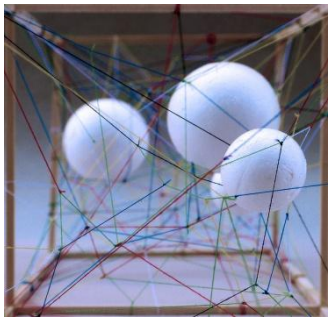
ESIL Reflections
Editorial board: Anne van Aaken, Jutta Brunnée, Jan Klabbers, André Nollkaemper (editor-in-chief)

January 10, 2014 Volume 3, Issue 1



'Cyberspace' by Gamdrup (cc)

International Law and 'Cyber Space'

Prof. Andreas Zimmermann, LL.M. (Harvard)
University of Potsdam

I. Introduction

Readers of this piece will have received it via email or will have accessed it online. Most probably they will also read their newspapers online and will have also purchased some of their Christmas gifts in the same manner. These simple examples alone, and manifold others could obviously be added, demonstrate to what extent communication via the internet shapes our day-to-day-life, far beyond the news that has recently made the headlines.

Yet, it is not the first time that international law faces new technological developments. In earlier times, to give but two examples, international law was in a similarly sudden manner confronted with radio waves crossing boundaries, and with mankind being able to reach extraterrestrial bodies; and each time it was taken for granted that such human behaviour was governed by existing norms of international law.

As in those earlier cases, activities in 'cyber space' too are governed by international law as such, and be it only by the norm that where no (general or specific) rule prohibiting the behaviour in question exists, States retain their freedom to act.[1] However, as in those earlier scenarios, it is for lack, for the time being, of more specific rules, that the basic and general norms of international law govern cyber activities, including concepts such as jurisdiction or attribution. Given the indeterminacy of certain of these more general rules, their inadequacy when it comes to cyber activities, as well as the lack of generally accepted, efficient and rule-based inter-State international governance structures, 'cyber space' nevertheless constitutes a major challenge for international law as it currently stands.

[1] See generally on that issue U. Fastenrath, Lücken im Völkerrecht - zu Rechtscharakter, Quellen, Systemzusammenhang, Methodenlehre und Funktionen des Völkerrechts (1991), *passim*.

It is against this background that one has to assess the extent to which human activties in ‘cyber space’ are governed by international law, and what the applicable norms are.

II. Notion of ‘cyber space’ and its (ir)relevance

Not infrequently ‘cyber space’ is referred to as a mere virtual space where computer-mediated communication takes place but which may not be spatially located. Yet, to state the obvious, any such communication requires hardware that must be located somewhere. What is more, any such information is then physically routed through the territory of one or more States (and possibly through outer space) before it reaches the addressee, which, again, confirms that there necessarily exists a territorial nexus of *any* activity in ‘cyber space’ to at least one State. Accordingly, while ‘cyber space’ might describe a phenomenon of information being routed through various jurisdictions, it still does not constitute some new form of ‘outer space’ where no State could, as a matter of international law, exercise its jurisdiction.[2] Rather, it is more an issue of technical feasibility which State (or international organization) is in a position to regulate behaviour in ‘cyber space’, and also an issue of the willingness of States to agree on more specific rules which States specifically (and to what extent, if at all, and if so, in which manner) may regulate such behaviour.

III. Challenges ‘cyber space’ poses for international law

Although communication in ‘cyber space’ is *de jure* subject to the jurisdiction of one or more States, and thus does not constitute a novel phenenomen for international law as such, communication via the internet nevertheless, given its specific technical characteristic features, does pose new challenges for international law. For one, and more generally, given the speed by which technological developments take place concerning ‘cyber space’, the more traditional ways of creating norms of international law, be it by way of multilateral treaties, be it by way of developing rules of customary international law, run the danger of being the hare in a new form of a ‘hare and the hedgehog’-race. As a result, only rather general and under-complex norms of international law tend to be applicable in any given cyber space-related scenario.

This phenomenon is compounded by an unwillingness of States, as well as non-State actors such as multinational enterprises that have a technological lead in ‘cyber space’, to have their behaviour in ‘cyber space’ regulated by specific treaty-based rules; these actors instead tend to take advantage of a lack of effective international regulation of their activities. By the same token, given the enormous technological gap that exists, on the one hand, between highly industrialized States such as, to give but one example, the United States and multinational companies such as Google or Microsoft, and small and less developed States on the other, many States are *de facto* simply not in a position to exercise even a minimal form of control of ‘cyber space’ activities emanating

[2] See generally as to jurisdictional issues related to ‚cyber space’ J. Zekoll, Jurisdiction in cyberspace, in: Günther Handl/ Joachim Zekoll/ Peer Zumbansen, Beyond territoriality - transnational legal authority in an age of globalization (2012); p: 341-369.

from or affecting their territory; indeed, they might even lack sufficient capabilities to frame an appropriate regulatory (legal) framework governing such activities.

