The European Union's Approaches to Cyber Diplomacy: Introduction to the Special Forum

Joachim A. Koops

Wilhelm Vosse

Joe Burton

George Christou

Even though cyber diplomacy as a field emerged only during the late 1990s, it has rapidly captured the attention, energies and focus of diplomats and policymakers with a wide range of national, regional and global initiatives that aim to respond to and catch up with technological threats and risks related to cyberspace.[1] States seek both to advance their national interests and security through unilateral, bilateral or regional diplomatic engagement and to shape rules, norms and conventions at the global level. At the same time, cyber diplomacy occurs in a space where corporate and non-state actors often dominate the agenda and the development of capabilities.

Building on Barrinha and Renard's conceptualisation of it, cyber diplomacy encompasses 'the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace'.[2] The scope of cyber diplomatic engagement has broadened considerably from the initial concerns with technical specifications and legal responsibilities; it now incorporates contemporary challenges of cyber weapons, disinformation campaigns and information manipulation. Nevertheless, addressing the escalating frequency and severity of cybercrimes, fortifying data privacy protections against both corporate and governmental intrusions, and supporting states through cyber capacity-building initiatives remain central priorities. Furthermore, divergent conceptualisations regarding the internet's future trajectory – ranging from state-controlled architectures to open, decentralised networks – persist as contentious issues within global cybersecurity governance forums and norm-development processes.

[1] For a comprehensive overview of the field of cyber diplomacy at the national, regional, global and multi-stakeholder levels, see Christou, Vosse, Burton and Koops (2025). See also Christou (2024) for a definition of cyber diplomacy and for an overview of how it has evolved, how it has developed and how it has been performed in relation to critical issues of cyber security and cyber defence.

[2] Barrinha and Renard 2017.

Amid these multi-level, multi-actor and multi-issue domains, the European Union (EU) has been advancing its own approach to cyber diplomacy since the early 2010s. The EU's early focus was on responding to cybercrime groups and repeated instances of state attacks, and on contributing to diplomatic initiatives at the United Nations. However, the Russia–Ukraine war has served as a core catalyst for a more comprehensive and action-oriented approach with wider linkages to combating foreign information manipulation and interference, and developing diplomatic cyber instruments in the context of wider EU security and defence policies.

In this context, the two forum articles 'Cyber Diplomacy and the Russia–Ukraine War: The European Union's Response', by Nicolò Fasola, Sonia Lucarelli and Francesco Niccolò Moro, and 'Forged in Crises: Learning and Adaptation in the European Union's Cyber Diplomacy', by Patryk Pawlak, examine how the EU has attempted to adapt and learn as a cyber-diplomatic actor, both in response to the Russia–Ukraine war and in the wider context of institutional and policy evolutions and 'organisational learning' since the early 2010s.

Fasola et al. provide a comprehensive examination of how the ongoing war in Ukraine has catalysed the operationalisation of EU cyber diplomacy instruments. It challenges a widely held assumption about Russian cyber capabilities by demonstrating that while cyber operations have failed to deliver decisive military advantages, they remain an integral part of Moscow's broader strategic competition framework, or *bor'ba* (non-violent confrontation). This is the reason the EU's response emphasises long-term strategic and legislative frameworks rather than immediate operational countermeasures. The article demonstrates how pre-existing cyber diplomacy initiatives, particularly the Cyber Diplomacy Toolbox and institutional mechanisms established in 2013, enabled swift yet durable responses to the crisis. It also reveals a division of labour: EU-level actions concentrated on coordination and integration, while member states prioritised critical infrastructure protection and direct military cyber support to Ukraine.

