Cybersecurity and extraterritorial obligations of states

Matthias C. Kettemann and Anna Sophia Tiedeke

Introduction

Be it online or offline, be it in the kinetic world or in cyberspace: we need norms – and have always needed them. ‘In the long march of mankind from the cave to the computer’, as Shaw puts it in his introduction to international law, ‘a central role has always been played by the idea of law – that order is necessary and chaos inimical to a just and stable existence’ (Shaw 2021 p. 1). Cyberspace as a truly global infrastructure is governed by rules of international law (some aspects of it are also governed by national law and transnational normative arrangements (Kettemann 2020)), but for the purposes of assessing extraterritorial obligations, this article will focus on international law). Indeed, international law is the only area of law with which global (public) goods can be managed and global public interests protected (Kettemann 2020). The ubiquity of the technology underlying the Internet, which is not restricted by national borders, renders strictly single-state regulation largely ineffective. A failure to ensure cybersecurity in one state leads to less cybersecurity in all states, and therefore has a direct impact on human rights protection across borders. Ensuring cybersecurity within a state, and thereby contributing to cybersecurity extraterritorially, ensures the stability of the international order and thus has to be understood as a key element of the extraterritorial protection of human rights.

Cybersecurity has become a pressing issue for the public as well as the private sector over the last decades. Considering the cross-border character of incidents like the WannaCry Ransomware attack or the hack of the Democratic National Committee, resorting to international law to accord responsibility seems intuitive. Even though political and legal approaches to preventing cyberwar and cybercrime have attracted considerable attention internationally, cybersecurity as a human rights issue has received less attention. In this chapter we will therefore concentrate on cybersecurity as a human rights issue, with a specific focus on the extraterritorial obligations of states and private actors. After taking stock and setting out a comprehensive concept of cybersecurity, we will continue to explain why protecting cybersecurity lies in the common interest of all states irrespective of their borders. We will then outline how extraterritorial obligations of states are conceptually developed, and what obligations states have to ensure an adequate level of cybersecurity and human rights protection. After that, we will identify approaches to improve the protection of cybersecurity in international law. The contribution ends with conclusions.
Taking stock

International law is needed to legitimately and effectively ensure cybersecurity in the common interest of all states; and therefore, international law foresees extraterritorial obligations of states in cyberspace. This is not a new insight.

Already in 2010, in its resolution A/RES/64/211 the General Assembly promoted the creation of a global culture of cybersecurity and expressed concerns in light of growing threats to the reliable functioning of the Internet. The Resolution affirms that states are obliged to deal systematically with these threats and coordinate both with national stakeholders and internationally with the goal of facilitating the achievement of cybersecurity. A similar self-commitment to an international law-based Internet policy was already presented by the European Commission in 2014 (COM/2014/072 final) and is also part of the EU Cybersecurity Strategy for the Digital Decade European Digital Strategy of 2020. Although it might seem evident that without legitimate and effective protection of cybersecurity under international law individuals and societies cannot develop to their full potential, to view these issues as a human rights issue has not been evident until recently. The 2013 UN Group of Governmental Experts (GGE) Report underlined that applying norms derived from existing international law relevant to the use of information and communication technologies (ICTs) by states is an essential measure to reduce risks to international peace, security and stability. The UN Charter is applicable to the whole gamut of socioeconomic activity on the Internet in that it is ‘essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment’ (UN GGE 2013, para. 19).

Applying international law to the Internet lies in the common interest, and safeguarding the Internet as such also lies in the common interest because a stable, secure and functional Internet is essential for international security. Building on this consensus, the GGE Report 2015 confirmed that international law, the UN Charter and international legal principles apply to the Internet (para. 26). Stating inter alia that the international community aspires to regulate the Internet in a peaceful manner ‘for the common good of mankind’ (UN GGE 2015, para. 28 (c)), ‘[t]he adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment’ (para. 25). After the GGE could not arrive at a decision in 2017, in December 2019 the UN Cybersecurity Groups OEWG (Open-ended Working Group) and GGE held an informal meeting discussing four topics relating to cybersecurity. Apart from threat scenarios, the two groups discussed norms for responsible state behaviour in cyberspace, measures regarding confidence-building and capacity-building. In 2021 the OEWG and the GGE published separate reports, both reaffirming their general commitment regarding the applicability of international law and the UN Charter in cyberspace but also their preference for voluntary norms. The GGE Report 2021 also reiterated the group members’ commitment to human rights (para. 36–41).

