Cybersecurity diplomacy: business and tech replacing the states?

Key words: cybersecurity diplomacy, international cybersecurity, power vacuum, norm-making, UN GGE, patchwork cyber governance, Digital Geneva Convention, Tech Accord, Siemens, Nornikel, GCCS.

The domain of global politics was traditionally formed by state actors, especially in the security field. However, the emergence of new technologies and subsequent challenges for nation-states brought some new actors to the table for talks.

Recent 20 years have seen a bunch of state efforts to come to a compromise on cyberspace regulation and the use of ICTs. Primordially, ICTs were seen from the angle of opportunities and innovation, meanwhile, only a small portion of governments voiced the concern about the risk of ICT abuse in military purposes; but today's background urges the necessity of cyberspace regulation.

Regulation of whatever subject on the international level is not a plain task. Cyberspace by its nature requires a special approach that definitely differs from previous legal exercises that states undertook in the past. The hardships in the regulation of cyberspace consist of many factors. Firstly, there are various discourses for cybersecurity understanding: interpretation of what is actually “secure” in cyber/information space differs from “eastern” to “western” states, as well as their perception of threats coming from the cyber domain. This discrepancy hampers the state dialog on rules and norms of “responsible behavior”. Secondly, we witness the “crisis in international cyber law”. After the five rounds of the UN Group of governmental experts (GGE) we can see the unwillingness of member states to develop the customary international law applicable to cyberspace. The process of acknowledgment that the existing international law is

---

1 Russia sponsored the first UN resolution on “Developments in the field of information and telecommunications in the context of international security” in 1998. (A/53/576)
applicable to it took almost 10 years since the kick-off meeting in 2004.⁴ In 2015 the states made a good progress building on the achieved consensus and broaden the list of non-binding norms and rules for state behavior in cyberspace. Unfortunately, the last convocation of the working group in 2017 ended ineffectually and left the whole process at a risk of a standstill.⁵ However, Russia will push the next convocation of the GGE for 2019. Despite the failure of the fifth group to conclude the work with a consensus report, “dozens of states have already expressed their readiness for this work within the UN GGE. There is a queue to enter this limited number of experts, which has expanded from 15 to 25 countries over time. Today, there are 68 countries wishing to join, which are trying to enlist the support of the Russian side, as the organizers of this process at the UN site”⁶. It is worth mentioning that the 2017 GGE collapsed, among other reasons, due to the position of the US and their supporters that the GGE format exhausted itself.⁷

Definitely, the main fault line between two camps was the disagreement on the applicability of international humanitarian law as it “would legitimize a scenario of war and military actions in the context of ICT.”⁸

Other reasons for state's impotence to agree on cyberspace regulation also deserve attention. Apparently, states are keeping a wait-and-see attitude towards any normative novelties. In addition, the articulation of cyber norms automatically imposes related restrictions on state actions in cyberspace: they have to acknowledge the availability of particular cyber capacities in order to further restrict them for maintaining the cyber stability. It is obvious that neither of the great powers will admit having in disposal a list of offensive cyber tools that enable them to conduct espionage, intrude into critical infrastructure networks, or influence the outcomes of elections. Until there is no quantifiable subject of talks in regards to cyber weapons, it is unlikely that states will make it similar to strategic offensive arms limitation treaties during the cold war, at least in the nearest future.⁹ Moreover, any dispositive norms for cyberspace will not be

---

⁴ The first consensus report of the UN GGE containing this provision was signed in 2013.
⁹ The negotiations on strategic offensive arms were stalled for a long time, until the parties agreed on the list and characteristics of the types of weapons that were acceptable by Russia and the USA and allowed for the accurate calculation of arms units.
counted as equal to imperative ones that explicitly prohibit particular misbehavior in cyberspace.

One should not forget that cyberspace is not a “lawless territory” despite the arguments above. On the contrary, it resembles “patchwork cyber governance” - bilateral cybersecurity agreements as well as regional systems of collective cybersecurity for NATO, CSTO, and SCO, for instance.\(^{10}\) Also, there is an increase in a number of national and regional regulation covering issues of cybercrime, data protection and localization. All these mechanisms are applicable to a limited scope of activities in cyber/information space, but they shouldn’t be neglected because they set up frameworks for member-states and consequently define the common point of view on cybersecurity.

Nevertheless, the idea of a comprehensive global treaty on cyberspace, similar to the one on the Antarctic, seems to be more and more unviable. Firstly, the process of its agreement would take too much time, while negotiations always happen with a time lag behind the technology developments. Secondly, states should conciliate their positions on the key issues for cybersecurity; otherwise, there is no progress to be expected. The last 10 years were devoted exactly to the discussions of what is admissible in cyberspace: various countries promoted their projects supported by expert and international community. To mention a few of prominent initiatives: International code of conduct for information security, promoted by SCO countries; the Russian proposal of the Convention on International Information Security; OSCE Confidence Building Measures to reduce the risk of conflict stemming from the use of ICTs; G7 Declaration on Responsible States Behavior in Cyberspace; Global Conference on Cyberspace launched in London to discuss the cybersecurity issues on the high level.\(^{11}\) Despite all these parallel processes tried to cope with cybersecurity, they contained competing discourses and distracted states from real cooperation. In the end, it was acknowledged, that it is better to come to a consensus on a range of general norms and rules that would be non-binding, but acceptable to everyone.

