TALLINN PAPERS

George Christou

Cyber Diplomacy: From Concept to Practice

Tallinn Paper No. 14
2024

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

No. 3 Hannes Krause "NATO on Its Way Towards a Comfort Zone in Cyber Defence" (2014)

No. 4 Liina Areng "Lilliputian States in Digital Affairs and Cyber Security" (2014)

No. 5 Michael N. Schmitt and Liis Vihul "The Nature of International Law Cyber Norms" (2014)

No. 6 Jeffrey Carr "Responsible Attribution: A Prerequisite for Accountability" (2014)

No. 7 Michael N. Schmitt "The Law of Cyber Targeting" (2015)

No. 8 James A. Lewis "The Role of Offensive Cyber Operations in NATO's Collective Defence" (2015)

No. 9 Wolff Heintschel von Heinegg "International Law and International Information Security: A Response to Krutskikh and Streltsov" (2015)

No. 10 Katrin Nyman Metcalf "A Legal View On Outer Space and Cyberspace: Similarities and Differences" (2018)

No. 11 Elaine Korzak "Russia's Cyber Policy Efforts in the United Nations" (2021)

No. 12 TALLINN PAPERS YOUNG SCHOLAR EDITION: Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe "Opportunities for Public and Private Attribution of Cyber Operations" (2021)

No. 13 Jeremy K. Davis "Developing Applicable Standards of Proof for Peacetime Cyber Attribution" (2022)

Disclaimer

The Tallinn Papers

The NATO CCD COE's Tallinn Papers are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarization of cyberspace, and technical. Focusing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by invitation, proposals dealing with issues of strategic importance and acuteness will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org

Introduction

The security of cyberspace is a national and international strategic priority and a necessity for many state and non-state actors that seek to create a trustworthy, safe and resilient digital ecosystem for the 21st century. It is only within such a system that the opportunities and benefits of the internet and new technologies can be maximised for all. There are, however, multiple risks and threats to achieving this, from increasingly sophisticated cybercrime and cyber attacks on public bodies and companies to political and economic cyber espionage, interference in democratic processes and elections and the use of cyber offensive weapons in times of (relative) peace and war. Events and crises such as the COVID-19 pandemic, the war in Ukraine and the rapid development and use of new technologies have only accelerated such trends. The challenge is also geopolitical and ideological, underpinned by normative differences and contestation between states on how cyberspace and new technologies more broadly should be governed. Put crudely, a battle between 'liberal' and 'authoritarian' visions[1] has manifested itself at all levels and will have major consequences for security and rights on the internet and on the prospect of consensus and a common understanding and framework emerging for cyber security.

Such trends and developments have galvanised a multiplicity of state and non-state actors to construct and reach a workable consensus on international rules and norms to govern the behaviour of those active in cyberspace. As noted by Chris Painter,[2] 'the rise of the Internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century'.[3] In this context and given the global and interconnected nature of the cyber world, cyber diplomacy has evolved as a necessary tool within the foreign, security and defence policy toolkits of state and regional organisations alike,[4] even though the development of the structures and resources to perform such

[1] Alexander Klimburg, *The Darkening Web*: *The War for Cyberspace*, New York: Penguin Press, 2017. For a nuanced analysis of the manifestation of authoritarianism in multilateralism see: Mark Raymond and Justin Sherman, 'Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice', *Contemporary Security Policy*, 2023, Open Access, https://doi.org/10.1080/13523260.2023.2269809. For positions of major powers on cyber security issues see also Arun Sukumar, 'The geopolitics of multistakeholder cyber diplomacy: A comparative analysis', in Ian Johnstone, Arun Sukumar & Joel Trachtman (Eds.), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Elgar International Law and Technology series. Edward Elgar Publishing, 2023.

[2] Former first coordinator and the first ever cyber diplomat in the United States (US) Office of the Coordinator for Cyber Issues at the State Department created in 2011.

[3] Chris Painter, 'Diplomacy in Cyberspace', American Foreign Service Association, June 2018. https://afsa.org/diplomacy-cyberspace (accessed 30 December 2023)

[4] Tobias Feakin and Johanna Weaver, 'Cyber diplomacy', in (eds) Eneken Tikk and Mika Kerttunen, *Routledge Handbook of International Cybersecurity* (Abingdon: Routledge), 18 February 2020, Routledge Handbooks Online (accessed 30 December 2023), pp277-285.

diplomacy remain at best uneven and asymmetric.[5] Concerning cyber defence and cyber warfare, Paul Meyer, a retired Canadian diplomat, argued in 2012 that 'the creation of significant capabilities within military structures for the conduct of cyber operations contrasts with the lack of parallel diplomatic processes to develop the agreed parameters for such operations'.[6] Meyer called for the establishment of a coherent diplomatic framework and norms to guide state behaviour in the face of the potential militarisation of cyberspace.