Ensuring cybersecurity and protecting the Internet’s stability, security and functionality in the form of reducing the potential for criminal or terroristic misuses of computers and networks are important in the international fight against cybercrime. Criminals continue to misuse the Internet both for online variants of common scams and for Internet-specific (technology-based) attacks. The size of monetary loss is small compared to the scale of the Internet economy, but the problem is nevertheless serious. Black markets for both buying cybercrime tools (such as complete botnets for as little as 50 USD) and for selling on the proceeds of cybercrime activities (such as credit card information) are increasingly sophisticated, resilient and international (Ablon, Libicki and Golay 2014). This threat requires international cooperation. At the same
time, some criminal misuses of the Internet are not direct threats to the Internet’s integrity, as criminal networks rely on the Internet to conduct their activities. But other attacks, including Distributed-Denial-of-Service attacks (DDoS attacks) or others not linked to monetary gain — such as attacks to cause social unrest — can amount to substantial threats to the cybersecurity and the Internet’s functionality.

Different levels of Internet security awareness and capabilities globally matter to all states because of the interconnectedness of ICTs and the networked nature of the Internet. These are amplified through disparities in national law, regulations and practices. Only international cooperation and the acknowledgement of extraterritorial obligations of states in the protection of the Internet can help to find answers to these challenges. In this context it is important to note with Wilde that ‘[e]xtraterritoriality is not the displacement of statism with cosmopolitanism’, but rather a combination of the two (2016, p. 153). In our globalized world, where the focus of international law is shifting away from governments to (multistakeholder) governance, we need to take a close look at the extraterritorial human rights obligations of states. This will also require a shift of perspective from a territorial protection of human rights towards a functional perspective. This shift ‘towards post-territoriality’ (Kilovaty 2020, p. 50) is never more apt or more important than when assessing state obligations related to cybersecurity.

While public international law offers useful tools and perspectives on cybersecurity, it also ‘suffers from a few fatal flaws that make it a less-than-perfect candidate to stymie the consequences of offensive cyberspace behaviour’ (Kilovaty 2020, p. 36). The flaws are rooted in the fact that international law focuses mainly on states that are defined by territory, not on individuals that are affected by breaches of cybersecurity. Transnational legal arrangements, including technical standards and agreements, influence the exercise of power online and shape the normative order in which it is legitimated and contested (Kettemann 2020). Apart from security interests of states, ensuring cybersecurity is closely linked to extraterritorial protection of human rights on the Internet. However, until recently ‘the majority of scholarship on transnational cyber operations has focused on the victim state’s rights, such as sovereignty and territorial inviolability to delegitimize these operations’ (Kilovaty 2020, p. 36). For a long time, human rights have not been in the spotlight of international cybersecurity debates. Looking at cybersecurity from a human rights perspective offers us the opportunity to see all dimensions of a cyberattack or the lack of cybersecurity. A human rights-based view on cybersecurity has the capacity to make the consequences of a lack of cybersecurity visible.

Towards a comprehensive concept of cybersecurity

Cybersecurity is defined very broadly by some states and is a legal (and policy) term that covers risks and threats such as cyberwarfare, cyberterrorism, cybercrime and cyberespionage. There is no doubt that cybersecurity is a crucial part of national domestic, security, foreign and defence policy. As a central theme of Internet policy, cybersecurity is closely linked with the stability, robustness, resilience and functionality of the Internet (Tikk-Ringas, 2015). Cybersecurity can be threatened by cybercrime and cyberterrorism, but also by a lack of legal and technical control of and cooperation between states and a lack of preventive measures, such as developing crisis intervention centres and teams, as well as transnational crisis communication structures for cyber-incidents. But can the term cybersecurity be useful in the context of a human rights discussion? In our view it is still too often the case that (cyber) security is contrasted with (Internet) freedom, and the two concepts are played against each other to the detriment of both. This view misses the point. As emphasized in the German Cybersecurity Strategy of 2016, what matters
is that ensuring both freedom and security are among the core duties of the state – offline and online (Cyber-Sicherheitsstrategie für Deutschland 2016, p. 8).

