Norwegian Institute of International Affairs

POLICY BRIEF – 14 / 2020

# Intergovernmental checkmate on cyber?

## Processes on cyberspace in the United Nations

*Erik Kursetgjerde*

### RECOMMENDATIONS

- Interdisciplinary methods should be applied to finding the best legislative solutions to reducing cyberspace instability.
- Given there has never been a cyberattack regarded as a violation of international law, a more innovative approach to major concepts is necessary if the debate on international cybersecurity and regulations in the domain is to develop further.
- Greater international agreement is needed on what basic principles should apply in cyberspace, with the groundwork laid in previous work – such as the successful United Nations Group of Governmental Experts processes, norm development in the GCSC, and the Tallinn Manual – serving as a useful starting point for discussion.
- Small states have the opportunity of pushing cybersecurity as a thematic priority in the United Nations Security Council – a path Norway could pursue in its forthcoming 2021–2022 Security Council term. The attribution of the assumed Russian cyber operations toward the Norwegian parliament earlier this year, actualizes the addressing of the issue in the Council

## The starting point

The beginning of cyberspace-related processes in the United Nations can be traced back to 1998, when the Russian Federation put forward Resolution 53/70: 'Developments in the field of information and telecommunications in the context of international security'. Since then, there has been a number of relevant resolutions, activities and processes, with the UN's Group of Governmental Experts (GGE) on 'advancing responsible State behavior in cyberspace in the context of international security' having been the most central. The GGE, based on a 2001 UN resolution and established in 2004 with a UN mandate, and can be seen as an attempt to establish international governance and agreements on cybersecurity-related issues.

Thus far, five GGE groups have completed their term, with the current group process due to end in 2021. This policy brief will focus on the processes and results from the 2014–2015 and 2016–2017 GGE groups, as they are regarded as the two most important within the process to date. While the 2014–2015 group ended in consensus and is seen as a success, the 2016–2017 group failed to do so, with negotiations breaking down.

The main actors in the GGE processes can broadly be divided into two blocks at the UN, with the US and the West on one side, and Russia, China and the East on the other. This division of actors fundamentally impacts the dynamics of gaining consensus on cyberspace norms, as well as how international law should apply in this arena. The disagreements between groups are not merely about law, but extend to strategy, politics and ideological differences, which combined make it an extremely complex situation to navigate.

## GGE 2014–2015: The golden standard?

The report from the 2014–2015 GGE process contained several references to international law being applicable in cyberspace. Even so, the group was not in a position to clarify how exactly international law was applicable. Thus, the section on international law was restricted to a selective listing of UN Charter provisions.

In negotiations, the US emphasised its concerns regarding previous discussions on a broader framework and a possible treaty regulating the use of ICTs in international conflict, which Russia had been promoting. Further, the US stressed that the work undertaken in the 2012–2013 process regarding the use of existing rules and norms should be continued. Thus, from the US perspective, the process was about confirming existing principles of international law, thereby demonstrating that these constituted an appropriate framework for governing cyberspace-related rules, norms and state behaviour. However, it became evident during the 2014–2015 process that Russia was not in agreement with the above premise, which went on to form the basis for the process' conclusions. Based on this, Russia's decision to conform to the views of the US during the 2014–2015 process can be seen as a calculated trade-off. For Russia, it was worthwhile compromising with the US, as not to do so potentially meant no progress at all being made. Given Russia has been one of the main actors pushing cyberspace onto the UN agenda, this approach was – arguably and despite Russia's tendency for discord – in line with the country's attempts to advance the process.

Some also point out that it would have represented a loss for Russia if consensus had not been reached, especially in regards to the view put forward by the US and the West that international law can deal with cyberspace issues. Russia's role in the UN system has made it a major player in these negotiations, and it was very concerned about being left behind. Several informants in my study emphasised Russia's commitments, pointing out they are based on previous resolutions and formal statements.

The disagreements in 2015 were, among other things, related to the status of such international law concepts as due diligence and state responsibility. In the group's report, the application of international law was discussed separately from norms, rules and principles. Thus, it was possible to circumvent the issue that, despite states being unable to agree on how international law should be applied in cyberspace, there was no requirement for a new treaty. In this way, disagreement was restricted to how international law should be applied, rather than the applicability of the framework itself. The attempt by the US to adapt existing rules to a new situation was an exercise in rule-based behaviour, whereby rules and situations are related to criteria of equality or difference through reasoning.

## GGE 2016–2017: Visible tensions between the blocks

Following the 2015 report, several states wondered if the GGE process had run its course and should be replaced with another form of process or forum. Despite this, a new GGE group was assembled in 2016, with a more explicit focus on the role of international law in cyberspace.

Over the course of the 2016–2017 process, it became clear that the application of international law in cyberspace was one of the key reasons provoking lack of consensus in the group. Several experts had already pointed out that, in the context of the group's ambitious mandate, it would be difficult to reach further consensus. Conflicting opinions on the use of international law not only prevented the group from developing further agreement on the issue,

Photo: NTB Scanpix

but – due to the time spent discussing it as the main priority – affected progress in other areas of the mandate. Russia, Cuba and China were among those who decided not to approve the draft report.

