Core concerns: the need for a governance framework to protect global internet infrastructure

Broeders, D.W.J.; Sukumar, A.M.

Received: 16 June 2023 | Accepted: 13 November 2023

DOI: 10.1002/poi3.382

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

Core concerns: The need for a governance framework to protect global Internet infrastructure

Dennis Broeders | **Arun Sukumar**

Institute of Security and Global Affairs, Leiden University, Leiden, The Netherlands

Correspondence
Dennis Broeders, Institute of Security and Global Affairs, Leiden University, Leiden, The Netherlands.
Email: d.w.j.broeders@fgga.leidenuniv.nl

Funding information
Ministerie van Buitenlandse Zaken, Grant/Award Number: The Hague Program on International Cyber Security

Abstract

The war in Ukraine has underscored the risks and threats to global Internet infrastructure from geo-politically motivated cyber operations. The Domain Name System and core protocols responsible for the routing, forwarding, and security of Internet traffic have been exploited by actors in Russia and Ukraine for denial-of-service attacks, surveillance, and censorship. Additionally, states have tried to compel organisations that maintain and govern such infrastructure to cut Russia off from the Internet. These cyber operations and sanctions targeting the 'public core of the internet' have serious transboundary effects, and threaten the stability and functionality of the Internet. Most such attacks appear, at the time of writing, to have been buffeted by the internet's resilience, but there is equally the risk that the Ukraine war becomes a permissive, norm-constitutive moment for similar operations in the future targeting its core physical, institutional and logical infrastructure. The technical community, a growing number of states and other stakeholders have been arguing for the protection of the 'public core' of the internet for nearly a decade, anchoring the concept in policy, multistakeholder and diplomatic fora and documents. This paper, while noting that states increasingly acknowledge the need to protect the public core of the internet, argues that norms and international law are still ill-equipped to regulate damaging cyber operations, given unsettled questions regarding the sovereignty of states over global

Internet infrastructure, and the precise scope of their existing international obligations towards its protection.

KEYWORDS

critical information infrastructure, cyber diplomacy, global internet, international law, public core of the internet

INTRODUCTION

In May 2022, the Internet Society (ISOC) published its assessment of the threats faced by 'global Internet infrastructure' on account of the war in Ukraine. Titled '2 Months of War: The Impact on the Internet's Core', the note highlighted cyber operations such as Border Gateway Protocol (BGP) 'hijacks' and Distributed Denial-of-Service (DDoS) attacks by actors in both Ukraine and Russia that weaponized the transport and network layers of the Internet (Internet Society, 2022a). Russia has continually used BGP hijacks as a geopolitical tool, manipulating the Internet's routing tables to direct traffic meant for occupied Ukrainian territories like Crimea and Kherson through its own networks (Burgess, 2022; Douzet et al., 2020). The war in Ukraine has also seen an exponential increase in DDoS attacks that target Domain Name System (DNS) services, and exploit key Internet protocols such as the Transfer Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) (Internet Society, 2022b). Protocols like UDP and ICMP, designed to ensure the fast exchange of data across the Internet, have been exploited by Russian and Ukrainian actors for that very reason to flood networks with data packets, degrading their normal operations or rendering them inaccessible. Early in the Ukraine conflict, a Russian cyber operation targeted satellite infrastructure—Viasat's KA-SAT network—which the United States Secretary of State Antony Blinken condemned as indiscriminate, as the attack was intended 'to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries'. (Pearson, 2022).[1] This attack was also hotly debated in the third session of the Open Ended Working Group (OEWG) in the UN first committee in March 2022, in which the spillover effects of the hack and even the mere possibility of spillover effects were discussed as threats to (cyber) stability in the region.[2] More recently, the (suspected) sabotage of the Nordstream subsea gas pipelines has alerted states to the vulnerability of subsea internet cable infrastructure (Kavanagh, 2023). In October 2023, Finland opened an investigation into a 'suspected sabotage' of its submarine cable connected to Estonia, with sources in Helsinki attributing the sabotage to Russian actors (BBC News, 2023). Within days of Finland's announcement, Sweden too announced that a submarine cable in the Baltic Sea belonging to Swedish telecom operator Arelion had been damaged in proximity to, and around the same time as, the Finland–Estonia cable (Pollard & Kauranen, 2023). These attacks and cyber operations are significant as they target the core logical and physical infrastructure of the global internet. The result is an intensification of protective measures, politicomilitary attention for, and even securitisation of, global physical internet infrastructure (Kavanagh, 2023). While most of these operations did not result in a serious disturbance of the internet, they signal to states (a) that these infrastructures are clearly on the menu in times of conflict and (b) that escalation of operations targeting logical and technical infrastructure of the core internet beyond the original conflict pose a genuine threat to the stability of cyberspace.

Aside from cyber operations targeting global Internet infrastructure, the war in Ukraine has also seen states seeking unilateral restrictions on their use. Several Internet Exchange Points (IXPs) around the world responded to sanctions imposed by the European Union and United Kingdom on Russia by 'de-peering' major Russian ISPs, posing a threat to Internet connectivity by limiting routes available for data packets to transit through networks. Sometimes these decisions were directly related to state sanctions and sanctioned entities (Moss, 2022), but sometimes they were based on corporate weighing of business and network continuity against moral responsibility (Goodin, 2022). Ukraine also called on the Internet Corporation for Assigned Names and Numbers (ICANN) to revoke Russia's country-code Top Level Domains (ccTLD) such as '.ru', and shut down instances of authoritative DNS root servers located in the country (Eamon, 2022). Additionally, Ukraine appealed to RIPE NCC, the Regional Internet Registry for Europe, the Middle East and parts of Central Asia to 'withdraw the right to use IPv4 and IPv6 addresses by all Russian members of the RIPE NCC'.[3] ICANN rejected the request, arguing that 'unilateral action [would have] devastating and permanent effects on the trust and utility' of the Internet (Needleman, 2022), as did RIPE NCC, citing that they do 'not have a mandate to take such actions […] unilaterally' and 'believe that Internet number resource registrations should not be used as a means to enforce political outcomes, and that doing so would have serious implications for the Internet, not just in the Russian Federation but also for the rest of the world'.[4] Meanwhile, Starlink, the private satellite-based internet service provider, was reportedly requested by the Ukrainian government in September 2022 to support an attack on Russia's naval assets in the Crimea (Copp, 2023). The company refused—Starlink was introduced in Ukraine primarily to bolster civilian internet access following the invasion—but Ukrainian intelligence services have candidly acknowledged its deployment and 'significant use' in the war's frontlines (Pennington & Lyngaas, 2023). The use of this satellite service raises the thorny question of whether such private infrastructure would be fair game during hostilities.