The German Cybersecurity Strategy defines cybersecurity as ‘IT security of the networked or network-capable information technology systems in cyberspace’. IT security is understood to be ensuring the ‘intactness of the authenticity, confidentiality, integrity and availability of information technology systems and the data processed and stored within these systems’ (2016, p. 24). This definition is very technology oriented and too short-sighted in light of how cybersecurity is practically perceived by business and society. The security on the Internet and of the Internet cannot simply be equated with the security of systems and data. Just as security has rightfully been understood more recently as human security, cybersecurity needs to include a human rights perspective.

Protecting cybersecurity lies in the common interest of all states

Already in 1998, experts working for the UNESCO asked the question whether the United Nations General Assembly [could] affirm the principle of regarding cyberspace as ‘the common heritage of humanity’ (UNESCO 1998, para. 9) and thus safeguard it. In the end, they failed to answer the question, which was well enough, because it was actually the wrong one to be posed in the first place. It is not ‘cyberspace’ we should concern ourselves with, but rather the Internet itself; and rather than using the concept of common heritage of mankind, which presupposes a certain historical stability the Internet does not have, we rather need to establish why protecting the Internet lies in the global common interest. Though ‘common interest’ still lacks a clear definition (Feichtner 2007, para. 1), the protection of the Internet’s key resources as lying in the common interest is firmly anchored in international documents. It is also in the common interest to protect human rights as the commitment during the World Summits on the Information Society (WSIS) show.

In a statement of the WSIS, which the UN convened in 2003 and 2005 to establish a normative trajectory for the Internet, states affirmed their common desire and commitment to build an information society that is ‘people-centred, inclusive and development-oriented’ (WSIS 2003, para. 1). Their goal was that individuals, communities and peoples can ‘achieve their full potential in promoting their sustainable development and improving their quality of life premised on the purposes and principles’ of the UN Charter and respecting fully and upholding the Universal Declaration of Human Rights (UDHR) (WSIS 2003, para. 1). This is a first, clear answer to the question what ‘vision’ the international community pursues regarding the impact of the Internet. To put it concisely: the Internet is envisaged to serve humankind. Of course, achieving world peace and international security, ensuring human development and respecting, protecting and implementing human rights – as normatively ordered in the UDHR – are in the global common interest.

But is protecting cybersecurity and thus the Internet’s integrity essential for reaching these goals? UN Special Rapporteur for freedom of expression, Frank La Rue, in a ground-breaking report on the impact of the Internet on freedom of expression, described the Internet as a ‘catalyst for individuals to exercise their right to freedom of opinion and expression’. He called freedom of expression on the Internet itself a ‘facilitator of the realisation of a range of other human rights’ (paras. 22 and 23). The multiple challenges that the Internet brings for human rights notwithstanding (Jørgensen 2006 and 2019), the absence of the Internet or of an Internet without cybersecurity would seriously challenge the realization of human rights. There are important corollary rights that are premised upon exercising free speech on the Internet, like the freedoms of assembly and association online, and the right to digital education. From all these
rights we can also derive a right to access to online information and communication, which is crucial for human development. Similar arguments have been voiced by courts and international organizations (e.g., CoE Res. 1877/2012; ECtHR Yildirim v. Turkey, 2012). Even though the Internet simultaneously introduces new threat vectors to human rights, it greatly enhances the potential of people to realize their human rights. It is similarly a facilitator for human security.

In the same vein, the UN GGE report of 2013 determined that the application of norms derived from existing international law is 'essential' to minimize risks to world peace and international security and stability (para. 16). Viewed in the context of information technology challenges, cybersecurity is now one aspect of ‘world peace’ (para. 16). When analyzing the protection of cybersecurity under international law, the GGE report 2015 that was adopted in consensus by a representative group of governmental experts is very helpful, stating inter alia that the international community aspires to regulate the Internet in a peaceful manner 'for the common good of mankind'. Protecting cybersecurity is a common interest of all states. This community interest is not an aggregate of the individual sets of interests; rather, it lies at their intersection. If a protected interest is part of the community interest, this entails consequences relevant to international human rights law. States are therefore responsible to the international community, with regard to cybersecurity according to their judicial authority over critical infrastructures pertinent to it in that ‘States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 (UN GGE 2021, para. 47–50).