For the first time since 1999, the UN was in placed a situation where the General Assembly was unable to adopt a resolution. The uncertainty this engendered cast doubt on the legitimacy of the GGE process and the way forward. After some time, it became clear that there would have to be a new round of the GGE process, accompanied by an additional group – the Open-Ended Working Group (OEWG) – which was the initiative of Russia, Cuba and others. This new initiative for two different working groups underlined the UN's role as facilitator for cyberspace processes.

Curiously, it was the US – which had previously opposed the GGE processes, as it regarded international law as being sufficient – that initiated the new GGE process. The new OEWG is therefore of particular interest, as both it and the GGE have similar mandates. The new OEWG process is believed to have affected the dynamics of the cyber policy debate in the UN, as it is not only parallel to the GGE-process but also involves open membership for all UN-countries and multi-stakeholder meetings with non-state actors.

While Russian attempts at drawing up a treaty have not been fulfilled by the GGE processes, they have facilitated a broader debate on norms and responsible state behaviour. It has also been a significant development that, instead of discussing whether international law is valid in cyberspace, there is now a focus on the actual application of it. It seems that this point has been a particularly difficult challenge in the GGE negotiations.

## Regulations in the international system

Irrespective of topic, the international system's processes of regulation are demanding and complex. Although cyberspace is sometimes compared to other domains – such as the regimes for space or Antarctica – this is often a fruitless endeavour due to, among other things, cyberspace's unique cross-border qualities. Nevertheless, similarities do exist in some respects, such as there also being little willingness on the part of the US and the Soviet Union during the Cold War to commit to binding rules that could lay the groundwork for space, with both sides taking the position that regulations would limit their room for manoeuvre. Here, though, it was effectively only the US and the Soviet Union that had the capacity to access space, whereas in cyberspace most states have such capabilities. Even so, several diplomats mentioned the parallels between cyberspace, space and Antarctica during interviews.

State practice in the cyberspace domain has lacked transparency due to national security challenges, which suggests that transparency among states participating in cyberspace governance processes is difficult and lacking. There have been challenges in terms of information-sharing between the states, as well as differences in capacity. While the mandate of the 2014–2015 GGE did involve attempts at capacity-building, this was addressed with a clearer focus on measures in the 2016–2017 GGE. The US resistance to Russian's position regarding a treaty can be seen in the context of the country potentially committing itself to obligations that many states have no real intention of following through on, while attribution of cyberoperations remains a major issue.

The need for a small state perspective to increase focus on the issue in the UN is becoming ever more evident. Given the great powers are apparently locked in great power politics, the initiative must come from elsewhere. In 2021–2022, Norway will serve as a member of the UN Security Council, providing the country with the opportunity to help shape policy in a number of international peace and security areas.

Cybersecurity as a thematic could be a designated priority within Norway's mandate, including continuing Estonia's work aimed at stimulating cybersecurity discussions among Security Council members. The goal should be to raise Security Council member awareness of cybersecurity norms and how existing international law can be applied in cyberspace. The groundwork laid in previous work – such as the successful GGE processes, norm development in the GCSC, and the Tallinn Manual – serves as a useful starting point in this regard.

The cyber operations which targeted the Norwegian Parliament 24 August this year, was attributed by Norwegian authorities to Russia a few months later. The attribution was the first time that Norway has gone public when their interests have been affected in the cyber domain. The attribution of the assumed Russian cyber operations toward the Norwegian parliament actualizes the addressing of the issue in the Council and is a possibility to develop clear international guidelines on attribution.

## Legislation on a moving target

Cyberspace is often regarded as a demanding domain to get a handle on, and there is little to suggest that its strategic importance will diminish in the years to come. In fact, the opposite is true, with cyberspace's bewilderingly rapid pace of change making it particularly difficult to legislate on compared to previous legislative challenges in other domains.

It must also be taken into account that the role of the GGE has never been to create or reject existing international law, but rather to discuss its application in terms of advancing responsible state behaviour in cyberspace. Russia and the US are united in wishing to protect their critical infrastructure against cyber operations. Despite the GGE's mandate and the fact that cybersecurity has been discussed for many years, however, there remains a lack of clarity around the norms, rules and principles underpinning the concept.

**Erik Kursetgjerde** holds a Master's degree in Political Science at the University of Oslo and is a Junior Research Fellow in NUPI's Research Group on Security and Defence. His research interest revolves around international relations, with a focus on the role of cybersecurity and cybersecurity governance.

This policy brief is published by NUPI's Cyber Security Centre with funding from the GAIA research project.

The project is funded by the IKT+ programme to the Research Council of Norway.

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 Oslo, Norway
www.nupi.no | post@nupi.no

Cover photo: NASA