These targeted operations and sanctions on shared, critical Internet resources—which can be called the 'public core' of the Internet—challenge the narrative that cyber-attacks have played a subdued role during the war in Ukraine.[5] BGP hijacks, DNS-enabled DDoS attacks, attacks on satellite infrastructure, and sanctions on IXPs are all part of the playbook of cyber conflict. Politically, the war in Ukraine lends urgency to the protection of global Internet infrastructure, as it reveals the increasing propensity of state actors to target critical information infrastructure with sometimes serious transnational risks and consequences. The technical community, a growing number of states, and other stakeholders have been arguing in favour of the protection of the 'public core' of the internet for nearly a decade, and have anchored the concept in policy, multistakeholder and diplomatic fora and documents. Some protection will result from technical solutions to public core vulnerabilities as internet corporations and internet standards bodies, alongside the broader technical community, continue to solve problems, patch vulnerabilities and increase redundancy in the internet's ecosystem. However, if the main threat to the public core comes from state actors, the problem is as much political as it is technical. The conflict in Ukraine, even if it has not resulted in widespread or sustained internet outages, is an important norm-constitutive moment for public core protections. If the aforementioned instances of attacks on core infrastructure are left unaddressed by states in diplomatic-political fora, that could signal a permissive attitude towards similar attacks in the future. Whether or not cyber attacks in the future will impact the availability of the internet is an open question. However, as Cloudflare, an influential actor in providing global DNS services has noted, Ukraine's internet resilience is owed largely to its 'widespread connectivity to outside networks' and unusually high number of IXPs (The Cloudflare Blog, 2023). Would other states embroiled in a future conflict, especially not so well-connected countries, be similarly resilient?

Given the history of UN cyber negotiations, states are not likely to wait to find out the answer. As transnational critical information infrastructure has become an international security issue, states have already turned to diplomatic processes to discuss constraints on state behaviour. The main discussion forum for these issues at the international level has been the UN General Assembly's first committee which puts this debate firmly in the key of international peace and security. This diplomatic tradition focuses on security threats which are often in the category of 'high impact, low probability', meaning that the fact that the world has not yet seen a cyber-attack that destabilises the internet, does not mean that it is out of bounds for their discussions. The fact that the first substantive sections of the 2021 GGE and OEWG reports are called 'Existing and *emerging* threats' and 'Existing and *potential* threats', respectively (emphasis added) is indicative of the Committee's approach.[6] This paper argues that in spite of concerted efforts to raise awareness on the issue in policy, legal and diplomatic circles, states have limited normative and legal tools to address threats to the Internet's public core, falling as the issue does within a 'grey zone' (Schmitt, 2017b) of international law. Given that states will continue to target transnational critical information infrastructure, we argue that states should increase their efforts to provide legal and normative guardrails to prevent cyber conflict from escalating in this domain. The paper is organised into five sections. The section on 'Threats to the Public Core of the Internet' offers an overview of threats to the public core of Internet, which have risen in severity and sophistication in just a few years. The section on 'Growing Recognition of the Need to Protect Global Internet Infrastructure' highlights the efforts by state and private stakeholders to articulate public core protections, mainly in the form of negotiated norms of responsible state behaviour but also through public policy pronouncements. The section on 'The Limits of International Law' lays out the challenges states face in applying existing international law to public core protections. The final section presents the paper's conclusions.

THREATS TO THE PUBLIC CORE OF THE INTERNET[7]

The public core of the internet services critical functions—routing, naming, numbering and cryptography—that ensure the smooth functioning of the Internet. These functions are engrained in three layers: physical infrastructure responsible for the seamless flow of Internet traffic; technical infrastructure and protocols that determine how data flows ('logical' layer), and the organisational layer of entities that govern such shared infrastructure (see Broeders, 2017, 2021; Global Commission on the Stability of Cyberspace [GCSC], 2018, 2019). Public core infrastructure may be targeted directly through cyber operations or indirectly through coercive political measures on their governing organisations (e.g., sanctions). As the previous section highlighted, both parties to the Ukraine conflict have targeted core Internet protocols and architecture—such as BGP and DNS—and Internet organisations such as IXPs for strategic advantage. The aim is to degrade each other's information infrastructure, but the risk of spillover beyond the zone of conflict is considerable. Russian cyber aggression towards Ukraine already gave the world NotPetya, among the most viral and indiscriminate cyber operations to date, that spread far beyond the zone of conflict (Kaminska, et al., 2021). It is plausible that continuing attacks on the public core by state and nonstate actors in Russia and Ukraine could have transnational effects. At the very least, the war emboldens other states to similarly target the public core through cyber operations and sanctions, jeopardising the stability of the Internet.

The easy-to-adopt and interoperable character of *core Internet protocols* makes them attractive tools for targeted cyber operations. DNS and BGP are the two main inroads for malicious behaviour. Pakistan's blocking of YouTube in 2008 is an early reminder of the vulnerability of the BGP system. The change Pakistan Telecom made to the routing

protocol—in response to a Ministry of Information order to block YouTube in Pakistan—was broadcast and adopted globally, causing YouTube to become inaccessible across the entire Internet (RIPE Network Coordination Centre, 2008). This shows just how tightly interwoven the Internet is through its core protocols, and how vulnerable those protocols are to national actions (Douzet et al., 2020). BGP hijacks have become more common in recent years. As there is no hierarchy between the BGP speaking routers, updates by a single BGP speaker can impact routing information for the entire Internet. While most routing incidents are caused by erroneous configuration, there are well-known cases where this has been caused by actors with criminal or political intentions (Steenman, 2020). For example, ISPs in Myanmar attempted to hijack Twitter routes in February 2021, in response to the Myanmar Army's order to block the platform during its coup against the elected government (Siddiqui, 2021). DNS hijacking, which refers to the manipulation of DNS records and certificate details of websites, has also been used more recently to target government agencies and companies to gather intelligence (Hirani et al., 2019). Rerouting of traffic through the ISPs of different countries can be used for mass surveillance and intelligence gathering, and potentially for sabotage. In a more general sense, they undermine trust in the integrity and trustworthiness of the Internet.

A less sophisticated approach to taking down the Internet was through the 2016 DDoS attacks on Dyn, a US-based DNS provider (Schneier, 2016). The Mirai botnet knocked Dyn offline, severely disrupting a number of services that relied on Dyn, including some large platforms such as Amazon, Slack, and Netflix. With more platforms relying on DNS services like Dyn, the effects of such attacks are highly likely to be transnational.

The war in Ukraine indicates that operations targeting core Internet infrastructure are increasingly becoming a part of the 'cyber' playbook during conflicts. To circumvent sanctions imposed against it, Russia created its own 'trusted certificate authority' to enable third parties to access Russian websites and services. However, it is widely suspected that the certification process—which involves a cryptographic handshake between the user and service through the transport layer security (TLS) protocol—will be exploited by Russia for Man-in-the-Middle attacks for espionage or data destruction (CPO Magazine, 2022). The exploitation of core protocols, which connect networks and infrastructure around the world, present a threat to the stability and the integrity of the Internet.