Therefore, to the extent that a state controls Critical Internet Resources (CIRs), e.g., the Internet's backbone infrastructure, Internet protocol numbers, name root servers and the Domain Name System (DNS), it has to exercise this jurisdiction mindful of threats to cybersecurity, and especially the security of these CIRs in a manner that ensures the common interest. To the extent that national politics (and policies) can impact the Internet negatively, a state has to refrain from their formulation and implementation. A state’s sovereignty is reduced because of the limits the protection of the Internet as a common interest lays upon it. The US, when it exercised its soft control over Internet key resources, via the Department of Commerce’s naming and numbering oversight functions, only exercised ‘custodial sovereignty’ (Scholtz 2008). This implied that the US had to enter into consultations with other states with regard to the management of CIRs and made sure that the management was transparent and accountable, ideally to the international community and now, after the transition (National Telecommunications and Information Administration (NTIA) 2016), to the global multistakeholder community. All other states, insofar as they can endanger the Internet’s stability, security and functionality, are pre-empted from doing so. In assessing whether politics may impact the Internet negatively, it makes sense to suggest the precautionary principle as a guide to decision-making.

A second consequence is that humankind – that is all actors making up the international community, and not only states – has a legitimate interest in making sure that all other actors protect the Internet (or at least do not actively harm it). Though sovereignty oriented states have suggested exclusive sovereignty over national Internet segments, the character of the Internet as protected by international law as a common interest limits their sovereignty. The 2005 Tunis Agenda, though valuable in its description of the normative goals of the information society, still lays down that ‘policy authority for internet-related public policy issues’ is a ‘sovereign right of States’ (WSIS 2005, para. 35). The internal and external dimensions of sovereignty relate to the control over territory and individuals, cyberactivity and infrastructure inside that territory and the capacity of states to maintain international relations (Schmitt 2017, p. 4).

This needs to be qualified in light of a common interest approach to protect the Internet, in that the state’s policy authority no longer is an exclusively sovereign right, but part and parcel
of their sovereignty, to be exercised in the common interest. What sovereignty they have over Internet-related resources has to be understood in light of changing circumstances and the importance of the pursuance of common interests. As far as international law extends to non-state actors, these are also under obligation to conform to, and support, the common pursuance of the global interest in safeguarding the Internet’s integrity. This means, for example, that there is an international law-based duty, via the Ruggie Principles of 2011, for companies to respect human rights and rights of victims of business-related abuses and their right to access to remedies. International law has arrived at a point in its development where pursuing the common interest, as Fassbender put it, is the only reasonable answer to its Sinnfrage (Fassbender 2002, p. 231). Ensuring a people-centric and development-oriented Internet is one of the key challenges for international law today. To protect human rights effectively, the protection of the integrity of the Internet and the guarantee of cybersecurity as a common interest are essential. The extraterritorial application of political and civil but especially economic, social and cultural human rights, is one of the key measures to ensure the respect for and the protection and fulfilment of cybersecurity, and thereby a people-centric and development-oriented Internet.

**Extraterritorial human rights obligations of states**

When we talk about extraterritoriality, we think about ‘the competence of a state to make, apply and enforce rules of conduct in respect of persons, property or events beyond its territory’ (Kamminga 2012, para. 1) and the human rights obligations of states that extend beyond the borders of states’ territory. Even though the discussion on extraterritorial obligations has been going on for a long time, what remains undetermined is the substance of these obligations. A strict territorial reading of human rights frameworks would render the protection under these frameworks ineffective, when thinking about the protection of these rights in the context of cybersecurity. This holds true in particular in the area of economic, social and cultural human rights, which ‘may directly or indirectly be impaired by cross-border “externalities”’ (Askin 2019, para. 1). Even though the ICESCR does not contain a provision on territorial applicability and despite the fact that the ICJ addressed the primarily territorial character of the obligations under the ICESCR in its Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (para. 112.), the ICESCR was always interpreted to contain an ‘international feature’ (Askin 2019, para. 14) and, therefore, an obligation for assistance and cooperation. However, the contours of the obligations remained blurred. In this regard, jurisdiction serves merely as one threshold criterion (Peters 2018, p. 303), especially in cyberspace which presents ‘new forms of extraterritorial human rights infringements’ (Askin 2019, para. 19). This and other new forms of infringements made revisiting the problem necessary.

