In his insightful LJIL article Kubo Mačák discusses the underdeveloped state of international cyber security law. He assesses that the absence of cyber security law-making has created a power vacuum that has been filled by non-state actor initiatives, such as the Tallinn Manual. He calls on states that now is the time to reclaim their central role in international lawmaking, in the short-term by articulating their opinio iuris more clearly, in the mid-term by overcoming their treaty aversion, and in the long-term by moving towards the adoption of a multilateral cyber security treaty.

While I fully agree with Mačák's central argument for more state engagement I would like to highlight a problem that states seem well-advised to address in their future engagement with international law in cyberspace.

**The need to distinguish between technical cyber security risks and content-based information security risks**
States seem well-advised to distinguish more clearly between technical cyber security and content-based information security risks. I submit that with regard to technical cyber security the three-step development Mačák points at is both feasible and desirable; that however with regard to content-based information security risks a multilateral treaty is hardly feasible and might even have severe downsides.

**First type of risk: Technical cyber security risks**

Technical cyber security risks are risks for the confidentiality, availability and integrity (CIA) of information and communications technology (ICT). This category of cyber incidents typically involves deleting, altering or revealing data saved on ICT and is characterised by breaking into an ICT system, for example through hacking, phishing or inserting malware – for such security risks ICT is the actual target. Already the violation of the CIA of ICT realizes the intended serious adverse consequence. Such serious consequence can range from disabling an electrical grid through violating the integrity of the ICT (e.g. the Black Energy attack in 2015), to temporarily or permanently hindering the availability of information or data on the ICT (e.g. the ransomware ‘Wanna Cry’ attack in 2017, or the Distributed Denial of Service attack on Estonia 2007) or to violate the confidentiality of the ICT (e.g. DNC hack in 2016).

**Second type of risk: Content-based information security risks**

By contrast, content-based information security risks are security risks which are facilitated or amplified by cyber tools but for which ICT is not the actual target. Examples are disinformation (dissemination of ‘fake news’, employment of ‘social bots’, e.g. in the US presidential election or the Brexit referendum in 2016) or incitement to terrorism (e.g. on social media). For such security risks the target is ultimately human intelligence, the CIA of ICT remains fully intact. The serious adverse consequence materializes
through the successful impact on human intelligence but is independent from the CIA of ICT.

**Indiscriminate discussion of content-based information security and technical cyber security risks**

Although both security risk are evidently substantially different both risks are often used synonymously in the international legal discourse and in public media – see here and here, adding to a general sentiment of cyber insecurity as the new normal. The distinction is rarely explicitly made – notable exceptions can be found here and here. This synonymous discussion of both risks is problematic for substantial legal progress for several reasons.

**Contestation exacerbated**

Most importantly, it risks hindering international consensus-building on cyber security norms by entangling the more consensual area of technical cyber security risks with the highly politicised and contentious area of content-based information security risks.

With regard to technical cyber security risks recent state practice shows that states gradually realize their commonly shared interests in stepping up cyber resilience and increasing cooperation, for example with regard to protecting ICT-dependent critical infrastructure, to preventing and mitigating international botnet operations or to cooperating in cases of internationally spreading cyber incidents, such as WannaCry). States have increasingly concluded bilateral Memoranda of Understanding (MoU) on technical cyber security risks, notably also sidelining the two blocks of the alleged ‘digital divide’, such as the US-China Memorandum of Understanding of 2015. India is systematically building a worldwide net of bilateral agreements to increase ICT resilience and cooperation, and also other countries, such as Singapore, follow suit (see here and here). The European Union Directive on Security of Network and Information Systems (NIS) tackles technical cyber security risks by establishing a network of computer security
incident response teams (CSIRT) and a cooperation group for strategic cooperation. The protection of CIA of ICT is also one of the core purposes of the Draft Convention on Cooperation in Combating Information Crimes proposed by Russia in 2018 (Art. 1 [b]).

By contrast, it is highly contested between states how to address content-based information security risks. Regulation of content-based information security risks touches upon content control and hence upon highly divergent and politicised stances on Internet governance, human rights and the concept of information sovereignty. While the concept of sovereignty is recognized in cyberspace its exact contours and implications for Internet governance are far from a shared understanding. Multi-lateral, multi-stakeholder and hybrid ‘in-between’ approaches to Internet governance deviate significantly as to the extent of content limitation by states. Despite partial convergent tendencies it is almost certain that substantial disagreement on Internet governance and its political implications will remain in the future. Tellingly, even where international consensus exists on which content-based security risks need to be counteracted – for example with regard to child pornography or certain forms of hate speech – there is disagreement on how to counteract these content-based security risks; the Budapest Convention of the Council of Europe on Cybercrime of 2001 for example requires state to state requests for assistance or the consent of the concerned private party to access stored computer data (Art. 31 [1], 32 [b]); by contrast, the Draft Convention on Cooperation in Combating Information Crimes of 2018 would allow data gathering suo motu without prior request to another state party or the consent of the concerned private party (Art. 44).