The public core's *physical infrastructure* is also vulnerable. Foremost, the submarine cable infrastructure connecting the continents and larger IXPs that constitute the central nervous system of the Internet, are vulnerable to disruption (Bueger & Liebetrau, 2021; Kavanagh, 2023). Cable cuts are usually the result of ship anchors or geological events (Qiu, 2022), but the potential for sabotage, as the aforementioned incidents in recent years has shown, is great and has begun to worry states. Recently, NATO announced the creation of a Critical Undersea Infrastructure Coordination Cell at NATO Headquarters[8] and the European Commission wants to help invest in 'cable projects of European interest' that would reduce its reliance on too few undersea internet connections and make it less vulnerable to sabotage (Pollet, 2023). When it comes to undersea cables there is increased redundancy in the 'technical sense', thanks to the number of cables, but there are political problems with countries not wanting to be dependent on Chinese cable infrastructure and worries about the (im)possibility to effectively protect this infrastructure. As discussed in the introduction, the Russian cyber operation that targeted the Viasat's KA-SAT network also raised concerns about the vulnerability of critical technical infrastructure, with US Secretary of State Antony Blinken highlighting the indiscriminate nature of the attack and condemning its 'spillover impacts on other European countries'. (Pearson, 2022).

Lastly, some of the *organisations* that manage or govern core Internet resources are also vulnerable to attack or risk becoming part of international conflict through coercive political measures, as is happening now in the Ukraine conflict. Compelling organisations such as

ICANN (US) or RIPE-NCC (NL) to comply with sanctions and cut off Russia from Internet resources, as the Ukrainian government has sought, would have effects beyond Russia (the central Asian countries are, for example, highly dependent on Russia for Internet routing). ICANN and RIPE NCC—though sympathetic to the Ukrainian cause—refused to disconnect Russia from the global Internet infrastructure, noting 'that using [core Internet organisations] as a means to enforce political outcomes […] would have serious implications for the Internet, not just in the Russian Federation but also for the rest of the world' (RIPE Network Coordination Centre, 2022). However, organisations that administer core internet resources such as domain names and IP addresses, may still be affected directly or indirectly through cyber sanctions and/or economic sanctions, resulting in gaps in the provision and availability of the internet (Badiei, 2023). Conversely, such organisations may also interpret and apply sanctions too broadly or choose sides in a conflict and act accordingly. Large internet companies such as Microsoft and Amazon and threat intel companies such as ESET have clearly chosen sides in the Ukraine conflict to the point that analysts are starting to wonder about their combatant status under international humanitarian law (van Benthem, 2023). While the technical/multistakeholder community generally errs on the side of global connectivity, even in this community there has been some debate about how—rather than if—internet organisations should comply with sanctions.[9]

GROWING RECOGNITION OF THE NEED TO PROTECT GLOBAL INTERNET INFRASTRUCTURE

The need to protect the public core of the Internet was highlighted in the recent reports of two intergovernmental groups—the 2019–2021 UN Group of Governmental Experts (GGE) and the 2019–2021 UN Open-Ended Working Group (OEWG) on cyber security—both of which were adopted by consensus.[10] Between 2018 and 2021, there were two parallel UN processes that deliberated rules and norms of responsible state behaviour in cyberspace. While the UN GGE comprised 25 states, the OEWG was open to all UN member states. Notably, the consensus reports of both groups linked the protection of the public core to existing norms on the protection of critical infrastructure. In the OEWG report, states agreed '[…] on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, *along with endeavouring to ensure the general availability and integrity of the Internet*' (emphasis added).[11] The UN GGE report underlined that such infrastructure is transnational, and goes beyond the protection of national critical infrastructure to include such infrastructure that 'provides services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet'.[12] Ever since the UN GGE in 2015 called on states to not attack or knowingly allow malicious cyber operations from their territory on critical infrastructure, negotiators have jealously guarded the designation of infrastructure as 'critical' as a sovereign prerogative. In that sense, the development of the norm on the protection of the public core of the internet is as much story of dissemination of the norm as of its contestation, and both are still in play.[13] The public core has both 'norm entrepreneurs' and 'norm anti-preneurs' behind its development (Bloomfield, 2016). Nevertheless, the acknowledgement by both UN groups of the fact that the protection of public core infrastructure is a shared, global concern and different from securing national infrastructure is an important first step.

With the adoption of these reports, the issue of protecting the public core has been placed within the ambit of the UN General Assembly's First Committee on Disarmament and International Security, and states will need to elaborate the precise scope and application of such protections. The concept of the public core has gained acceptance since 2015, and

some of its history may speak to interpretations of its content and to growing state and nonstate support.

The call to protect the public core of the Internet was originally formulated by the Netherlands Scientific Council for Government Policy in 2015 as a norm of restraint for states. The aim of the norm was to protect the Internet as a global public good, by establishing and disseminating an international standard stipulating that the Internet's public core – its main protocols and infrastructure—must be safeguarded against unwarranted intervention by governments (Broeders, 2015). Both states and non-state actors have subsequently deliberated the concept at length, specifically developing proposals for state behaviour on the protection of the public core. The Netherlands addressed the protection of the public core of the Internet in its 2017 *International Cyber Strategy*[14] and in the same year, the multi-stakeholder (GCSC, 2017 published a norm on the issue. The commission called on state and non-state actors to 'neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace' (GCSC, 2017). The norm highlights 'intentional and substantial damage' to the public core, acknowledging that many states will allow military and intelligence operations that (mis)use public core protocols and infrastructure, while disallowing substantial damage with intended or unintended transnational effects. Since 2017, this norm has found wide support from states. In 2018, it was absorbed into the *Paris Call for Trust and Security in Cyberspace*, a multi-stakeholder initiative championed by the French government (France Diplomacy—Ministry for Europe and Foreign Affairs, 2021). While nonbinding in character, the Paris Call has, at the time of writing, been endorsed by 81 states, with the United States joining in November 2021. The 'public core' concept has become part of the *EU Cyber Security Act*, which gives ENISA—the European Union Agency for Cybersecurity—the responsibility to '[…] support the security of the public core of the open Internet and the stability of its functioning' (European Commission, 2020). In 2022, the European Union updated the Network and Information Systems Directive (NIS2), reiterating its support for the protection of the public core. The directive underlines the cross-border nature of both critical infrastructure and cyber-attacks and urges member states to adopt policies that sustain 'the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables'.[15] In April 2022, the US-sponsored *Declaration for the Future of the Internet*[16] called on states to 'refrain from undermining technical infrastructure essential to the general availability and integrity of the Internet'. The Declaration has been signed by over 65 states, indicating that state support for protecting the public core continues to grow.

However, the norm on the protection of the public core of the internet has also become part of the tug of war in the UNGA first committee debates about cyber security between the 'likeminded' states—a loose coalition of states led by the United States—and states like Russia and China that are arguing for an internet made up of cyber-sovereign states.[17] Russia circulated a proposal in the ITU in 2021 using the language of the public core of the internet to argue in favour of an international cyber treaty—a long standing wish of the Russian Federation—that would transfer the administration of critical internet resources from the current multistakeholder model to an intergovernmental model. The proposal[18] puts states at the centre of internet governance—'it is the states that must act as guarantors of the stability and integrity of the Internet's public core'—while the original thinking on the public core is built on a negative norm of *restraint* for states and underlines the importance of the multistakeholder model. Similarly, Chinese scholars have grasped the ambiguity of the concept to (re)interpret the public core, 'moving the norm beyond its infrastructure security to a state security goal' that is firmly embedded in the Chinese thinking on cyber sovereignty (Fung, 2022). Being able to agree on shared language when divisions between the main

state powers are as deep as they currently are, is testimony to the strength of the UN process, as norms scholars such as Maurer (2020), Levinson (2021) and Raymond (2021) have underscored. However, even the shared language leaves ample room for contestation and interpretation of that language which many norms scholars increasingly see as the new normal of international diplomatic cyber negotiations (Kurowska, 2019; Wiener, 2014).