The Maastricht Principles on extraterritorial obligations of states in the area of economic, social and cultural rights (*Maastricht Principles*) were drafted in 2011 with the intention to finally make some decisive progress. As the preamble of the *Maastricht Principles* 2011 states: ‘Drawn from international law, these principles aim to clarify the content of extraterritorial State obligations to realize economic, social and cultural rights with a view to advancing and giving full effect to the object of the UN Charter and international human rights’ (para. 8 (emphasis added)). The *Maastricht Principles* follow a ‘facticist conception of jurisdiction’ (Askin 2019, para. 25), envisaged to close the gap in the universal human rights protection, caused by the fact that ‘States still interpret their human rights obligations as being applicable only within their borders’ (*Maastricht Principles* 2011, p. 3). As cyberspace is the space in which the challenges of extraterritorial obligations are not only most visible but also amplified, clarifying the
The scope of extraterritorial human rights obligations of states in online settings is of particular importance. However, whereas the extraterritorial obligation of states to protect civil and political human rights is well established by judgments of the ECtHR (Loizidou v. Turkey; Al-Skeini and Others v United Kingdom; Ocalan v Turkey) and determined by the ‘effective control test’, the protection of social, economic and cultural human rights (so called second generation of human rights) has not yet been equipped with a robust framework of hard legal obligations (Askin 2019, para. 7).

Even though the Committee on Economic, Social and Cultural Rights (CESCR) also relied on the effective control test in the context of Crimea (Concluding Observations on the Sixth Periodic Report of the Russian Federation, paras. 9–10), in many regards the contours of the extraterritorial protection of economic, social and cultural rights are still not defined. This fact may have led Wilde to observe: ‘The Maastricht initiative notwithstanding, commentary on extraterritorial applicability remains skewed towards coverage of civil and political rights, and the determinations by the CESCR and the jurisprudence of the ICJ notwithstanding, international enforcement remains similarly skewed’ (2020, p. 68). Despite this accurate observation, we should not make the mistake to discard the Maastricht Principles.

On the contrary, the Maastricht Principles are a crucial tool that helps us analyse the different dimensions of extraterritorial obligations of states. The Maastricht Principles ‘invite us to see human rights as global public good, and a guide for the reshaping of the international legal order’ (De Schutter 2012, p. vii). The open character of the Maastricht principles offers us a new way of speaking about extraterritorial human rights obligations of states. As De Schutter trenchantly notes, ‘they are sufficiently precise to provide a focal point for deliberations as to how to build international regimes – how to regulate trade, how much to protect foreign investors, or how to allocate the responsibilities in combating climate change – yet they are vague enough not to pre-empt the result of these deliberations’ (2012, p. vii). By approaching the issue in three steps (‘to respect, to protect and to fulfil’) (Maastricht Principles 2011, p. 8), we will show how the Maastricht Principles provide us with a language to formulate standards regarding the obligations of states more precisely. The three different dimensions may, e.g., oblige states to conduct a human rights impact assessment, considering real and foreseeable effects of their conduct abroad, and to put in place measures that ensure that they respect and protect human rights and under specific circumstances fulfil these rights, too. Following the CESCR, in an extraterritorial setting, the main focus lies on the dimension of protection, which means that ‘States parties [are obliged] to take steps to prevent and redress infringements of Covenant rights that occur outside their territories due to the activities of business entities over which they can exercise control, especially in cases where the remedies available to victims before the domestic courts of the state where the harm occurs are unavailable or ineffective’ (CESCR 2017, para. 33).

Enhancing the effectiveness of extraterritorial human rights obligations in cyberspace

The commitment of the WSIS in 2005 to a ‘people-centred, inclusive and development-oriented Information Society’ (WSIS 2005, no. 2), to ‘the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development, as enshrined in the Vienna Declaration’ (WSIS 2005, no. 2), to a stable and secure Internet as a worldwide institution and to the multi-stakeholder approach (WSIS 2005, no. 3) may serve us as guidance in order to identify relevant principles of international law that protects cyberspace as a common interest. We will then show how applying
Protection of cyberspace as common interest via principles

Particularly relevant to ensuring and promoting cybersecurity are the following principles of international law: sovereign equality, the ban on aggression and intervention, peaceful settlement of disputes, the protection of human rights, the cooperation principle (which draws on the principle of good neighbourliness (‘no harm’) and the precautionary principle (‘due diligence’)). Some of these principles have been translated into treaty law in the UN Charter, some are protected under customary international law or are recognized as part of the general principles of international law.