Pawlak adopts a broader perspective to examine institutional learning mechanisms that have shaped the evolution of EU cyber diplomacy over the past decade. Through the analytical framework of crisis-driven learning, the article identifies three distinct adaptation pathways: inferential learning from the failures of deterrence doctrine to address slow-burning crises; contingent learning necessitated by fast-burning crises such as the Ukraine conflict; and 'failing forward' dynamics within UN multilateral processes. He reveals how the EU's Cyber Diplomacy Toolbox has evolved from a deterrence-oriented framework to a tool of persistent engagement and proactive defence postures. Pawlak clearly shows how the democratisation of UN cyber processes through the Open-ended Working Group forced substantial adjustments in EU working methods, resource allocation and diplomatic engagement strategies with non-like-minded states. In addition, his article highlights some recent EU innovations, ranging from inter-regional partnerships and capacity-building initiatives to the creation of cyber rapid response teams for supporting partners.

The convergent themes and lessons of these forum articles underscore how the Russia–Ukraine conflict has served as a decisive catalyst for the maturing of cyber diplomacy, but also how such crisis-driven evolution was built upon foundations established through previous institutional developments. The pre-existence of frameworks such as the Cyber Diplomacy Toolbox, the EU–Ukraine Cybersecurity Dialogue and established attribution mechanisms has proved essential for enabling rapid response capabilities. The lesson here is that effective cyber diplomacy requires sustained institutional investment rather than reactive crisis management.

Both articles also identify a shift from reactive to proactive cyber diplomatic postures. This can be seen in the EU's response to individual incidents towards addressing cumulative campaign effects; from defensive resilience towards shaping global norms and accountability mechanisms; and from technical capacity building towards comprehensive digital literacy initiatives across society. Lastly, they also show that persistent institutional challenges limit EU cyber diplomacy effectiveness. The leadership vacuum identified by Pawlak in the context of mid-level management driving policy innovation in the absence of senior political engagement correlates with the fragmentation between EU-level coordination and member state implementation described by Fasola et al. The forum articles suggest that without addressing these organizational pathologies, the EU risks falling behind and undermining its own achievements as an emerging actor in cyber diplomacy.

Both forum articles advance a policy-oriented understanding of how the EU can adapt its cyber diplomatic capabilities under conditions of systemic competition, technological disruption and inter-state war. This forum therefore also contributes important empirical insights into studies on how a regional organisation such as the EU seeks to adapt traditional tools of diplomacy to the increasingly complex cyber domain. The 'diplomatisation' of cyber policies and, arguably, the 'cyperpoliticisation' of diplomacy are driven not only by states and private actors but also by regional organisations such as the European Union.[3] The articles will be of interest both to scholars and policymakers of EU foreign and security policy, and also to those studying and engaged in the evolving nature of diplomacy itself.

Bibliography

Barrinha, André and Thomas Renard. 'Cyber-Diplomacy: The Making of an International Society in the Digital Age'. *Global Affairs* 3 (4–6) (2017), 353–364. DOI 10.1080/23340460.2017.1414924.

Barrinha, André. (2024). 'Cyber-Diplomacy: The Emergence of a Transient Field'. *The Hague Journal of Diplomacy* 19 (3), 439–466. DOI 10.1163/1871191x-bja10183.

Christou, George. 'Cyber Diplomacy: From Concept to Practice'. Tallinn Paper No. 14, NATO Cooperative Cyber Defence Centre of Excellence, 2024.

[3] Barrinha 2024.

https://ccdcoe.org/library/publications/tallinn-paper-cyber-diplomacy-from-concept-to-practice/

Christou, George, Wilhelm Vosse, Joe Burton and Joachim A. Koops, eds. *The Palgrave Handbook on Cyber Diplomacy* (Cham: Palgrave Macmillan, 2025).

Joachim A. Koops
is Professor of Security Studies at the Institute of Security and Global Affairs of Leiden University and Chair of the Board of the Global Governance Institute in Brussels.

Wilhelm Vosse
is Professor of Political Science and International Relations and Chair of the Department of Politics and International Studies at the International Christian University in Tokyo, Japan.

George Christou
is Professor of European Politics and Security in the Department of Politics and International Studies at the University of Warwick, UK.

Joe Burton
is Professor of Security and Protection Science at the School of Global Affairs, Lancaster University, UK.