Moreover, both the *de facto* (but *de facto* only!) de-territorialisation of 'cyber space' activities (in that information is being routed through a large number of States and territories), as well as the sheer amount of information being produced, lead to a lack of effective regulatory mechanisms to be used by States when it comes to detecting, and eventually addressing, harmful activities in 'cyber space', regardless of whether they emanate from private actors or from other States.

Another aspect of the *de facto* de-territorialisation of 'cyber space' activities can be seen in the fact that the effects of activities in 'cyber space', even when they emanate from States, take place abroad, which in many cases raises the question whether the international (be they treaty-based or of a customary nature) obligations a State has undertaken also apply in such cross-boundary and extraterritorial settings, human rights obligations being a particularly relevant issue at hand.

Moreover, given the technological environment in which 'cyber space' activities occur, it will be often, if not always, difficult or even impossible, to trace back any such activities, even when they emanate from actors the behaviour of which would otherwise be attributable to a given State under applicable norms of international law, codified in the ILC Articles on State Responsibility.[3] Accordingly, in many cases, while being applicable as such, the general law on State responsibility is, to a large degree, unable to cope with 'cyber space'-related activities.[4] This in turn requires international law to either develop specific norms of attribution (including specific evidentiary norms), or to come up with specific primary norms that can adequately address the matter.

Yet another challenge concerning 'cyber space' relates to the possibility of States (and indeed private actors) to effectively collect comprehensive information on any given person active on the internet in one way or the other. This reality leads to the question whether human rights standards, and namely guarantees relating to privacy, also apply in 'cyber space' as a matter of their applicability *ratione materiae* and *ratione loci*.

Finally, a last challenge relates to the lack of any form of effective inter-State governance structure of 'cyber space', and indeed the very question whether such structures are needed at the first place.

Having thus outlined some of the more *general* challenges, this piece will now also briefly address some of the more *specific* international law issues as they arise with regard to activities in 'cyber space'.

[3] GA Res. A/RES/56/83, Annex.

[4] See on this issue *Michael N. Schmitt,* Cyber Activities and the Law of Countermeasures, in: Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (2013), p. 659 et seq.(668 et seq.)

IV. ‘Cyber space’ and interstate due diligence obligations

So far, much of the legal discourse on ‘cyber space’ activities has been framed in terms of ‘cyber warfare’, and thus in terms of *jus ad bellum* and *jus in bello*.[5] Yet, this debate is, to a large degree, misplaced. While, obviously, both sets of rules, do apply, as a matter of course, to activities in ‘cyber space’, such activities do not normally reach, and so far have not reached, the threshold of Art. 2 (4) UN Charter.

Rather, it is the ‘normal’ rules of international law, applicable in peace-time, that govern the matter. More specifically, general rules of due diligence, as specified *inter alia* by the International Court of Justice in the *Corfu Channel* case, oblige States to ensure that their territory (including ‘cyber space’-related infrastructure located on their territory) is not being used for acts that unlawfully harm other States.[6] Some of the crucial, so far largely unanswered legal questions, deriving from this generally accepted, yet quite general, concept of due diligence, relate, when it comes to ‘cyber space’, to the specific content of such due diligence obligations, *i.e.* to the question what level of precautions a State has to undertake, taking into account its level of technological development. Another question concerns whether transit States (*i.e.* States through which harmful data are being processed) and victim States (*i.e.* States where the harm materializes) are also under such due diligence obligations (and, if so, which and to what extent).

VI. ‘Cyber space’ and the prohibition of the use of force

It is, of course, conceivable that a harmful ‘cyber-space’ activity that is attributable to a State amounts to a violation of Art. 2 (4) UN Charter, given its character and effects. Whenever such use of force even reaches the threshold of an armed attack, as defined by general rules of international law and, in particular, the jurisprudence of the International Court of Justice, in principle, the right of self defence comes into play. In that regard, ‘cyber attacks’ (provided they do amount to armed attacks in the first place, which they will only in extremely rare circumstances, if at all), just like other armed attacks, might raise the question whether such attacks, if they emanate from non-State actors the acts of which are not attributable to a State, do trigger the applicability of Art. 51 UN Charter.

What is more, in such scenarios the question who carries the burden of proof will usually arise, not only as to the attribution of a given activity to a *State or a non-State actor*, but also as to its attribution to a *specific* State. In these respects, the holding of the ICJ in the Oil Platforms case[7] is of particular relevance.