Today, it is evident that offensive cyber operations among mature cyber powers in particular are a common feature of cybersecurity strategies.[7] Given the reluctance of states for a variety of reasons to respond with hard military power to any cyber interventions, it is 'sensible for states to consider pursuing their cyber-related interests through forms of soft power, including by framing discourses, setting agendas, forming preferences, developing norms, persuasion and negotiations'.[8] Such cyber diplomacy is essential if state and non-state actors alike are to move towards finding solutions to cyber threats and challenges going forward through an agreed understanding of what constitutes legitimate behaviour in a contested cyberspace characterised by competing and often conflicting normative and interest-based visions[9] of how it should be governed. In this article, I will focus on cyber diplomacy defined as the use of diplomatic tools to manage and resolve problems in cyberspace and conducted by those accredited by national governments, regional organisations (ROs) and international organisations (IOs).

I posit that cyber diplomacy should be considered as an equal and essential part of a broader and holistic state cybersecurity policy toolbox. To this end, I provide an overview of the current state of play in cyber diplomacy; first, conceptually on what it is and second, in terms of how it is evolving in practice. I then go on to discuss the relationship between cyber defence and cyber diplomacy and provide examples of how cyber diplomacy can be used to prevent and respond to cyber incidents, ameliorate tensions and conflict and promote stability in cyberspace. I conclude with thoughts on the challenges, development and practice of cyber diplomacy going forward.

---

[5] Stephanie Borg Psaila, 'Improving the practice of cyber diplomacy: Training, tools, and other resources Phase I', DiploFoundation, www.diplomacy.edu, September 2021.
[6] Paul Meyer, 'Diplomatic Alternatives to Cyber-Warfare: A Near-Term Agenda', *The RUSI Journal*, February/March 2012, 157:1, pp14-19.
[7] Klimburg, *The Darkening Web*, p.301
[8] Eugenio Lilli and Christopher Painter, 'Soft power and cyber security: the evolution of US cyber diplomacy', in (ed) Hendrik W. Ohnesorge, *Soft power and the future of US foreign policy* (Manchester: Manchester University Press, 2023), 161-179.
[9] André Barrinha and Thomas Renard. 'Power and Diplomacy in the Post-Liberal Cyberspace', *International Affairs*, 96:3, pp749-766, 2020, DOI: 10.1093/ia/iiz274.

Cyber Diplomacy

Cyber diplomacy is an extension of diplomacy more broadly, itself a field that has witnessed much change over the years to adapt to new and address pressing issues of our time such as climate change and space in a still-evolving post-liberal[10] and increasingly more chaotic global order. Certain authors have argued that the nature of (inter) national diplomacy has been transformed in terms of both boundaries and complexity.[11] There has thus been a widening and broadening of the processes, scope and actors involved and a transformation of the modes of diplomacy in the multilateral 2.0 world of the 21st century.[12]

As part of this increasingly more complex diplomatic milieu, we can observe that diplomacy in the cyber domain emerged because of the increased political and strategic salience of cyberspace and the criticality of digitalisation and new technologies across all domains of life. We have thus had to move away from the perception that technicians can provide technical solutions to all the problems in cyberspace because 'Cyberspace is developing its own geopolitics, which shape the behaviour of state and non-state actors'.[13] The interconnectedness of the technical and geopolitical has added urgency to the need for diplomacy to maximise opportunities and benefits in cyberspace by protecting against risks and threats and building a trustworthy global ecosystem for the actors that operate in cyberspace. Cyber diplomacy has become necessary for agreement (or at least consensus based on mutual interest) to be reached on the rules for state and non-state behaviour in cyberspace and more broadly to ensure resilience, safety and security across civilian and military physical and virtual networks and infrastructure.

Diplomacy concerning cyberspace has been variously defined in the literature and thus needs some clarification for this article. The literature, for example, often uses cyber

