REBOOTING THE EU'S CYBER DIPLOMACY

*Patryk Pawlak**
November 2019

States' reliance on cyber operations in pursuit of their national security and foreign policy objectives is no longer taboo. In 2019 alone, the United States conducted a range of high-profile cyber operations against targets in Russia and Iran. North Korea targeted financial institutions and cryptocurrency exchanges to fund its nuclear weapons and ballistic missile programmes. Meanwhile, cybersecurity and trust in the digital world has moved to the forefront of bilateral diplomatic relations, as demonstrated by the debate over the deployment of 5G technology.

It is urgent that modern diplomacy and progressive foreign policy agendas embrace cyber- and technology-related issues. And yet, they often don't. The EU has signifciantly ramped up its tools and policies, but it still has not answered one basic question: How does cyber diplomacy support its broader foreign and security policy objectives? Big players like China, Russia, and the US view cyber diplomacy as one little piece in their bigger effort to shape the future world order, yet the EU lags behind. Without strong political leadership that acknowledges cyber diplomacy as an important aspect of the EU's foreign and security policy, the EU risks missing the forest for the trees. What can be done?

Be strategic

The EU needs a clear vision and a sense of direction for its cyber diplomacy – not as a stand-alone discipline but as an integral part of its foreign and security policy. An "**EU International Cyber Engagement Strategy**" could provide such a vision by establishing a clear link between broader foreign policy objectives – defending a rules-based global order, supporting global stability and prosperity, promoting EU values and standards – and the EU's cyber diplomacy. This kind of strategy should put forward the clear message that the EU is a "forward-looking" cyber player by bringing together all manner of digital policies like conflict prevention, international law, internet governance, 5G, norms, data economy, AI, research, innovation, skills, etc.

To that end, substantial work is already being done in the context of UN processes, the implementation of the Cyber Diplomacy Toolbox, and other sectoral digital strategies. The final product is important, but there would also be great added value in creating bridges between already existing digital and sectoral strategies, projects, and programmes. Different EU institutions should be involved in developing such a strategy in close consultation with member states for clarity on conceptual issues and the use of resources. Drafting such a document should not become yet another bureaucratic exercise – stakeholders from academia, the private sector, and civil society should all play a central role.

Be coordinated

The EU's voice is louder on the international stage when it is more than the sum of its parts. With cyber issues pervasive across various European policy areas, there is a clear need to streamline ongoing efforts and **mainstream cyber diplomacy across all of the EU's external actions**. This level of coordination is currently provided by the European External Action Service and the Council, however many Commission services pursue their own bilateral relations with their counterparts around the world. As the method for designing the EU's strategy towards China in early 2019 showed, closer coordination between different actors leads to better outcomes. A joint approach also requires close cooperation with the member states, some of whom are already spearheading important initiatives: Netherlands and Estonia on capacity building, international law, and
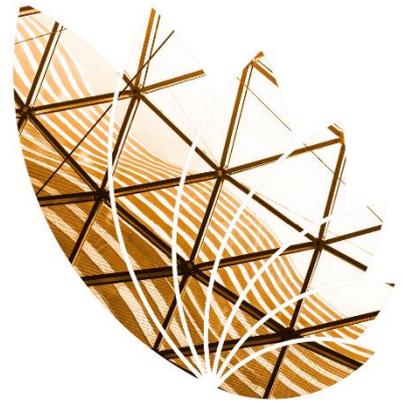
norms; Estonia on resilience building and cyberdefence; Germany on data protection and resilience; and France on international norms and state response. It is clear that the EU institutions cannot go it alone and that its strength comes from working together.

Be political

The EU's cyber diplomacy requires strong political leadership to enact a strategic vision, ensure better coordination and, most importantly, give visibility and weight to its actions. This could be achieved by the appointment of a **Special Representative for International Cyberspace Policy**. Without a politically empowered envoy to present and defend the EU's positions on the international stage, any investment in this domain will fail to translate into political influence or impact. Currently, the focus on day-to-day business wins over a more strategic approach. The EU's involvement is also often reduced to a mere presence at the discussion table instead of showing the real sign of political commitment. Placing this dossier in the hands of a capable and experienced diplomat who answers directly to the EU High Representative (as is the case with other EUSRs) – and enjoys a privileged link to the Political and Security Committee and works closely with the Security and Defence Directorate in the EEAS, the Commission services, and counterparts in the member states – would send a strong signal to allies and perpetrators and give cyber policy the political attention it deserves.

Why does it matter?

Despite the existing shortfalls, the EU has managed to project the image of a reliable partner in shaping cyberspace. When its vision and commitment have been clearly defined, the EU has set the tone of the global debate. This grace period, however, is coming to an end. Powers like China, the US, and India aspire to play a more active role in shaping the digital environment – and the EU needs a powerful voice.

We have reached a critical junction that will determine what kind of player the EU will be in cyberspace. Will it have meaningful powers and adequate resources? Or will it be undermined by national interests and institutional rivalries? Answering these questions and ensuring real progress in the European project will require strong political will. With digitalisation featuring permanently on the new Commission's agenda, there is a unique window of opportunity to ensure that the EU's norms and practices proliferate and that a stronger voice for Europe is found. Like with any system-wide upgrade, there is a need – and a suitable time – for a reboot. For EU's cyber diplomacy, that time is now.

Dr. Patryk Pawlak is Brussels Executive Officer at the EU Institute for Security Studies and the Project Coordinator for EU Cyber Direct.

Portfolios
of commissioner designates 2020-2024
(based on their mission letters)

INTERNAL MARKET

PROTECTING OUR EUROPEAN WAY OF LIFE

JUSTICE

A EUROPE FIT FOR THE DIGITAL AGE

AN ECONOMY THAT WORKS FOR PEOPLE

HOME AFFAIRS

INNOVATION AND YOUTH

FOREIGN POLICY AND SECURITY POLICY

Full implementation of GDPR

A New Digital Services Act

Intellectual property regime

Digital taxation

Digital Economy

A European Innovation Council

Raise awareness against disinformation and online threats

A Digital Education Action Plan for digital literacy

Research and Innovation

Support technological leadership and strategic autonomy

A coordinated EU approach on human and ethical AI

Improve information exchange

A common approach on cryptocurrencies

Justice

EU Internet Forum to counter hate speech and terrorist content online

#VDL #EC CYBER–RELATED ISSUES

Single market for cybersecurity with certifications, rules, 5G standards, rapid emergency response strategies

Resilience across sectors

A Joint Cyber Unit

Security

Diplomacy

A rules–based multilateral order that promotes global stability and prosperity

EU's technological sovereignty in key value chains, defence and space EU's technological