The principle of sovereign equality is a key principle of international law. As a ‘pivotal principle’ (Besson 2011, para. 1) it is also of special importance for cybersecurity. Each state has jurisdiction and power over its territory and over the ICT infrastructure located there; this also means, however, that it bears a responsibility to ensure that no attacks against other states or institutions, which would infringe on international law, are organized or carried out from its territory.

In addition, the non-intervention principle can be brought to fruition: an intense damage to Internet functionality in another state (e.g., by cyber-attacks) could constitute an intervention, although attribution problems will regularly arise. Only some of the attacks originating from the territory of a state represent an ‘intervention’ in terms of international law, because most attacks will be attributable to non-governmental protagonists, or to protagonists whose association with governmental agencies cannot be proven (GGE 2015, para. 28 (f)).

The ban on the use of force prohibits states from using measures of power beyond simple ‘intervention’ (the former being stated in the non-intervention principle). In the context of the Internet, this article could only be applied to especially serious cases of cyberattacks with substantial kinetic effects. The principle of peaceful settlement of disputes is relevant to cybersecurity insofar as any state has the duty, in the event of an incident, to first determine the facts and to collect evidence for attribution of a breach of international law to a particular state. Even if this succeeds, peaceful means of dispute settlement should first be sought. The principle of the protection of human rights is a fundamental principle of international law that is also relevant to cybersecurity. What is problematic under international law are attempts by a state to enforce cybersecurity through an excessive control of the Internet (such as setting up and using surveillance capabilities, or government screening of all Internet communication). The principle of good neighbourliness (UN Charter, Friendly Relations Declaration, art. 74), or ‘no harm’ principle, can be considered as a global principle in the Internet era. Originally only relevant in terms of the relationship with adjacent states, the principle has been gradually extended. In the Corfu Channel Case, the ICJ described the principle as ‘every state’s obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states’ (p. 22).

The ‘no harm’ principle has its roots in the Trail Smelter Arbitration and Lac Lanoux Arbitration. It was formulated in Principle 21 of the Stockholm Declaration of 1972 and Principle 2 of the Rio Declaration of 1992: signatory states are committed ‘to ensure that activities within their jurisdiction or control do not cause damage to the environment of other states or of areas beyond the limits of national jurisdiction’. This can be easily applied to other areas in analogy to the environment. The obligation to prevent cross-border damage has crystallized into customary law. Confirmation of treaty consent to this matter can be found in Art. 194 (2) of the UN Convention on the Law of the Sea of 1982 and Art. 20 (1) of the ASEAN Agreement on the
Matthias C. Kettemann and Anna Sophia Tiedeke

Conservation of Nature and Natural Resources of 1985. Most recently, the ICJ confirmed in the Nuclear Weapons Advisory Opinion (1996, p. 226, para. 29) that the threat to the environment is ‘no abstraction but represents the living space, the quality of life and the very health of human beings, including generations unborn’. In accordance with the ‘no harm’ principle, no state may utilize its dominion in such a manner that would cause damage to other states. In the preventive dimension of the ‘no harm’ principle, a state must take measures to prevent such hazards. Among other things, a commitment to an appropriate infrastructure, the development of emergency plans and the establishment of an international crisis cooperation structure (and culture) can be construed from this.

The shift towards due diligence

The precautionary principle (‘due diligence’) is of special importance for cybersecurity. Firstly, the due diligence principle entails information and consultation obligations (Koivurova 2010, para. 3). In the scientific world, it is controversial as to what extent the precautionary principle has a ‘due diligence’ dimension, or whether the precautionary obligations of states are covered in practice by the ‘no harm’ principle. The Maastricht Principles may give some guidance in this regard, as Principle no. 14 foresees an impact assessment and prevention of adverse effects on economic, social and cultural human rights. Along with state obligations based on individual human rights communicators, recipients and the contents of communications are protected by Art. 19 ICCPR, which has largely crystallized into customary law. Positive obligations related to Internet infrastructure can also be derived from state obligations to provide protection and assurance pertaining to information- and communication-related rights (Kettemann 2020, p. 226). Following the Maastricht Principles, states are therefore obliged to respect, protect and fulfil the sustainability and security of the networks in order to allow individuals to realize their human rights, extraterritorially.