[10] Barrinha and Renard, 2020.
[11] Luk Van Langenhove and Elke Boers, 'Multilevel Diplomacy in Europe in the Digital Century', in George Christou and Jacob Hasselbach (eds.) *Global Networks and European Actors: Navigating and Managing Complexity*, Abingdon, Oxon and NY: Routledge, 2021; Brian Hocking and Michael Smith, 'An Emerging Diplomatic System for the European Union? Frameworks and Issues', *Cuadernos Europeos de Deusto*, 44, 2011, pp.19– 42; Michael H. Smith (2015) 'The EU as a Diplomatic Actor in the Post- Lisbon Era: Robust or Rootless Hybrid?' in Joachim A. Koops and Gjovalin Macaj, *The European Union as a Diplomatic Actor*, European Union in International Affairs Series, Houndmills, Basingstoke: Palgrave Macmillan, 2015.
[12] Luk van Langenhove 'Global Science Diplomacy for Multilateralism 2.0', *Science & Diplomacy*, 5 (3), December 2016; Knud Eric Jørgensen 'EU Diplomacy in Global Governance: The Role of the European External Action Service', in Joachim A. Koops and Macaj, G. (eds*) The European Union as a Diplomatic Actor*, European Union in International Affairs Series, Houndmills, Basingstoke: Palgrave Macmillan, 2015; Christer Jönssson and Richard Langhorne (eds) *Diplomacy Volume III: Problems and Issues in Contemporary Diplomacy*, London: Sage, 2021.
[13] Shaun Riordan and Mario Torres Jarrin, 'Global Policy Perspective Report: Ciberdiplomacy', European Institute of International Studies, Salamanca-Stockholm, January 2020, pp1-10.

diplomacy, e-diplomacy and digital diplomacy interchangeably, despite important differences.[14] Whilst e-diplomacy is now much less used, digital diplomacy has been widely deployed to discuss the increasing use of digital tools to pursue diplomatic objectives.[15] Given the risks and opportunities associated with the development of digital technologies and technology, ROs such as the EU have also articulated the need to 'ensure that digital diplomacy becomes a core component and an integral part of the EU external action'.[16] The EU sees digital diplomacy as more than simply using digital tools to pursue diplomacy and its conclusions highlight the need to promote capacity-building and to be more strategic in promoting technological solutions and governance frameworks that are compatible with its human-centric approach. The EU has opened a dedicated office in San Francisco to pursue and enhance its digital diplomacy with and in the US. It also distinguishes digital diplomacy from cyber diplomacy, whilst acknowledging that the two should be closely coordinated given the synergies between them.[17]

Cyber diplomacy has been defined in the literature as 'the use of diplomatic tools and mindsets in resolving or at least managing, the problems in cyberspace'[18] and the use of 'diplomatic tools and diplomatic thinking'[19] to address issues arising in cyberspace. This is the central focus of this article, whilst also acknowledging that the use of digital tools is not an entirely separate activity while promoting and pursuing diplomacy in cyberspace. To give an example, digital tools may be used in cyber diplomatic strategies and cyber diplomacy may also be needed to address some of the political problems digital diplomacy causes in cyberspace. The debate on cyber diplomacy is not simply limited to what it looks like, but rather to how we think about it in terms of agency; who is it that does and can do cyber diplomacy? This debate is linked to a wider one on diplomacy where commentators have identified 'quasi-diplomatic' actors and argued that 'twenty-first-century diplomacy is coming to resemble that of the Middle Ages: Rising powers, multinational corporations, powerful families, humanitarians,

[14] Shaun Riordan Cyber Diplomacy vs Digital Diplomacy: A Terminological Distinction. USC Center on Public Diplomacy, May 12, 2016. Available at https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digital-diplomacy-terminological-distinction

[15] Shaun Riordan, *Cyberdiplomacy: Managing Security and Governance Online,* Cambridge: Polity Press, 2019; see also, on digital and public diplomacy, Karin Aggestam and Constance Duncombe (eds.), Advancing a New Research Agenda on Digital Disruption in Diplomacy, Special Issue, *The Hague Journal of Diplomacy*, online, 18 December 2023. Available at: https://brill.com/view/journals/hjd/19/1/hjd.19.issue-1.xml

[16] Council of the EU, 'EU Digital Diplomacy: Council agrees more concerted European approach to the challenges posed by new digital technologies', Press Release, 18 July 2023

[17] Council of the EU, 18 July 2023

[18] Riordan 2019, p.5

[19] Carmen Elena Circu, 'Addressing the Gap in Strategic Cyber Policy', *The Market of Ideas*, 2019.

religious radicals, universities and mercenaries are all part of the diplomatic landscape'.[20]

