RESEARCH IN FOCUS

Pathways to Change: Resilience, Rights and Rules in Cyberspace

Input paper for the
EU-UNGGE regional consultations

Patryk Pawlak
Xymena Kurowska
Eneken Tikk
Caitriona Heinl
François Delerue

June 2019

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Acknowledgments

This paper has benefited from numerous discussions with the civil society organisations and the private sector organised as part of the EU Cyber Direct project between March and June 2019. The views expressed in this paper are of the authors alone and do not represent official positions of the European Union or any of its institutions. The authors would like to thank experts and government officials who provided comments on the earlier drafts of this paper. Any mistakes or omissions are those of the authors alone.

Disclaimer

The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the author(s).

Introduction

European citizens live a privileged digital life in one of the most prosperous and free regions of the world. The EU's member states are among the most connected nations in the world: for Europeans, a free, open, peaceful and secure cyberspace is a reality. This is not necessarily the case for other people around the globe who despite similar – or sometimes even higher – levels of dependence on internet-based platforms in their daily lives, do not always enjoy the same levels of protection, security, and civil liberties. What we do share, however, is our vulnerability to malicious activities by state and non-state actors whose actions and behaviour in cyberspace poses a threat to peaceful, trustworthy and prosperous digital societies.

The two parallel processes at the United Nations – the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) – can serve as useful vehicles to take concrete actions towards strengthening the commitment of states to behave responsibly in cyberspace[1]. As the European Union and its member states are active in these two platforms, they need to recognise that the EU reality is not shared by everyone and that their core values are not uncontested in the world.[2] Remaining mindful of the differences that surround the development and use of information and communications technologies (ICTs), the EU's approach in these processes must remain open towards the views and ideas of others.

At the same time, we must take pride of our achievements, demonstrate the benefits of our choices, and expose the costs of authoritarian models.[3] The EU's success in the digital domain is built upon an unwavering commitment to fostering a **resilient digital society with full respect for human rights and the rules-based order**. A free, open and secure cyberspace that underpins this approach is a universal ideal. But sadly, for many societies it remains an aspirational goal.

Therefore, the EU's experience and demonstrable accomplishments need to drive its engagement in the UN-led processes, with the following three observations in mind:

- **Resilient societies are better able to prevent unintended conflict.** The higher the level of preparedness and capabilities of a state and society, the lower the chance of over-reaction, miscalculation and conflict. It is therefore essential that cyber capacity building to strengthen resilience receives adequate attention in the new round of the UNGGE (and possibly OEWG) – not only as a remedial mechanism but also as the key element in cooperation and inclusive dialogue among the states. Consequently, digital risks can be best addressed through an international cyber resilience regime that builds on the existing processes that promote a risk-based approach.
- **Rights and freedoms are the precondition for a stable and peaceful cyberspace.** Protection and promotion of human rights is at the core of the EU's foreign and security policy. Protection and promotion of human rights is at the core of the EU's foreign and security policy. The EU recognises that the same rights that people enjoy offline must be guaranteed online. Such a clear commitment helps prevent the misuse of the internet for political ends and the

[1] In short, states should behave in a way that ensures the safety and well-being of all people in their territory, as well as others in the event of conflict, protects their national interests, and shapes their relations with other states and the international community respecting the rights and obligations resulting from the existing international law and international custom. See for instance: P. Cornish and C. Kavanagh (2019) *Report from the Geneva Dialogue on Responsible Behaviour in Cyberspace*, May 2019.

[2] X. Kurowska (2019) *The politics of cyber norms: Beyond norm construction towards strategic narrative contestation*, Research in Focus, EU Cyber Direct, March 2019.

[3] See: OECD (2019) The European Union: a people-centred agenda. An international perspective, May 2019; M. Hohmann and T. Benner (2018) *Getting "free and open" right. How European Internet foreign policy can compete in a fragmented world*, GPPI Policy paper, June 2018.

undermining of the rule of law. With 'digital authoritarianism' on the rise[4], the EU needs to renew its support for civil society organisations and existing international platforms committed to political freedoms.

