25
2017

ISSUE ALERT

GLEBSTOCK/ADOBESTOCK

Minilateralism and norms in cyberspace

by Jakob Bund and Patryk Pawlak

In June 2017, the UN Group of Governmental Experts (UNGGE) – a gathering of cyber specialists – failed to present a consensus report. Although not entirely unexpected, the deadlock prolongs the uncertainty surrounding the application of international law to cyberspace and norms of responsible state behaviour. After several years of seemingly consistent progress, the approach adopted through the UNGGE appears to have reached its limits due to problems related to expanding membership, format and timing.

However, for many years now states have been pursuing a parallel bilateral track for developing cyber norms, including through bilateral agreements and in regional groupings (e.g. the Shanghai Cooperation Organisation, the G20 and the BRICS). At the same time, members of the G77 and the Non-Aligned Movement expect to play a larger role and bring different perspectives to these discussions. With the UNGGE-led process stalled for the moment, there is a clear need for reflection on the potential impact of bilateral and regional approaches for the EU, as well as on the Union's role within this new web of norms.

Norm diffusion through the UN

For many years now, building normative safeguards against high-impact-low-probability cyberattacks has detracted attention from the vast majority of hybrid cyber operations, which are characterised by the involvement of state-sponsored groups and actions that remain below the threshold of armed conflict. Yet in many ways, this is where the real work of establishing state practice and inducing conforming behaviour begins.

In this regard, the 2015 UNGGE report still provides relevant guidance. In particular, the proposed norms concerning due diligence, mutual legal assistance, the transparency and integrity of ICT supply chains could serve as a basis for advancing the current debate. At the same time, the past politicisation of UN-based processes cautions against throwing unconditional support behind the UN as the primary vehicle for cyber norms conversations. For instance, earlier this month in its position paper for the 2017 UN General Assembly, China affirmed its support for the UN as the main channel for developing international rules for cyberspace. In a distinct appeal for multilateralism, the statement underscored the need to 'adopt international norms for cyberspace that are acceptable to all'. Although seemingly innocent, such statements are a *de facto* expression of support for a system which grants states the leading role in governing cyberspace – an approach that may ultimately undermine its free and open nature.

Norm diffusion and minilateralism

Against this backdrop, building coalitions with like-minded (mostly Western) countries – minilateralism in cyberspace – has emerged as a

UNGGE 2015 Catalogue of norms

- States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
- States, in ensuring the secure use of ICTs, should respect […] the promotion, protection and enjoyment of human rights on the Internet;
- A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure […];
- States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts;
- States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
- States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams […] of another State;
- A State should not use authorised emergency response teams to engage in malicious international activity.

complementary mechanism. This is not only a response to the shortcomings of the UN-based process but also a recognition that agreements concluded between states do not always deliver the expected outcome. The nature of existing agreements in the cyber domain – both in terms of format and substance – means that there are few effective ways to monitor compliance.

Even though the political deal concluded between Washington and Beijing in 2015 resulted in a reported drop in economic cyber espionage originating from China, enforcing such agreements proves very difficult in practice. Violations of agreed norms often only leave the targeted state with the option of taking unilateral action – either economic (for example, economic sanctions against Russia and North Korea imposed by the US) or judicial (for example, the indictment of five Chinese PLA officers by the US on charges of economically-motivated cyber espionage, but who were never extradited). None of these unilateral steps, however, has proven consistently effective. Pursuing cooperation through like-minded alliances of 'cyber norm enforcers' could make divergent behaviour more costly for states outside these blocks.

At the same time, the prioritisation of building coalitions with like-minded countries runs the risk of making norm negotiations dangerously divisive and ignoring the lessons of past successes. An open and inclusive global internet cannot be safeguarded by parochial norms, and emphasising progress over process may end up damaging both. The forming of a 'coalition of the willing' (that draws a line between different approaches) may force others to unnecessarily pick sides – ultimately defeating the purpose of the normative endeavour. The added value of norms is significantly reduced when restricted to certain countries which already find themselves on converging trajectories in practice.

Reaching an understanding with those who have a different perspective – although perhaps idealistic and time-consuming – is crucial precisely because they lack a common reference point. In particular, the right to regulate information flows continues to be a critical point of contention, with China and Russia arguing that it is the state's prerogative to control data and online content within its sovereign sphere. Producing tangible outcomes requires persuading counterparts that they stand to gain from a new understanding or that they stand to lose from a deteriorating *status quo* in the absence of an agreement. In this regard, multilateral settings develop a dynamic of their own by creating a reputational cost when a country is seen as spoiler – a reputation that could invite further repercussions. Yet in the long term, such minilateralism should be seen not a viable alternative but a means to revive multilateralism.

The EU: from norm-taker to norm-maker?

Supporting the promotion of a rules-based international order and multilateralism are key priorities identified in the EU Global Strategy (EUGS). Consequently, the September 2017 Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' endorses the voluntary non-binding norms, rules and principles of responsible state behaviour that have been articulated by the UNGGE.

As the EU moves to strengthen its cyber resilience (through, for example, a proposed fully-fledged European Cybersecurity Agency and a Cybersecurity Emergency Fund) and build an effective EU cyber deterrence capacity (through the 'cyber diplomacy toolbox' and increased cooperation with NATO), there is also a clear need to reflect on the norms that the EU wishes to uphold. The EU's position as a norm-maker in other policy areas – notably on privacy and data protection – demonstrates its potential when it is more proactively involved. With the US taking steps to downsize its multilateral engagements on cyber issues, there is both a window of opportunity and a need for the EU to embrace fully the idea of becoming a 'forward-looking cyber player', as stated in the EUGS.

Jakob Bund is an Associate Analyst at the EUISS. Patryk Pawlak is the Brussels Executive Officer and is responsible for cyber-related issues at the EUISS.

© EU Institute for Security Studies | QN-AL-17-025-2A-N | ISBN 978-92-9198-532-6 | ISSN 2315-1129 | doi:10.2815/372100