In other words, despite the spread of the norm, a common understanding of it—and the protection that this would support—is not a done deal. The debate within the group in the 2019–2021 UN OEWG on how to classify public core infrastructure in the OEWG report underlines this point. The OEWG predraft report suggested, on the recommendation of Singapore, the term 'supranational' to describe public core infrastructure, thus highlighting it as a 'special category of critical infrastructure, whose protection was the shared responsibility of all states' (Broeders, 2021). However, the United States, Estonia, France, and Japan rejected the use of this term, as supranational suggests a higher level of authority than the national, highlighting that such infrastructure is ultimately territorial and within the jurisdiction of respective states on which it is located. The group was able to resolve internal differences and propose language on public core protections that was ultimately adopted in the final OEWG report. Emphasising the need to protect the public core was an important first step, but equally important is addressing the extent to which states can and cannot assert their jurisdictional claims to such infrastructure.

THE LIMITS OF INTERNATIONAL LAW

Despite growing acknowledgement of the need to protect public core infrastructure at the level of international diplomatic norms, it is unclear whether such infrastructure enjoys protection under existing international law, and consequently, what measures are available to states to prevent or respond to malicious cyber operations that target it. The state- and sovereignty-centric approach of international law means that the legality of cyber operations is evaluated mostly on the basis of their territorial effects, that is, whether such operations have harmed individuals or infrastructure within a state's territory or impaired the exercise of its sovereign functions. In other words, cyber operations that target public core infrastructure are not per se unlawful, but attacks that implicate such infrastructure and result in serious territorial effects could potentially violate international law. In this section, we present a number of scenarios where targeting public core infrastructure could lead to responsibility on the part of the perpetrator state. This section first outlines scenarios where cyber operations conducted during peacetime that could fall foul of international law, and subsequently address the targeting of public core infrastructure during war.

Consider the prohibition on the threat or use of force in international relations, which is a customary rule of international law that has been codified under Article 2(4) of the UN Charter. A cyber operation by a state can certainly be considered forceful, depending on the scale of damage and (physical) effects it manifests in another state's territory (Eichensehr, 2022).[19] It is conceivable that cyber operations by states which destabilise or disrupt the functioning of core infrastructure such as DNS could result in serious, even catastrophic damage to critical services that run on them. Should such damage extend to loss of life or widespread damage to property, they would arguably constitute a use of force by that state. If such consequences have thus far not materialised, it is because cyber operations that use DNS infrastructure as attack surfaces are often buffeted by the redundancy built into the public core. For instance, the 2013 Spamhaus DDoS attack, which targeted four major IXPs, caused global Internet traffic to slow down but did not create major disruptions because traffic could still be routed around affected servers (The Cloudflare Blog, 2013). Nevertheless, with more applications and critical infrastructure services—especially those that rely on Internet of Things (IoT)

devices—increasingly dependent on efficient DNS functions such as routing, even momentary disruptions of public core infrastructure could harm the smooth functioning of healthcare services, transport grids, or industrial control systems, leading to loss of life or property (Microsoft, 2022). Such operations against public core infrastructure, if executed or sponsored by a state, could result in its violation of the rule against the use of force.

Cyber operations need not arise to the level of a 'use of force' to be wrongful under international law. There are some 'below the threshold' scenarios where attacks on public core infrastructure could lead to state responsibility for wrongful acts. First, take the rule of nonintervention in international law, that requires states not to intervene in matters that are the remit of another. Would cyber attacks on public core infrastructure located in another state, such as DNS servers or IXPs, constitute a violation of this rule? This is a complex issue to address. Two elements are key to evaluating the wrongful nature of an intervention[20]: first, the cyber operation should have targeted 'matters, which each state is permitted, by the principle of sovereignty, *to decide freely*' (emphasis added), and second, it must involve coercion. In other words, only coercive interventions in activities that are considered the *domaine réservé* of other states are prohibited.

The public core is critical to the global Internet's functionality, but its components—IXPs and Regional Internet Registries, certificate authorities, DNS servers, standard-setting organisations, and so on—are distributed across states. For example, ICANN develops policies for the DNS as a whole, but as a US-based nonprofit organisation, it is answerable to laws of the United States and those of California, its state of incorporation. However, the territoriality of public core infrastructure or organisations does not necessarily render their activities within the *domaine réservé* of states (Helal, 2019). State practice supports the view that the governance of public core infrastructure is beyond the purview of any single state. At the 2012 World Conference on International Telecommunications in Dubai, a number of key states rejected or expressed reservations against International Telecommunications Regulations (ITR) that specifically recognised the right of states to determine international routing, allocate numbering resources, and 'authorize' providers of international telecommunications services (Fidler, 2013). Similarly, the US government's decision to transfer its oversight of key Internet numbering and naming functions to the 'global, multistakeholder community'—the so-called 'IANA transition' which was endorsed by most states—was both in defiance of calls for greater state control over critical Internet resources and in response to perceived US control over those resources (see Raustiala, 2023). Public core infrastructure exists to support global Internet governance, which cannot be the *domaine réservé* of any single state. The 2019 EU Cybersecurity Act declares the public core of the Internet to be a 'global, public good'.[21] While states retain the prerogative to set Internet policies for their territory, the use or manipulation of public core infrastructure for data localisation or surveillance, and for other purposes not regulated by international law such as espionage, has invited criticism by states (Cybersecurity and Infrastructure Security Agency, 2019; KrebsonSecurity, 2019). Even in relation to ccTLDs such as '.us', which correspond unambiguously to the 'territory' of a state, 'sovereignty claims' on the delegation and administration of those domains are contested (Mueller & Badiei, 2017).

Whether the targeting of public core infrastructure located in the territory of another state constitutes a violation of the nonintervention rule is therefore an open question. However, where cyber operations attempt to disrupt activities that fall within the *domaine réservé* of a state, the use of public core infrastructure to execute such attacks arguably highlights the coercive intent of the perpetrator state. At the time of writing, states and legal scholars differ in their views towards coercion in cyberspace: some states and scholars consider cyber operations to be coercive only when those operations influence the outcome of *domaine réservé* activities, such as the conduct of elections (Pijpers, 2023; Schmitt, 2017a).[22] Others seek an expansive interpretation of coercion, arguing that the very fact of targeting certain

activities or sectors that are critical to a country—for example, the health or energy sectors—would constitute coercive behaviour (Braverman, 2022; Helal, 2019; Kilovaty, 2021). In this context, the disruption of *domaine réservé* activities through attacks on supporting public core infrastructure would be a significant factor in ascertaining the coercive character of cyber operations. Targeting critical services through DNS flood attacks or BGP hijacks arguably raise a strong presumption about the coercive intent of the perpetrator state, given the possibility of widespread and significant disruption of those services. For example, some countries allow their diaspora to vote via the Internet. Through a BGP hijack, Country X could reroute traffic meant for the e-voting system of Country Y (Krähenbühl et al., 2022). Country X's actions would arguably constitute coercive intervention, because the scale and significance of disruption caused through such the BGP hijack is not only foreseeable, but also because it raises the possibility that election returns filed from abroad may have been tampered with or manipulated in some manner.