It seems hence rather futile to expect substantial consensus-building on information security risks in the international sphere.

**Risks for right to freedom of expression and information**
Moreover, moving quickly towards a new multilateral treaty that includes content-based information security risks might plausibly have detrimental effects on the right to freedom of information and freedom of expression online. Under human rights law restrictions of the rights under Art. 19 ICCPR must be sufficiently clear, accessible and predictable.

Presently, it seems hard to envision a new multilateral treaty for cyberspace that could satisfy this requirement. An open-ended clause akin to the proposed draft code of conduct for information security introduced by Russia and China in the UN General Assembly in 2011 (and an updated version in 2015) with states vowing to ‘curb the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment’ would fall short of being sufficiently clear, accessible and predictable. Notably, the concern of insufficient clarity, accessibility and predictability has also been raised against the German network enforcement act of 2017, aimed to tackle hate speech and ‘fake news’. As international legal scholars currently discuss election meddling through disinformation as a prohibited intervention under Art. 2 (7) UN Charter (see here and here) clear legal criteria to ascertain the intervention threshold have not yet evolved.

These examples show that it is extremely difficult to strike a fine balance between the right to freedom of information and expression and the security need to limit content disseminated via ICT. A broad one-size-fits-all restriction clause in a new multilateral information security treaty could plausibly grant a carte blanche for surveillance and content control to authoritarian states.

With respect to human rights it seems hence more promising to slightly deviate from the three-step development Mačák points at and to adopt a more tailored and evolutionary approach with regard to information security risks and to, inter alia, strengthen ‘soft’ parameters, such as transparency, media and information literacy.
and self-regulation of private intermediaries (see the [High Level Expert Group](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/) on Fake News and Online Disinformation of March 2018 for the European Commission calling for a ‘self-regulatory approach based on a clearly defined multi-stakeholder engagement process’), and simultaneously clarify the application of already existing multilateral treaties, such as the ICCPR, to content-related risks in cyberspace.

**Conclusion and outlook**

At the present stage one can only hypothesize which direction the future international discourse on international law and cyberspace will take. It is uncertain to what extent states will pick up non-state actor initiatives, such as the rules of the Tallinn Manual – a recent case study draws a rather skeptical interim conclusion. Also the forum for future global discussion is uncertain – after the failure of the UN GGE 2017 to conclude on a report the continuation of the UN GGE remains an option, but also an open-ended working group, a cyber committee of the General Assembly or the creation of an inclusive body for interaction of both state and non-state actors within the OECD have been discussed (see [here](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/) and [here](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/)).

Yet, regardless of the forum the example of the UK Attorney General [statement of 23 May](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/) shows states’ engagement with international law and cyberspace will rather increase than decrease; more states begin to realize that – just like Mačák had argued – it is in their self-interest to articulate their cyber opinio iuris. To what extent states will distinguish more clearly between [technical cyber security risks](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/) and [content-based information security risks](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/) remains to be seen (see [here](https://voelkerrechtsblog.org/disentangling-the-cyber-security-debate/)) – however, and this is the main argument here, they would be well-advised to do so.

Leonhard Kreuzer is a Research Fellow at the Max Planck Institute for Comparative Public Law and International Law, Heidelberg, Germany.

This post continues our cooperation with the Leiden Journal of International Law (LJIL). It is a reply to Kubo Mačák’s article ‘From

ISSN 2510-2567

Tags: Cyber Security, Human Rights, Peace and Security

Related

On 'cyber trafficking' and the protection of its victims
26 July, 2017
In "Discussion"

‘Cyber’ Trafficking? An Interpretation of the Palermo Protocol in the Digital Era
28 June, 2017
In "Discussion"

Security mindsets and international law: thinking differently about security and adjudication
22 September, 2014
In "Discussion"

PREVIOUS POST

CfP: Cultural Heritage in a Post-colonial World – New Framings of a Global Legal Problem

NEXT POST

This is the most recent story.

No Comment

Leave a reply

Logged in as ajv2016. Log out?