---

[5] But see most recently the various contributions in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (2013), *passim*.

[6] *ICJ, Corfu Channel Case,* Merits, (1949) ICJ Rep 4, para 22: „(...) certain general and well-recognized principles, namely: elementary considerations of humanity, even more exacting in peace than in war; the principle of the freedom of maritime communications; and every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States“.

[7] ICJ, *Oil Platforms,* Merits (2003) ICJ Rep 161, para 59.

VII. 'Cyber Space' and *jus in bello*

Once the threshold of an (international or non-international) armed conflict has either been reached by a 'cyber attack' as such, or where cyber attacks are being undertaken as part of already ongoing hostilities, applicable norms of international humanitarian law also govern 'cyber space'-related activities that are undertaken as part of the armed conflict against another party to the conflict (or indeed neutral powers) and that constitute an 'attack' within the meaning of international humanitarian law. Yet, 'cyber warfare' raises significant, and so far largely unresolved, questions *inter alia* as to the character of installations as military objects, as well as to the legal characterization of persons involved in 'cyber operations,' which questions too State practice has not yet fully addressed.[8]

VI. 'Cyber space', human rights and data protection: the need to develop appropriate legal standards

One of the most recent questions triggered, in particular, by activities of the US National Security Agency, relates to the protection of human rights in 'cyber space' and, in particular, relates to the right of privacy, as codified in Art. 17 ICCPR. Apart from specific treaty-based norms that may be applicable in a given case (such as *e.g.* the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[9]), the area is so far under-regulated. For one, it is already doubtful whether *de lege lata* all, or at least some, electronic data available in 'cyber space' are protected by the concepts of 'privacy' and / or 'correspondence' under Art. 17 ICCPR, one of the main problems being whether the 1966 ICCPR (or parallel norms of customary international law) may be interpreted in such dynamic a manner as to also cover areas not foreseen in 1966.

What is more (provided one assumes that the relevant rules of international do apply *ratione materiae* to 'cyber space'), it is doubtful whether, under either customary law or Art.17 ICCPR, an individual not present on the territory of a State collecting the private data of this individual via the internet is 'within the jurisdiction' of the said State within the meaning of Art. 2 (1) ICCPR (or the parallel norm of customary law), so as to trigger the applicability of the respective human rights norm.

Given the indeterminacy of these and related issues, it is more than laudable that Brazil and Germany recently launched an initiative within the United Nations to further clarify and develop applicable norms of international law, which led the General Assembly to adopt, by consensus, a resolution[10] requesting the United Nations High Commissioner for Human Rights „to present a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of

[8] See generally on those issues the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013).
[9] CETS No.: 108; text available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[10] Text available at http://www.auswaertiges-amt.de/cae/servlet/contentblob/660692/publicationFile/186815/131127_Right2Privacy_EN.pdf

digital communications and collection of personal data, including on a mass scale to the Human Rights Council".

VIII. 'Cyber Space' governance: which way forward?

Unlike most other areas of international law 'cyber space' so far lacks any significant inter-governmental governance structure. Rather, key private organizations acting with the aim of preserving the operational stability of the Internet, such as ICANN, the "Internet Corporation for Assigned Names and Numbers," as well as interconnection and peering agreements among internet service providers, provide for some form of self-regulatory capabilities of 'cyber space'. It remains to be seen whether this form of self-regulation will continue to be able to provide sufficient safeguards as to the functioning of the internet, in line with the applicable principles of international law outlined above, or whether one should not aim at some form of intergovernmental internet governance. Yet, recent initiatives within the ITU system have shown that such attempts of coming up with universally accepted inter-state governance structures might run the risk of being (mis-)used for subjecting 'cyber space'-based activities to over-broad governmental regulation, and thus run the risk of limiting the above-mentioned human rights of internet users.

IX. Outlook

As with other novel areas of international law which have developed in the last decennials, such as international environmental law,[11] only time will tell whether the international community of States will be able and willing to over time come up with specific and adequate rules of international law applicable to 'cyber-space'.

Pending such a development, States and other actors can only rely on general, and thus necessarily relatively vague, rules of international law, such as the concept of due diligence, and attempt to apply them to human activities in 'cyber space'. Yet, as mentioned, this is nothing peculiar to 'cyber space' – rather we have previously seen the very same development in other areas, international environmental law again being a particularly relevant example at hand before specific treaty regimes were established.

[11] As to the possibility of transposing principles developed within international environmental law to ‚cyber-space,' see Thilo Marauhn, Customary Rules of International Environmental Law - Can they Provide Guidance for Developing a Peacetime Regime for Cyberspace?, in: Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (2013), p. 465 et seq.