record/799853. Accessed 21 Dec 2022.

Watts, S. (2015). Low-intensity cyber operations and the principle of non-intervention. In J. D. Ohlin, K. Govern, & C. Finkelstein (eds.), *Cyber war: law and ethics for virtual conflicts* (pp. 249–270). Oxford: Oxford University Press.

Willett, M. (2022, 6 Oct). The cyber dimension of the Russia-Ukraine war. IISS. https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war. Accessed 20 Nov 2022.