The framework of state responsibility—codified in the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)—is similarly ambiguous on the wrongfulness of cyber operations that target the public core. The intention of a state does not in any way mitigate the internationally wrongful nature of its actions, and consequently, its international responsibility.[23] Therefore, the targeting of say, DNS infrastructure or the exploitation of BGP by states for domestic surveillance could potentially lead to their international responsibility if such operations impair the general availability and integrity of the Internet. However, the operative question is whether such a primary obligation to protect the Internet's seamless functioning exists in the first place. While the public core is shared among states and critical to the overall functioning of the Internet, it would be difficult to claim at the time of writing that there exists a collective, *erga omnes* obligation towards its protection (Roguski, 2020).[24] The widespread acceptance of the norm to protect the general availability and integrity of the Internet is indicative of *opinio juris*, but whether the norm will crystallise into an obligation depends ultimately on the practice of states, including the signing of bilateral and plurilateral agreements to collectively secure the public core. The value of the norm so far is political, but not legal.

Related to this question is whether states have a due diligence obligation to prevent or stop cyber operations targeting public core infrastructure on their territory. While several states have adopted the view that there exists such an obligation, many major powers have expressed their reservations against a 'cyber due diligence' rule. In particular, the Five Eyes countries—whose cooperation and capacity-building assistance will be essential to any global monitoring or surveillance effort against malicious, transboundary cyber operations—have been very cautious in endorsing this principle (Cyber Law Toolkit, n.d.). At the time of writing, the United States, United Kingdom, and New Zealand contest the existence of a cyber due diligence rule, while Australia and Canada prefer a case-to-case assessment of any obligation to stop malicious attacks. A due diligence obligation to monitor harmful cyber operations emanating from or transiting through a state's territory may be helpful in mitigating some threats to public core infrastructure, but the application of such a 'rule' also carries some risks. Specifically, the due diligence obligation may lead to a hardening of sovereignty claims by states over territorial public core infrastructure. Due diligence obligations are generally considered to flow from the principle of sovereignty: the idea here is that states have sovereign control over infrastructure within their territory, and hence must exercise diligence to ensure those objects are not used to cause harm to other states (Coco & de Souza Dias, 2021; Schmitt, 2017a, 2017b).

It is also important to address whether injured states can undertake operations targeting the public core in response to internationally wrongful acts. Such operations need not be technical countermeasures alone, but could also take the form of coercive sanctions cutting off access of violator states to IXPs or even authoritative DNS resolvers. Such measures,

which will be evaluated against their temporality and proportionality, would not be prohibited under international law. But states should seriously consider whether strong responses such as BGP sink-holing against DDoS attacks (Jonker, 2019) or sanctions against IXPs and RIRs should be permissible as countermeasures, keeping in mind the need to preserve the general availability and integrity of the Internet at all times. The G7′s statement on sanctions against Russia for its invasion of Ukraine specifically carves out an exception for Internet access, and is a good step in this regard (Fact Sheet, 2022). Similarly, the EU issued a 'internet carve out' when it sanctioned Russia in 2022.[25] These political choices for restraint are significant, but are more vulnerable to changes in the (geo)political climate than legal restraints would be.

The public core also requires a *jus in bello*, that is, wartime regime of rights and responsibilities, since DNS infrastructure and core Internet protocols serve as critical lifelines for communication and essential services as well as the activities of local and international relief organisations during war. A 2019 roundtable convened by the International Committee of the Red Cross with military cyber experts and IT companies concluded that 'the risk of seriously compromising core Internet services was […] unlikely at the present moment thanks to the high degree of redundancy in the DNS', but should such disruption occur, 'it could have widespread and potentially serious consequences' (International Review of the Red Cross, 2021). The fact that major disruptions to the public core are unlikely does not obviate the need for rules around its protection. As the war in Ukraine has shown, states are increasingly likely to target public core infrastructure for reasons ranging from domestic censorship to DDoS attacks, making transboundary disruptions more probable in the future. In particular, the ongoing debate on the status of 'data'—understood both as content and code—in international humanitarian law applies squarely to the public core as well (Mačák, 2015): can protocols such as BGP or UDP be considered an 'object', and thus be protected in certain circumstances under IHL? One view could be that core Internet protocols are themselves not objects, and only the functionality of civilian systems and networks that rely on them would be protected under IHL.[26] Another, more permissive view is that modern militaries 'rely primarily on [public core infrastructure such as] cables, routers, switches and satellites (as well as the firmware and software that run them) that are used for civilian communications' for cyber operations and therefore, it would be impractical to suggest they are off-bounds during war (Harrison Dinniss, 2015). Nevertheless, the targeting of such infrastructure as part of a larger military objective should account for potential civilian impacts given the requirement under IHL of proportionality (Harrison Dinniss, 2015). What the war in Ukraine has shown is that the organisations, protocols, and infrastructure that make up the public core of the Internet will be under extraordinary duress and repeated targeting by belligerents during armed conflict. To ensure that such operations do not disrupt the functioning of essential civilian services or result in the cutting off of internet access to affected populations, states should be more forthcoming in declaring how IHL protections apply to core infrastructure, with a view protecting civilian interests.

CONCLUSION

States are increasingly seized of the need to protect the public core of the Internet, but the precise scope of international rules to address threats against it remains unclear. The protracted conflict in Ukraine raises the possibility of 'aggressive cyber operations that spread beyond their intended target' (Tucker, 2022) and cause transboundary harm, and can conceivably jeopardise global Internet infrastructure in some cases. Building on the progress made at the UN GGE and OEWG, it is imperative that states (a) clarify the precise

scope of the norm on the protection of the public core and build a framework for its protection and (b) identify and apply international law to regulate cyber operations and coercive political measures targeting it. On both counts, a lot of work needs to be done. The delineation and interpretation of what the public core is and what protection thereof entails, is laborious even among those states that in principle endorse the norm. When states need to talk across the political and diplomatic divide(s) in the UN the conversation sometimes becomes 'weaponized' with states like Russia and China trying to use the concept as a Trojan horse to get their ideas on state-led internet governance and cyber sovereignty on the diplomatic agenda. While a concept like the public core should be open to honest contestation among states and other stakeholders, it should also be protected against being instrumentalised to serve political agendas that go against the fundamentals of the concept. To stick with the metaphor, those who support the idea of the public core in its original formulation(s) should 'beware of Russians and Chinese bearing gifts'. The normative and legal framework around the public core should be built around the principle of restraint, and if geopolitical contestation leads to a radically different interpretation of this framework that invites states to interfere in the functioning of global internet infrastructure, the whole exercise may prove to be counterproductive. While the lack of trust among states in the current geopolitical climate admittedly impedes honest contestation of the scope of public core protections, it is important to acknowledge that there is no alternative to the fora in the UN first committee to talk across the divide. As the biggest manifested and potential threats come from state actors, it is vital to advance the conversation about the (im)permissibility of using core internet infrastructure for offensive purposes in a setting that includes the major cyber powers. Making a (legal) norm explicit does not in and of itself stop actors from violating it, but does give other actors the language to condemn that violation.