- **Rules-based order in cyberspace is not a choice. It is a necessity.** The growing number of malicious activities in cyberspace is a cause for concern as it increases the risk of misunderstanding, miscalculation and conflict. To minimise such risks, the international community – including through a previous UNGGE report – has committed to norms of responsible state behaviour, agreed on a set of Confidence Building Measures, and reaffirmed that existing international law, including the UN Charter in its entirety, applies to cyberspace. But the implementation of these measures has fallen short, suggesting that certain states are not fully committed to preserving a peaceful and secure cyberspace. Without a sustained effort from governments to prove their commitment (e.g. through state practice and concrete policies and positions), grassroot initiatives launched by specific communities of practice (e.g. FIRST, Meridian, GFCE, the Paris Call) are emerging as alternatives to state-led efforts[5] and the role of civil society organisations as watchdogs in cyberspace is growing in importance.

Five ideas to translate vision into reality

A clearly defined vision for a global engagement on cyber-related issues is a precondition for achieving progress towards a peaceful and secure cyberspace. It also requires a roadmap which outlines the steps of such a process, including by **(1)** setting the goal, **(2)** designing a strategy towards achieving it, **(3)** engaging others in the execution of the strategy to multiply the EU's voice, **(4)** showing why the goal is worth pursuing, and **(5)** demonstrating possible actions to convince others.

1. Make a resilient, rights- and rules-based cyberspace a clear and non-negotiable goal.

Despite its limited timeframe and prescribed mandate, the UNGGE sets the agenda for international cyber-related dialogues. Mindful of this role, the UNGGE Chair and members should actively participate in and follow other global discussions with the aim of promoting a resilient, rights- and rules-based international order in cyberspace. It is critical for the new UNGGE to recognise that the landscape of cyber initiatives and actors has significantly evolved over the past five years: the conversation now includes civil society organisations, research institutes and the private sector, and accordingly requires more intensive engagement with other stakeholders. Issues not dealt with by the UNGGE should be addressed in other international and regional venues and platforms. In addition, rather than centralising the discussion within the UN, the UNGGE should support a decentralised two-way approach for information gathering, exchanges and debates that is more inclusive and better reflects regional decision-making processes. The consensus-making processes within regional bodies (e.g. EU, ARF, OAS, OSCE and AU) have already resulted in the emergence of a culture of cooperation which could feed into global debates, albeit tailored to unique regional needs. Furthermore, there are several other state and non-state actor-led platforms that could add value to the ongoing conversations. Initiatives such as the Global Forum on Cyber Expertise, the Internet Governance Forum, the Global Commission on Stability in Cyberspace and the RightsCon Summits bring together different policy communities, all of which have a stake in a free, open, peaceful and secure cyberspace. Adopting a decentralised approach and including additional voices generates a greater ownership of the processes and reinvigorates existing

[4] Freedom House (2018) *Freedom on the Net 2018: The rise of digital authoritarianism*, October 2018.
[5] L. Kaspar and S. Kumar (2019) *Takeaways from the OEWG meeting and UNIDIR Cyber Stability Conference*, Global Partners Digital, 12 June 2019.

capacities. This approach does, however, require a clear communication strategy to manage the expectations of all stakeholders.

2. Clearly define the EU's approach to steering the change.

Working towards a resilient digital society grounded in a rights- and rules-based international order requires responsible behaviour in cyberspace by both state and non-state actors. Such behaviour materialises by promoting concrete standards and upholding the rule of law through multilateral processes, national strategies and laws.[6] As the EU engages in the UN-led processes[7], it should not neglect the ongoing efforts in other regional and international organisations. At the same time, the EU and its member states need to demonstrate how cooperation through the UN contributes towards building a resilient, rights- and rules-based order in cyberspace. Simply rejecting the ideas proposed by others – however justified – may not be enough to convince the EU's partners. For instance, the negotiations of a new international instrument that addresses the problem of states' compliance with agreed norms would almost certainly fail as they require the existence of verification tools and a basic level of trust among states. In the current international environment, this precondition is not met and the EU (with like-minded partners) is right to question the validity of such approach. But they also need to propose a more realistic alternative that could unite both sides – including within the UNGGE and OEWG. One approach could be to invest more resources in mechanisms that address the root causes of mistrust, including the implementation of Confidence Building Measures, as well as strengthening the capacity of individual states to engage in global debates about peace and security in cyberspace, including by fully assuming and further exploring their rights and obligations stemming from international law.