But with general norms and rules, too, it is not so easy. (Finnemore and Hollis, 2016) indicated that in the pursuit of harmonization of the rules, all participants forgot that

\(^{10}\) NATO Cyber Defence Pledge, 2016 [https://www.nato.int/cps/en/natohq/official_texts_133177.htm](https://www.nato.int/cps/en/natohq/official_texts_133177.htm)


Intergovernmental agreement of SCO countries on cooperation in promoting international information security, 2009

in "cultivation of cyber norms" the process is important, not the final result in the form of a coordinated text. In addition, the norm itself is a very tricky construct, as not everyone has a full understanding of its relationship with the law as such. In addition, the meaning of norms, despite they can be enshrined in the document, can be modified over the time, as those who use them constantly interpret norms according to the context.

In summary, today the majority of powerful states remains silent and avoids signing any legally-binding agreements on cyber norms, on the reasons listed above, as far as it will impose legal responsibility for in compliance. This situation leads to the “vacuum of power” to produce cyber norms, that is why non-state actors incentivize their efforts to get the advantage of the state's bewilderment.  

These new actors – business and technical community - are getting powerful, as they produce content, soft and hardware, own and operate critical Internet infrastructure. Lack of cyber capacities for proper incident response and investigation forced the establishment of CERTs/CSIRTs. They vary from national\textsuperscript{14} to a specific industry/government sector. Recent Internet Governance Forum in 2017 mentioned the phenomenon of CERT diplomacy, as such cooperation requires a high level of trust and strong personal connections between CERT members.\textsuperscript{15} Governments are suspicious of each other due to different political reasons, while tech actors seem to be much more cooperative in security issues.

Business is also interested to participate in cybersecurity debate as it suffers from cyber attacks too. There is a demand for some global code of conduct to protect common cyberspace. Microsoft pioneered in 2014 with the proposal of Digital Geneva Convention – six basic principles for international cybersecurity, applicable in the peaceful time in contrast to the Tallinn Manual. Since Microsoft had been actively promoting its project,\textsuperscript{16} last year brought to us a series of other non-state proposals: Tech Accord, Siemens

\textsuperscript{12} Сотоношение норм и права. Что из чего вытекает Simply put, laws can serve as a basis for formulating norms, just as norms can be codified in law.
\textsuperscript{14} https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Organizational-Structures.aspx
Charter of trust, Nornikel Charter of information security for critical industrial facilities, and two norms proposed by the Global Commission on Cyber Stability (GCCS).17

For the purpose of the paper, we took the norm concept described by (Finnemore and Hollis, 2016) to look at the above mentioned initiatives. A norm consists of four “essential ingredients”: identity – the group to which the norm applies; behavior - specific actions required by the norm of the group; propriety - the basis on which norms label behavior as appropriate or inappropriate; and collective expectations - shared understandings about appropriate behavior held by members of the designated group. 18

The scope of this article doesn't let to describe all these proposals in details. However, there are some interesting insights at the first glance. Each proposal appeals to different identities: Tech Accord to tech industry; Microsoft appeals to states; Siemens requires action from both states and tech; Nornikel and GCCS propose behavior to all stakeholders. The common idea of the initiatives is to reduce the level of cyber attacks by different means: to suppress the abuse of networks, software, devices for malicious activity, to advance the investigating efforts, and to promote the culture of cybersecurity (for a detailed description, see the table below). Interestingly, each proposal refers to its own propriety indicator. Participants of the Tech Accord seem to be using their corporate ethics and customer relations as a basis for norms internalization. Signatories of the Siemens Charter appeal to the concept of trust in digital future: “People and organizations need to trust that their digital technologies are safe and secure; otherwise they won’t embrace the digital transformation – that why we sign the Charter”. So does the Nornikel Charter, though also adds references to the UN GA resolutions on “Developments in the field of information and telecommunications in the context of international security” adopted annually from 1998 up today. Microsoft apparently builds upon the International law, as well as GCCS. The latter, by the way, puts forward a new indicator of propriety: the stable functioning of the public core of the Internet as a vital component of the cyberspace.19 Collective expectations are hard to be identified yet, as the initiatives mentioned above are only proposals; we may see enough data for the

---

17 Tech Accord https://cybertechaccord.org/accord/
GCCS - https://cyberstability.org/
analysis only in case these entities will voluntary follow the proposed norms for some time. Norm-making is not a finite process – the stage of interpretation is one of the most important in the cultivation process.