The norm to protect the public core of the internet should ideally be connected to protection under international law. However, the conceptualisation—and technological reality—of the public core as an inherently *transnational* critical information infrastructure or even a 'global public good' is hard to reconcile with international law that is firmly built on the foundation of national sovereignty and territoriality. International law's 'toolbox' is often hard to fit onto the problem at hand. The prohibition of the use of force, the rule of non-intervention and due diligence obligations all have limitations when it comes to the protection if the public core. Some of those limitations are connected to sovereignty and territoriality and some are connected to the threshold values of the 'use of force' and 'coercion'. Both states and scholars, as noted in the section on 'The limits of international law', have been discussing the question whether the nature of the cyber domain and state-led cyber operations require a rethink of these threshold values. In addition to state positions and scholarship cited in in the section 'The limits of international law', it is worth pointing here to the robust and ongoing debate among reputed international lawyers of the Oxford Process on International Law Protections in Cyberspace on the evolving threshold of coercion and the rule of non-intervention in the cyber context (ELAC, 2022). Although consensus within the group on the precise threshold appears elusive, some Oxford Process lawyers have even considered the possibility, in this vein, of 'fleshing out rules that protect the public core of the internet' (ELAC, 2022, n.69, 291).

The ongoing dissemination and deepening of the norm to protect the public core of the internet—for example, through the recent US acknowledgement that the Internet's architecture and protocols are 'threatened by intentional abuse by malicious actors' (United States Government Accountability Office, 2022)—is of vital importance, but also needs to be a stepping stone for (re)thinking through the role of international law in the protection of transnational critical information infrastructure.

ACKNOWLEDGEMENTS

The authors would like to thank two anonymous and persistent reviewers whose critical reviews resulted in making this a substantially better paper. The work of the authors at the Hague Program on International Cyber Security is generously supported by the Dutch Ministry of Foreign Affairs.

ORCID

Dennis Broeders http://orcid.org/0000-0002-8827-2814
Arun Sukumar http://orcid.org/0000-0001-7137-0525

ENDNOTES

[1] Russia now seems to restrain its cyber-attacks using wipers, preventing them from spreading across borders (see Grossman et al., 2023).

[2] See, for example, the statements on Existing and Potential threats delivered by the delegations of Germany, the United States, the United Kingdom and the Netherlands. All statements can be found on: Open-ended working group on information and communication technologies. https://meetings.unoda.org/meeting/57871/statements?f%5B0%5D=segment_statements_%3ASecond%20substantive%20&f%5B1%5D=segment_statements_%3ASecond%20substantive%20session

[3] Letter from Mikhaylo Federov, Vice-Prime Minster of Ukraine, to Hans Petter Holen, Managing Director RIPE NCC, 2 March 2022. https://www.ripe.net/publications/news/announcements/request-from-ukrainian-government.pdf

[4] Letter from Hans Petter Holen, Managing Director RIPE NCC, to Mikhaylo Federov, Vice-Prime Minster of Ukraine, 10 March 2022.

[5] See for a recent overview of cyber operations in Ukraine: Grossman et al. (2023).

[6] United Nations General Assembly, Open-ended working group on developments in the field of information and telecommunications in the context of international security ('OEWG Report'), Final Substantive Report, UN Doc A/AC.290/2021/CRP.2; United Nations General Assembly. Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security ('UN GGE Report'), UN Doc A/76/135.

[7] The authors acknowledge the contribution of Olaf Kolkman to arguments developed in this section.

[8] NATO—News: NATO stands up undersea infrastructure coordination cell, 15 February 2023. https://www.nato.int/cps/en/natolive/news_211919.htm

[9] Multistakeholder imposition of internet sanctions. https://www.pch.net/resources/Papers/Multistakeholder-Imposition-of-Internet-Sanctions.pdf

[10] United Nations General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security* ('OEWG Report'), Final Substantive Report, UN Doc A/AC.290/2021/CRP.2; United Nations General Assembly. *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security* ('UN GGE Report'), UN Doc A/76/135.

[11] *OEWG Report*, B.26; For an in-depth analysis of the OEWG and GGE processes and the public core, *see* Broeders (2021).

[12] *UN GGE Report*, III.46.

[13] See Finnemore and Sikkink (1998) on norms processes with an emphasis on norm dissemination; see Wiener (2014), on norms processes with an emphasis on the contestation of norms.

[14] Government of the Netherlands, (2017); the new 2023 International Cyber Strategy reiterates the importance of the Protection of the public core of the internet, see: Government of the Netherlands (2023).

[15] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common level of Cybersecurity Across the Union, 14th December 2022, (NIS 2 Directive).

[16] Declaration for the Future of the Internet, at https://www.state.gov/declaration-for-the-future-of-the-Internet

[17] See for the debate about cyber sovereignty in relation to internet governance in general for example: Mueller (2019). For the specific notions of Russian and Chinese 'cyber sovereignty', see Creemers (2020) and Kurowska (2020).

[18] Contribution by the Russian Federation to the ITU CWG-Internet, 'Risk Analysis of the Existing Internet Governance and Operational Model' (document CWG-Internet-16/4-E), 9 September 2021.

[19] Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), Rule 11, 45.

[20] *Military and Paramilitary Activities in and against Nicaragua, Judgment, [1984] ICJ Rep. 205*.

[21] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), L 151/20 (2019).

[22] See generally, the positions of Australia, the Netherlands, Israel, and Finland on the topic in United Nations General Assembly, 76th session, 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266', A/76/136, July 13, 2021, 56. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

[23] Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission on the Work of Its 53rd session, UN GAOR, 56th Sess., Supp. No. 10, at 36, UN Doc. A/56/10 (2001) *c.f*. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations (Michael N. Schmitt ed., 2017), Rule 14, 86.

[24] Erga omnes obligations are those obligations 'in whose fulfilment all states have a legal interest because their subject matter is of importance to the international community as a whole' 'erga omnes obligations'. *Oxford Reference*; Accessed 5 June 2023. https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095756413

[25] Council Regulation (EU) 2022/880 of 3 June 2022 amending Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

[26] Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), Rule 38, 127.