3. Accept that cybersecurity is a shared responsibility and therefore non-state stakeholders need to be part of the process.

While governments retain exclusive control over the UN-led processes, the decisions taken in those venues have broad implications for the work of other communities (e.g. first responders, law enforcement agencies, etc.). Therefore, in order to ensure that norms developed as part of the UN processes are sufficiently robust, states need to engage with other stakeholders in an open dialogue about expectations and responsibilities. Expanding the conversation would also contribute to strengthening cyber diplomacy, in particular through stimulating discussions with national lawmakers and other actors participating in the law-making process. Civil society, the private sector and technical communities can also help to promote and tailor certain EU positions in other parts of the world and consequently bolster EU leadership. This does not mean that non-state actors should neglect their traditional functions in national and international policymaking (e.g. as agenda-setters, watchdogs, implementors, etc.) or abandon their objectives within the existing specialised channels (e.g. academic conferences, civil society platforms). Just as states should ensure equitable participation and representation from all regions, so too should civil society organisations and the private sector facilitate, support and provide space for the participation of peers from other regions.

4. Better communicate the value of the EU's normative agenda.

The commitment to human rights and multilateralism form the pillars of the EU's normative agenda. Yet in the complex and multifaceted world of global governance, they may be perceived as paternalistic and tools of domination rather than democratisation. As this sentiment can be (and is) instrumentalised by actors who resist the EU's freedom-based agenda, the EU's message and modes of engagement

[6] M. Kerttunen and E. Tikk (2019) *Strategically normative. Norms and principles in national cybersecurity strategies*, Research in Focus, EU Cyber Direct, April 2019.

[7] Including on the basis of the Report of the UN Secretary-General's High-level Panel on Digital Cooperation released in June 2019.

need to be adjusted. One way to do this is through an acknowledgment that not all issues linked to internet are a matter of national security: the debate on insecurity and vulnerability of internet infrastructure as a threat to national security should be systematically disassociated from the discussion about information security as a national security issue. The EU's normative discourse on rights- and rules-based international order in cyberspace needs to be more firmly centred around the priority of human security, safety and prosperity, in line with the Sustainable Development Goals. Such a focus will respond to the agenda of those countries that need to reconcile cybersecurity objectives with other more urgent needs (e.g. access to clean water, education, poverty, social exclusion, etc.).

5. Lead by example. Present an ambitious set of guiding principles supported by concrete actions.

The EU's approaches to network information security or data protection are but some of many possible approaches that need to be tailored to regional and national realities. To facilitate this, the EU needs to better communicate and explain the normative underpinnings of its policy choices and demonstrate the expected and achieved benefits. The EU's policies and laws emerge through a collaborative process that is derived from the national experience of individual member states. As such, they exemplify 'bottom-up' norms entrepreneurship where EU good practices are considered useful rather than as an attempt by the Union to push its agenda on others. To exemplify, explain and promote their experience and success stories, but also to learn from each other's experience, EU member states are invited to clarify their views on the issues of cybersecurity and introduce their solutions of cyber resilience in line with the UN General Assembly resolutions 73/27 and 73/266. Member states should follow the example of certain countries that have already provided clarification on their understanding of how the existing international law in cyberspace. A normative pragmatic EU approach to cyberspace also calls for a 'de-securitisation' of internet issues, including at the UN. This can be achieved through a greater involvement of appropriate UN bodies and committees, in particular the Economic and Financial Affairs (Second Committee), Social, Humanitarian and Cultural (Third Committee) and the Legal (Sixth Committee).