With some justification, normative principles for the regulation of cybersecurity can therefore be derived from the principle of due diligence that is reflected in Principle 14 of the Maastricht Principles. As a result, the responsibility of states includes not only the duty to prevent and stop cyberattacks originating from their own territory and to (proactively) establish a legal system that ensures and fosters cybersecurity (Schmitt 2015), but also to provide effective remedy in such cases.

All of these are duties which, when translated for cybersecurity, imply certain ‘preparatory’ duties for states as substantiation of the precautionary principle. We are all neighbours on the Internet, and just as states cannot let their power plants pollute the air in neighbouring states, their ill-secured national networks and tools can be misused to attack third countries. They who leave a gun lying around or a car unlocked can be held liable for what happens with the gun or the car. States that fail to adhere to their due diligence obligations leave themselves open to attack and may be held responsible under, e.g., Articles 2 or 9 ASR.

In its preventive dimension, the due diligence principle helps to identify the obligations of states with regard to cybersecurity, particularly with regard to cybercrime, global cooperation and establishment of capacities. Cybersecurity due diligence was described as part of customary international law, whereby particularly the following preventive duties have emerged as recognized obligations under international law: that governments and other stakeholders bolster cybersecurity and develop cybersecurity strategies to protect crucial infrastructures (UN GA Res 64/221), that states (and other relevant stakeholders) work together more closely in the fight against cybercrime and cyberterrorism, and that they ratify conventions such as the Convention on Cybercrime of the Council of Europe, that states conclude treaties promoting
cooperation between their police authorities and that states establish confidence-building measures and increase the level of information sharing, generally as well as (and especially) in the event of cybersecurity related incidents (UN GGE 2013, paras 22, 26 et seq.).

This can be fulfilled, for instance, by ‘passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders’ (Sklerov 2009, p. 62). The GGE also agreed that human rights law applies to cyber activities and that ‘States must not use proxies to commit internationally wrongful acts’ (UN GGE 2013, paras 20–23). Confidence-building measures are more extensive than obligations under international law, ensuing from the duty of cooperation (OSCE Decision No. 1202, 2016). They are relevant to the evolution of legal norms, however, insofar as they indicate the direction of how obligations under international law are developing.

In fact, the Maastricht Principles take the due diligence principle one step further. With the three steps approach, the Principles have contributed to a more concrete understanding of the extraterritorial human rights obligations of states.

The duty to respect is designed as a negative obligation that requires states to directly or indirectly refrain from infringing upon human rights outside their territory. It is widely recognized, and the CESC in its General Comment No. 14 even uses the language of ‘have to’ with respect to these negative duties (E/C.12/2000/4, para. 39). This dimension can, therefore, easily be integrated into ‘existing human rights architecture’ (Askin 2019, para. 31). However, it also poses some challenges in the context of the distinction between positive and negative human obligations of states, and the wide scope of protection carries the risk that these obligations become frayed and thus ineffective.

The duty to protect is a positive obligation. However, it depends on the degree of involvement. The protective ambit increases relative to the state’s involvement. The duty to protect may require states to establish mechanisms to ensure that cross border activity of companies has no adverse effects on human rights. This can be understood as a duty to implement a legal framework that ensures ‘human rights due diligence in order to identify, prevent and mitigate the risk of violations of the Covenant rights’ (CESCR 2017, para. 14). If a state fails to implement an effective legal framework even though it has the capacity, it might violate its due diligence obligations under international law.

The duty to fulfil reflects the third step of effective extraterritorial protection of human rights. The ‘obligation of international assistance and cooperation’ (ICESCR, art. 2(1)) is to be understood as an obligation of states that have the possibility to assist to do so. This dimension rests controversial (Askin 2019, para. 37) and has merely been considered a secondary dimension of the extraterritorial obligations. A state will not be obliged to fulfil the right to cybersecurity in a third state, but it is obliged to respect it and may be obliged to protect it, depending on the level and intensity of its influence/involvement. This shows that, dogmatically, it is becoming increasingly difficult to differentiate legally between the three dimensions. However, in the multistakeholder setting of cybersecurity, the duty to assist and cooperate could offer an effective tool to ensure a high level of cybersecurity for individuals as well as for states themselves.