REFERENCES

Badiei, F. (2023). Sanctions and the Internet. (Report commissioned by RIPE NCC) digital Medusa. Sanctions and the Internet-DigitalMedusa.pdf

BBC News. (2023, October 10). Finland investigates suspected sabotage of baltic-connector gas pipeline, sec. Europe. https://www.bbc.com/news/world-europe-67070389

van Benthem, T. J., (2023). Privatized frontlines: Private-sector contributions in armed conflict. In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, Estonia (pp. 55–69). https://doi.org/10.23919/CyCon58705.2023.10182177

Bloomfield, A. (2016). Norm antipreneurs and theorising resistance to normative change. *Review of International Studies*, *42*, 310–333.

Braverman, S., (2022, May 19), The Attorney General's Office. International law in future frontiers. https://www.gov.uk/government/speeches/international-law-in-future-frontiers

Broeders, D. (2015). *The public core of the internet: An international agenda for internet governance*. Amsterdam University Press.

Broeders, D. (2017). Aligning the international protection of 'the public core of the internet' with state sovereignty and national security. *Journal of Cyber Policy*, *2*(3), 366–376. https://doi.org/10.1080/23738871.2017.1403640

Broeders, D. (2021). The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: A mid-process assessment. *Journal of Cyber Policy*, *6*(3), 277–297. https://doi.org/10.1080/23738871.2021.1916976

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129;

Burgess, M. (2022). Russia is taking over Ukraine's Internet. *Wired*. Retrieved June 19, 2022, from: https://www.wired.com/story/ukraine-russia-internet-takeover/

Coco, A., & de Souza Dias, T. (2021). Cyber due diligence': A patchwork of protective obligations in international law. *European Journal of International Law*, *3*(32), 790–794.

Copp, T. (2023, September 11). Elon Musk's refusal to have starlink support Ukraine attack in crimea raises questions for pentagon. *AP News*, sec. Politics. https://apnews.com/article/spacex-ukraine-starlink-russia-air-force-fde93d9a69d7dbd1326022ecfdbc53c2

CPO Magazine. (2022). Russian certificate authority issuing native TLS certificates to beat sanctions, but plan has limitations. Retrieved June 16, 2022, from: https://www.cpomagazine.com/cyber-security/russian-certificate-authority-issuing-native-tls-certificates-to-beat-sanctions-but-plan-has-limitations/

Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. In D. Broeders, & B. van den Berg (Eds.), *Governing cyberspace: Behaviour, power and diplomacy*. Rowman & Littlefield.

Cyber Law Toolkit. (n.d.). Due diligence, international cyber law: Interactive toolkit. Retrieved January 9, 2022, from: https://cyberlaw.ccdcoe.org/wiki/Due_diligence

Cybersecurity and Infrastructure Security Agency. (2019). Emergency directive 19-01. Retrieved June 18, 2022, from: https://www.cisa.gov/emergency-directive-19-01

Douzet, F., Pétiniaud, L., Salamatian, L., Limonier, K., Salamatian, K., & Alchus, T. (2020). Measuring the fragmentation of the Internet: The case of the border gateway protocol (BGP) during the Ukrainian crisis. In *2020 12th International Conference on Cyber Conflict (CyCon)*, Estonia (pp. 157–182). https://doi.org/10.23919/CyCon49761.2020.9131726.

Eamon, J., (2022). Ukraine asked the Internet's governing body to remove Russian sites, *CNBC*. Retrieved June 16, 2022, from: https://www.cnbc.com/2022/03/01/ukraine-asked-icann-to-revoke-russian-domains-shut-dns-servers.html

Eichensehr, K. E. (2022). Ukraine, cyberattacks, and the lessons for international law. *American Journal of International Law Unbound*, *116*, 149.

ELAC. (2022). *The Oxford process on international law protections in cyberspace: A compendium*. Oxford Institute for Ethics, Law and Armed Conflict. https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf

European Commission. (2020) The EU's cybersecurity strategy for the digital decade: Joint communication to the European parliament and the council by the high representative of the union for foreign affairs and security policy. JOIN 18 final: 151/19, 151/35.

Fact Sheet. (2022). United States, G7 and EU impose severe and immediate costs on Russia, The White House. Retrieved June 11, 2022, from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

Fidler, D. (2013). Internet governance and international law: the controversy concerning revision of the international telecommunication regulations. Retrieved June 18, 2022, from: https://www.asil.org/insights/volume/17/issue/6/Internet-governance-and-international-law-controversy-concerning-revision

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(4), 887–917.

France Diplomacy—Ministry for Europe and Foreign Affairs. (2021). Ministère de l'Europe et des Affaires étrangères, cybersecurity: Paris call of 12 November 2018 for trust and security in cyberspace. Retrieved June 21, 2021, from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

Fung, C. J. (2022). China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet. *Journal of Cyber Policy*, *7*(3), 256–274. https://doi.org/10.1080/23738871.2023.2178946

GCSC. (2017). Call to protect the public core of the Internet. https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-Internet

GCSC. (2018). Definition of the public core, to which the norm applies. https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf

GCSC. (2019). *Advancing cyberstability*. Final report of the global commission on the stability of cyberspace.

Goodin, D. (2022). Why Russia's "disconnection" from the internet isn't amounting to much. Ars Technica. https://arstechnica.com/information-technology/2022/03/why-russias-disconnection-from-the-internet-isnt-amounting-to-much/

Government of the Netherlands. (2017). Building digital bridges: International cyber strategy: Towards an integrated international cyber policy. https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

Government of the Netherlands. (2023). *International cyber strategy 2023–2028*. Decisive Diplomacy in the Digital Domain. https://www.government.nl/documents/publications/2023/09/12/international-cyber-strategy-netherlands-2023-2028

Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023). *The cyber dimensions of the Russia-Ukraine war*. Workshop Report. UK NCSC and ECCRI.

Harrison Dinniss, H. A. (2015). The nature of objects: Targeting networks and the challenge of defining cyber military objectives. *Israel Law Review*, *48*, 39–54. https://doi.org/10.1017/S0021223714000272

Helal, M. S. (2019). On coercion in international law. *New York University Journal of International Law and Politics*, *52*, 65–67.

Hirani, M., Jones, S., & Read, B., (2019). Global DNS hijacking campaign: DNS record manipulation at scale. Mandiant. Retrieved June 19, 2021, from: https://www.mandiant.com/resources/global-dns-hijacking-campaign-dns-record-manipulation-at-scale

International Review of the Red Cross. (2021). ICRC-affiliated reports: Digital technologies and war. Retrieved June 18, 2021, from: http://international-review.icrc.org/articles/icrc-affiliated-reports-digital-technologies-and-war-913

Internet Society. (2022a). Two months of war: The impact on the Internet's core. Retrieved Jun 11, 2022, from: https://www.Internetsociety.org/blog/2022/05/two-months-of-war-the-impact-on-the-Internets-core/

Internet Society. (2022b). Internet perspectives: Ukraine and Russia. Internet Society Pulse. Retrieved June 11, 2022, from: https://pulse.internetsociety.org/blog/internet-perspectives-ukraine-and-russia

Jonker, M. (2019). The drawbacks of blackholing. APNIC Blog. https://blog.apnic.net/2019/07/16/the-drawbacks-of-blackholing/