The European Union is often criticised for inaction or insufficient follow through with its calls and commitments. The EU's engagement on cyber-related issues is an example to the contrary. The EU has built a systemic, comprehensive and functional framework for cyber resilience that supports its member states and the partner countries in benefiting from ICTs to the fullest extent. With its global presence, ambitious digital agenda, and ample instruments for its implementation, the EU can and should assume its role as a forward-looking cyber player. At a moment when international rules and human rights are being called into question, the EU should be clear about its normative commitments and principles: the soft approach it sometimes adopts should not be mistaken for weakness.

About the authors

Dr Patryk Pawlak is the EUISS Brussels Executive Officer and Project Coordinator for the EU Cyber Direct.

Dr Xymena Kurowska is Associate Professor at the Central European University (CEU) in Budapest. Currently, she is a Marie Skłodowska-Curie fellow at the Department of International Politics at Aberystwyth University.

Dr Eneken Tikk heads the Cyber Policy Institute's normative, power and influence studies. She holds PhD in Law and is a specialist in the development of national legislation and international cyber diplomacy.

Caitriona Heinl is the Executive and Lead Strategist for Asia-Pacific at EXEDEC International.

Dr François Delerue is a researcher in cyber defence and international law at the Institute for Strategic Studies, French Military School (IRSEM).

VISION

RESILIENT DIGITAL SOCIETY GROUNDED IN THE RIGHT- AND RULES-BASED INTERNATIONAL ORDER

State-centric pathway

LONG-TERM OBJECTIVES

STATES BEHAVE RESPONSIBLY IN CYBERSPACE

- States cooperate to reduce risks of conflict and avoid miscalculation
- States pursue policies to reduce vulnerabilities to cyber risks
- States adopted policies that respect international law
- States pursue policy-making processes that involve all relevant stakeholders (i.e. multistakeholder approach)
- …

EXPECTED OUTCOMES

Cooperation through multilateral processes
(it is a global problem that needs to be addressed through international cooperation)

- *UN: 1st Committee (UNGGE, OEWG), 3rd Committee*
- *Regional organisations: ARF, OECD, OAS, OECD, G7/G20*
- *Communities of practice: GFCE, Meridian*
- *Non-state led initiatives: IGF, RightsCon*

Adoption of adequate policies and laws
(states play primary role in shaping international security environment)

- *Laws, policies, and strategies integrate the Rights-Based Approach*
- *Laws and policies that respect the international law obligations and agreed norms*
- *Whole-of-government and whole-of-society approaches*

EU STRATEGIES

- A joined-up approach to promote responsible state behaviour through the EU's internal and external policies;
- Providing guidance and promoting compliance at the Member States level, including by defining norms and identifying good practices;
- Support to building capacities of Member States and partner countries, in particular regulatory, institutional, technical, and legal;
- Creating inclusive and open environment for policy deliberations.

Society-centric pathway

LONG-TERM OBJECTIVES

NON-STATE STAKEHOLDERS ACT RESPONSIBLY IN CYBERSPACE

- Non-governmental actors participate in the policy-making processes
- Stakeholder groups convene platforms for action, including group-specific norms and rules of responsible behaviour in cyberspace
- Non-state actors adopt approaches strengthening state and societal resilience
- …

EXPECTED OUTCOMES

Robust and functioning non-state ecosystem
(the complexity of the problems calls for diversity of views)

- *Participation of diverse groups of actors in terms of profile (e.g. NGOs, research and academia, private sector) and expertise (e.g. human rights, digital skills, development)*

Access and input channels for non-state actors
(it is a shared responsibility that requires broad

- Externally: a joined-up approach to promote responsible state behaviour through the EU's internal and external policies (i.e. diplomacy, trade, security cooperation)

EU STRATEGIES

- Improving awareness and knowledge about cyber diplomacy related issues in order to adapt the traditional roles of non-state actors to the challenges of the digital domain (e.g. scrutiny, awareness raising)
- Clearly define the roles and expectations towards various groups of stakeholders (e.g. self-regulation, capacity building, standard setting)
- Provide support to non-state actors to boost their capacity to participate in domestic and international policymaking.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

RESEARCH IN FOCUS

is a series of research papers aimed at supporting the EU's cyber-related policies by providing a timely and policy-relevant analysis.

EU CYBER DIRECT

This project is funded by the European Union.