**Shedding some light on the grey zones**

In the light of the importance of the Internet for states, business and society, cybersecurity – as a prerequisite for a reliably functioning and secure Internet and therefore for the protection of human rights – has become a global community interest, which needs protection. The
technologicalization and informationalization of many key infrastructure provision functions and of many industry control systems open up new vulnerabilities within states and across territorial borders that can threaten, if an attack is substantial, international peace and security and thereby humans and their rights. Similarly, the increased use of mobile devices and cloud computing and the use of social networks increase the vulnerability of citizens to acts of cybercrime.

Cybersecurity is a key functional condition for an era defined by information and communications technology. States must step up and take on the responsibility through an (effective) extraterritorial application of human rights and the principles and processes of international law. Otherwise, there is no possibility to shed light onto the still existing grey zones of international law in the protection of cyberspace (Schmitt 2017, p. 21). Only if the obligations are clarified, the room for exploitation of grey zones will shrink and, as Schmitt put it: ‘The brighter the red-lines of international law as applied to cyber activities, the less opportunity States will have to exploit grey zones in ways that create instability’ (2017, p. 21). Kilovaty therefore promotes a ‘new’ human right, the human right to cybersecurity (2020, p. 52). He envisages a ‘robust human right to cybersecurity’ (2020, p. 54) that protects individuals from ‘carefully tailored cyber operations’ and, e.g., establishes encryption in private communication of individuals as a default standard as was suggested by the UN Human Rights Special Procedures, Mandate of the Special Rapporteur in his Encryption and Anonymity Follow-Up Report (p. 4 no. 7 and HRC 2017, para. 9).

Establishing a baseline cybersecurity or more advanced forms are necessary for states to implement in order to meet their obligations under international human rights law: the debate on how best to ensure a stable and resilient Internet for all is far from over – and it is international law that provides the impetus, frame and objective of the debate. The Maastricht Principles serve and will continue to serve as guidance for the extraterritorial application of obligations under international law. However, applying the recent judgment of the German Federal Constitutional Court (BND judgment, 2020) and considering the growing body of literature on extraterritorial human rights obligations, especially cyberspace-related activities might emerge as a reference field for the diminishing importance of the difference between acts ‘from within’ a territory that have extraterritorial applications and acts ‘outside of a territory’ that have outside (or even inside-of-territory) implications.

Succinctly put: human rights-related extraterritorial obligations of states serve to make this obligation more concrete and are important normative vectors for an increasingly robust protection of cybersecurity by all states, within and outside of their territories. Notwithstanding recent trends towards reterritorialization on the Internet, we are and continue to be all neighbours in cyberspace with a potential Trail Smelter lying in each smart refrigerator, home router and unsecure local library network. While the challenges this implies for international law, human rights obligations and international legal scholarship have not all been clearly delineated yet, some key ones are distilled in this contribution.

Note

1. This contribution builds on ideas previously published in Kettemann, The Normative Order of the Internet (Oxford: Oxford University Press 2020). The authors express their thanks to Mark Gibney, Markus Krajewski and Vito Todeschini for valuable comments and to Rike Heyer, Johanna Friederike Stelling (Hamburg) and Ilse Kettemann (Graz) for valuable editorial support.
Cybersecurity and ETOs of states

References


Agreement on the Conservation of Nature and Natural Resources, (1985) Association of South East Asian Nations (ASEAN)


Arbitral Tribunal (1957) Lac Lanoux (France v. Spain), 12 R.I.A.A. 281, Arbitral decision of 16 November 1957 United Nations, Reports of International Arbitral Awards XII.


Communication by the European Commission to the European Parliament, the European Council (2014) the European Economic and Social Committee and the Committee of the Regions: Internet Policy and Internet Governance, Europe’s Role in Shaping the Future of Internet Governance, COM/2014/072 final.

Council of Europe (2012) Parliamentary Assembly Resolution 1877 on the protection of freedom of expression and information on the Internet and online media.

Cyber-Sicherheitsstrategie für Deutschland (2016) Bundesministerium des Innern, für Bau und Heimat.


European Court of Human Rights (ECHR) Judgments:


_______ (1949) Corfu Channel Case (United Kingdom v. Albania), Merits.


415


United Nations General Assembly (UN GA) Resolutions:


(2010) Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, A/RES/64/211.


UN Open Ended Working Group (UN OEWG) (2021) Final Substantive Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security, UN Doc. A/AC.290/2021/CRP.2
Cybersecurity and ETOs of states


WSIS (2005) Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6 (Rev. 1).