The form in which the norm is expressed is also important for its internalization. The practice shows that business tends to deliver cyber norm proposals in the form of a public commitment. It is an interesting turning point for further research in the norms consolidation. For the effective public commitment, a company must be transparent in communicating its progress to meet the announced goals. Only participants of the Tech Accord claimed to “report publicly on our progress”. Furthermore, there is a point of view that cybersecurity is a public good dilemma, in which individual group members have to decide on whether or not to contribute to a certain public good. (Lokhorst et al, 2009) found that public commitments help to structurally change the behavior of people with different levels of trust. Those with a low level are willing to contribute if they know that the public good is likely to be provided, especially if the key players have already committed to doing a contribution. So far the tech initiatives for cybersecurity has been recently announced by the industry giants and the first supporters are big businesses, a considerable amount of time should pass before a norms cascade (if any) will happen, and we can conduct a thorough analysis of the norms cultivation.

To conclude, the current state of affairs can be characterized as an interim phase in cybersecurity diplomacy: states have put some efforts to elaborate a new cyberlaw but it turned out to be an overwhelming task to agree on legally binding rules in the end. The most probable scenario now is that states skim the cream of business and tech proposals and eventually include some suitable norms for intergovernmental discussions. At this point, the groups of like-minded states are diametrically opposed in their vision of cybersecurity and are not willing to barter away their free rein in cyberspace for the sake of common security. In this light industry giants are likely to surreptitiously follow particular standards and norms of cybersecurity they acknowledged as appropriate because they suffer from cyber attacks on a more frequent basis.

---

<table>
<thead>
<tr>
<th>Identity</th>
<th>The Cybersecurity Tech Accord</th>
<th>Siemens Charter of Trust</th>
<th>Nornikel Charter of information security for critical industrial facilities</th>
<th>Microsoft Digital Geneva Convention</th>
<th>Global Commission on Cyber Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tech industry</td>
<td>States and industry</td>
<td>All actors</td>
<td>States</td>
<td>All actors</td>
<td></td>
</tr>
</tbody>
</table>

**Behavior**

- protect all our users and customers from cyberattacks
- design, develop, and deliver products and services that prioritize security
- oppose cyberattacks on innocent citizens and enterprises
- not to help governments launch cyberattacks
- help to empower users, customers and developers
- partner with each other and with like-minded groups to enhance cybersecurity - establish formal and informal partnerships with industry, civil society, and security researchers
- information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks

- designate specific ministries and CISOs
- establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements.
- Adopt the highest appropriate level of security and data protection
- Combine know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules
- include dedicated cybersecurity courses in school/uni/professional curricula
- establish mandatory independent third-party certifications
- multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into (FTAs).
- Drive joint initiatives including

- condemn the use of ICT for the purpose of unfair competition and damage to industrial facilities
- condemn the development and integration of hidden vulnerabilities in information and communication systems
- condemn the activities aimed at the hidden accumulation of information about vulnerabilities
- welcome the efforts of States and the international community to establish an effective system and transparent procedures to combat cyber crimes
- welcome the efforts of the international community to give the basic information and communication infrastructures, which form the basis of the global network, the status of a demilitarized zone, free from the military confrontation of political actors
- welcome the participation of

- Refrain from attacking critical infrastructures and cloud-based services
- Refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes
- Refrain from using ICT to steal the intellectual property
- Refrain from inserting or requiring "backdoors" in mass-market commercial technology products
- Agree to a clear policy for reporting of vulnerabilities
- States should also ensure that they maintain control of their weapons in a secure environment. + restrain development
- Agree to limit proliferation of cyber weapons. Governments should not distribute, or permit others to distribute, cyber weapons and should use intelligence, law enforcement, and financial sanctions tools against those who do

Protect the Public Core of the Internet: Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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.”

Protect the electoral infrastructure: State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.”
<table>
<thead>
<tr>
<th>Propriety</th>
<th>Corporate ethics</th>
<th>“People and organizations need to trust that their digital technologies are safe and secure; otherwise they won't embrace the digital transformation”</th>
<th>Refers to the UN GA resolutions on ICT in the context of international security</th>
<th>International law</th>
<th>Secure Public core of Internet as a basis for compliance with the UN Charter (non-interference in elections)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The form of norms</td>
<td>Public Commitment</td>
<td>Public Commitment</td>
<td>Looks like a UN resolution “code of ethics, joining which corporations declare their intention to follow the principles of fair play in their actions in the cyber”</td>
<td>Convention (proposal)</td>
<td>Expert recommendation</td>
</tr>
<tr>
<td>Collective expectations</td>
<td>???</td>
<td>???</td>
<td>???</td>
<td>???</td>
<td>???</td>
</tr>
</tbody>
</table>