Kaminska, M., Broeders, D., & Cristiano, F. (2021). Limiting viral spread: Automated cyber operations and the principles of distinction and discrimination in the grey zone. In 2021 13th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 59–72. https://doi.org/10.23919/CyCon51939.2021.9468290

Kavanagh, C. (2023). Wading murky waters: Subsea communications cables and responsible state behaviour, UNIDIR. https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf

Kilovaty, I. (2021). The international law of cyber intervention. In N. Tsagourias, & R. Buchan (Eds.), *Research handbook on international law and cyberspace*. Edward Elgar Publishing. https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00014.xml

Krähenbühl, C., Wyss, M., Burkhard, R., Wanner, J., & Perrig, A. (2022). Swiss post E-voting scope 4: Network security analysis. https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Scope%204%20Final%20Report%20Network%20Security%20Group,%20ETH%20Zurich%2006.01.2022.pdf

KrebsonSecurity. (2019). A deep dive on the recent widespread dns hijacking attacks—Krebs on security. Retrieved June 18, 2022, from: https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Kurowska, X. (2019). *The politics of cyber norms: Beyond norm construction towards strategic narrative contestation*. EU Cyber Direct: Research in Focus.

Kurowska, X. (2020). What does Russia want in cyber diplomacy? A primer. In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace: Behaviour, power and diplomacy*. Rowman & Littlefield.

Levinson, N. (2021). Idea entrepreneurs: The case of the United Nations open-ended working group & cybersecurity. *Telecommunications Policy*, *45*(6), 102–142.

Maurer, T. (2020). A dose of realism: The contestation and politics of cyber norms. *Hague Journal on the Rule of Law*, *12*, 283–305. https://doi.org/10.1007/s40803-019-00129-8

Mačák, K. (2015). Military objectives 2.0: The case for interpreting computer data as objects under International Humanitarian Law. *Israel Law Review*, *48*, 55–80.

Microsoft. (2022, December 14). *Cyber signals issue 3: The convergence of IT and OT and the risks to cybersecurity*. Security Insider (blog). https://www.microsoft.com/en-us/security/business/security-insider/reports/cyber-signals/cyber-signals-issue-3-the-convergence-of-it-and-ot/

Moss, S. (2022). London internet exchange disconnects Megafon and Rostelecom. DCD. https://www.datacenterdynamics.com/en/news/london-internet-exchange-disconnects-megafon-and-rostelecom/

Mueller, M. (2019). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mueller, M. L., & Badiei, F. (2017). Governing internet territory: ICANN, sovereignty claims, property rights and country code top-level domains. *Science and Technology Law Review*, *18*, 435–491.

Needleman, S. E. (2022, March 3). Steward of Internet domains punts on Ukraine's request to punish Russia. *Wall Street Journal*. Retrieved June 16, 2022, from: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-03/card/steward-of-Internet-domains-punts-on-ukraine-s-request-to-punish-russia-u8ITKecCuJoeJWg4l8op

Pearson, J. (2022, May 11). Russia downed satellite internet in Ukraine—Western officials. *Reuters*. Retrieved June 19, 2022 from: https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/

Pennington, J., & Lyngaas, S. (2023, September 10). Starlink in use on 'all front lines,' Ukraine spy chief says, but wasn't active 'for time' over crimea. *CNN*. https://www.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html

Pijpers, P. (2023). *Influence operations in cyberspace and the applicability of international law*. Edward Elgar.

Pollard, N., & Kauranen, A. (2023, October 17). *Sweden says telecom cable with Estonia damaged but operating*. Reuters. sec. Europe, https://www.reuters.com/world/europe/sweden-says-telecom-cable-with-estonia-damaged-2023-10-17/

Pollet, M. (2023). EU looks to boost secure submarine internet cables in 2024. Politico. https://www.politico.eu/article/eu-looks-to-boost-secure-submarine-internet-cables-in-2024/

Qiu, W. (2022). Tonga cables cut after volcano eruption, at least four weeks to restore—Submarine Networks. Submarine Cable Networks. Retrieved June 19, 2022 from: https://www.submarinenetworks.com/en/systems/australia-usa/tonga-cable/tonga-cable-cuts-after-volcano-eruption

Raustiala, K. (2023). Multistakeholder regulation and the future of the internet. *Federal Communications Law Journal*, *75*(2), 161–195. http://www.fclj.org/wp-content/uploads/2023/02/75.2.1-Multistakeholder-Regulation.pdf

Raymond, M. (2021). Social practices of Rule-Making for international law in the cyber domain. *Journal of Global Security Studies*, *6*(2), ogz065. https://doi.org/10.1093/jogss/ogz065

RIPE Network Coordination Centre. (2022). RIPE NCC response to request from Ukrainian Government. Retrieved June 20, 2022, from: https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

RIPE Network Coordination Centre. (2008). YouTube hijacking: A RIPE NCC RIS case study. Retrieved June 19, 2022 from: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Roguski, P. (2020). Collective countermeasures in cyberspace—Lex lata, progressive development or a bad idea? In *1300 in 2020 12th International Conference on Cyber Conflict (CyCon)* (Vol. 39).

Schmitt, M. N. (Ed.). (2017a). *Tallinn manual 2.0 on the international law applicable to cyber operations* (1st ed., p. 318). Cambridge University Press.

Schmitt, M. N. (2017b). Grey zones in the international law of cyberspace. *Yale Journal of International Law Online*, *42*, 21pp.

Schneier, B. (2016). Lessons from the dyn DDoS attack, security intelligence, 1 November 2016. securityintelligence.com

Siddiqui, A. (2021). Did someone try to hijack Twitter? Yes!, MANRS. Retrieved June 19, 2022, from: https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/

Steenman, H., (2020). *The Internet today has major flaws. What can AMS-IX do to overcome them?* AMS-IX. Retrieved June 19, 2022, from https://www.ams-ix.net/ams/stories/the-internet-today-has-major-flaws-what-can-ams-ix-do-to-overcome-them

The Cloudflare Blog. (2013). *The DDoS that almost broke the Internet*. Retrieved June 17, 2022, from: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet/

The Cloudflare Blog. (2023, February 23). One year of war in Ukraine: Internet trends, attacks, and resilience. http://blog.cloudflare.com/one-year-of-war-in-ukraine/

Tucker, P. (2022). Russia might try reckless cyber attacks as Ukraine war drags on, US warns. Defense One. Retrieved June 19, 2022, from: https://www.defenseone.com/threats/2022/06/russia-might-try-reckless-cyber-attacks-ukraine-war-drags-us-warns/368242/

United States Government Accountability Office. (2022). Internet architecture is considered resilient, but federal agencies continue to address risks. Retrieved June 19, 2022, from: https://www.gao.gov/assets/720/719340.pdf

Wiener, A. (2014). *A theory of contestation*. Springer.

How to cite this article: Broeders, D., & Sukumar, A. (2024). Core concerns: The need for a governance framework to protect global internet infrastructure. *Policy & Internet*, 1–17. https://doi.org/10.1002/poi3.382