It is hard to disagree that there are multiple actors involved and indeed that shape the cyberspace landscape and much has been written about the role of the private sector in shaping cyberspace across a number of issues.[21] But the question that arises is whether this activity can be considered as diplomatic or whether such diplomacy, in line with a more classical or narrow definition, should be limited to the confines of those accredited by national governments, ROs or IOs.[22] Whilst it can be argued that all actors engaged in shaping the rules of the road and international negotiations on cyberspace are 'diplomats', others argue that this can lead to a hollowing out of diplomacy as a concept and that it makes it difficult to differentiate between the actors that address technical (and often purely legal) rather than political issues in cyberspace. In this article, the focus will be on cyber diplomacy as conducted by those accredited by national governments, ROs and IOs. Its focus is on how such diplomats engage and interact with other actors in cyberspace. This has the advantage of recognising the significance of actors from big tech to civil society in the geopolitical cyber landscape and of ensuring that the significance of diplomats and diplomatic action in the form of dialogue, negotiation, communication and representation in bilateral and multilateral forums to find political solutions to the challenges in cyberspace is not lost. The focus on such 'state' diplomats whilst not straightforward or easy to maintain given that there are grey areas[23] provides a starting point for assessing how states use their diplomatic resources and functions to secure their national interests in and through cyberspace.[24]

[20] Khanna Parag, *How to Run the World*: *Charting a Course to the Next Renaissance*, New York: Randan House, 2011, pp1-272.
[21] For example, on cyber norms, see Louise Marie Hurel and Luisa Cruz Lobato, 'Unpacking Cyber Norms: Private companies as norm entrepreneurs', https://eprints.lse.ac.uk/115525/1/Hurel_unpacking_cyber_norms_published.pdf; J.T Jacobsen, 'Microsoft's challenge to US militarization of cyberspace: A Lacanian study of norm entrepreneurship', *International Studies Quarterly* 2023, DOI: 10.1093/isq/sqad051; N.S. Levinson, 'Idea entrepreneurs: The United Nations Open-Ended Working Group & Cybersecurity', *Telecommunications Policy*, 45, 102142. DOI: 10.1016/j.telpol.2021.102142. See also Riordan, 2019, pp.95-104; and Arun Sukumar, 'The Geopolitics of multistakeholder cyber diplomacy: A comparative analysis', in Ian Johnstone, Arun Sukumar & Joel Trachtman (Eds.), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Elgar International Law and Technology series. Edward Elgar Publishing, 2023.
[22] Riordan and Jarrin, Ciberdiplomacy, 2020.
[23] Riordan, 2019, pp19-29.
[24] André Barrinha and Thomas Renard, 'Cyber-diplomacy: The Making of and International Society in the Digital Age', *Global Affairs*, 3 (4-5), 353-364, 2018.

Finally, in terms of understanding and explaining cyber diplomacy, it must be acknowledged that it is still an emergent field in the academic literature.[25] Indicative of this is that the only existing monograph with a sole focus on cyber diplomacy has come from a practitioner's perspective.[26] From an International Relations (IR) perspective, some works have sought to discuss cyber diplomacy within the English School of IR and as an emerging institution of international society.[27] This situates cyber diplomacy and the use of diplomatic resources and functions to secure cyberspace in an emergent but still-evolving post-liberal order.[28] Aside from these, there is academic work from mainly critical and institutional perspectives that is relevant to cyber diplomacy in practice but does not conceptualise or theorise it explicitly; such works vary from work on attribution and deterrence to international regimes, governance, multi-stakeholderism,[29] cyber power,[30] cyber norms and strategic narratives.[31] Whilst it is beyond the scope of this article to delve further into the theoretical attempts to conceptualise and theorise cyber diplomacy, it is important to acknowledge the growing significance of such work from across different disciplines as cyber diplomacy evolves and as we seek to explain and understand what it is, what it looks like, what it does and who does it, as well as its effects locally, nationally, regionally and globally.

Cyber Diplomacy in Practice

We have already established the geopoliticisation of cyberspace and the significance of digital technologies which has meant that issues of cybersecurity have become more prominent on political agendas. In relation to cyber diplomacy, in 2010 Gady and Austin asserted that 'Few governments have even thought about the diplomatic dimension of cybersecurity and they certainly haven't developed diplomatic strategies commensurate with the threats'.[32] This was echoed in 2013 by Heli Tiirmaa-Klaar[33] who wrote:

[25] Barrinha and Renard, Cyber-diplomacy, 2018. André Barrinha and Mark Raymond, 'Cyber diplomacy in International Relations', in George Christou, Wilhelm Vosse, Joe Burton and Joachim Koops, *Handbook on Cyber Diplomacy*, Palgrave MacMillan, (forthcoming, 2025).
[26] Riordan, 2019.
[27] Barrinha and Renard, 2018.
[28] Barrinha and Renard, 2020.
[29] Johnstone et al, 2023.
[30] Richard J. Aldrich and Athina Karatzogianni, 'Cyber Power and Cyber Diplomacy', in George Christou, Wilhelm Vosse, Joe Burton and Joachim Koops, *Handbook on Cyber Diplomacy*, Palgrave MacMillan, (forthcoming, 2025).
[31] See Barrinha and Raymond (forthcoming 2025) for an excellent overview of IR theory and cyber diplomacy. See Christou et al, *Handbook on Cyber Diplomacy* (forthcoming 2025), Part I, for a review of how cyber diplomacy is treated from numerous disciplinary perspectives.
[32] Franz-Stefan Gady and Greg Austin, 'Russia, the United States and Cyber Diplomacy: Opening the Doors', East-West Institute, 2010, 1-19.
[33] Former Ambassador at Large for Cyber Diplomacy and Director General of the Cyber Diplomacy Department, Estonian Ministry of Foreign Affairs (2018-2021); Former Head of Cyber Policy

> We are still in a very early stage of shaping cyber foreign policy, few MFAs have a special cyber office. In most of the MFAs, cyber aspects are being mainstreamed into daily work on human rights, international security, transnational threats and other issues, even if there is no special cyber unit established. If states would like to cover all relevant cyber aspects, they need a good team of cyber diplomats.[34]

The rationale for cyber diplomacy is now more prominently articulated globally and its practice has evolved since 2013 and we have witnessed an accelerated development nationally, regionally and within international institutions.

However, there is still little substantive comparative work on how states have adapted their governance structures to the growing need for cyber diplomacy and cyber diplomats. Barrinha and Renard observed in 2020 that:

> Dozens of ministries have been creating offices exclusively dedicated to cyberspace and appointing "cyber diplomats" [...] This move has concentrated more international cyber policy activities in foreign affairs ministries, elevating the issue in government hierarchies and increasing the level of international activity of each state in cyberspace.[35]

To this end, it has been argued that the logic that underpinned the development of institutional capacity within states to deal with cyber security was that of avoiding fragmentation and achieving coherence in coordination on cyber issues. Initial observations of such institutionalisation in Ministries of Foreign Affairs have suggested two main approaches, although hybrid models have also emerged: centralisation of cyber activities as in the UK, similar to other foreign policy themes; and creation of coordinating units, thus acknowledging the cross-cutting nature of cyber issues as in the US.[36]

The first state to set up such structures was the US under the Obama administration through its Office of the Coordinator of Cyber Issues in 2011. The US also provided the impetus for other, mainly Western, like-minded states and ROs to act in the cyber domain including Germany, the EU, Japan and Australia[37]. Under the Trump administration (2016-2020), organisational changes such as the decision to abolish the position of 'cyber czar' signalled that the US was stepping back from its leadership role in cyber diplomacy, even though there were elements of continuity in using diplomacy across a range of cyber issues including those related to the tech supply chain. Under

Coordination, European External Action Service (2012-2018); Former Cyber Defence Policy Advisor, NATO HQ International Staff (2011-2012); Former Executive Director of the National Cyber Security Council and Senior Advisor, Estonian Ministry of Defense (2007-2010).

[34] Heli Tiirma-Klaar, 'Cyberdiplomacy: Agenda, Challenges and Mission', in Katharina Ziolkowski (ed) *Peacetime Regime for State Activities in Cyberspace*: *International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, pp509-529.

[35] André Barrinha and Thomas Renard, 'The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Space', Blog Post, Council on Foreign Relations, 10 June 2020.

[36] Barrinha and Renard, 2018. On 'diplomatisation' in the cyber domain see also André Barrinha, 'Cyber-diplomacy: the emergence of a transient field', *The Hague Journal of Diplomacy*, 2024, pp. 1-28.

[37] Barrinha and Renard, 2018. On Australia's cyber diplomacy see Feakin and Weaver, 2020. On Japan, see Wilhelm Vosse, 2023; see also Mark Bryan F. Manantan, Advancing cyber diplomacy in the Asia Pacific: Japan and Australia, *Australia Journal of International Affairs*, 75 (4), pp432-459.

President Biden, cyber diplomacy was once again elevated and made a top priority at every level of government, with cyber diplomats seen as critical in preventing cyber incidents, mitigating risks in cyberspace and defending democratic values.[38] This re-prioritisation of cyber diplomacy was underpinned by the establishment by Congress of the Office of the National Cyber Director (ONCD) in 2021. The Office advises the President on cybersecurity policy and strategy and is a part of the Executive Office of the President[39] at the White House. The ONCD also led the development of a new US National Cybersecurity Strategy, published in March 2023 and coordinates a whole-of-government approach to implement this strategy. The US Cyber Diplomacy Act of 2021 also addresses key aspects of international cyberspace deliberation and the Bureau of Cyberspace and Digital Policy was created in 2022, along with the appointment of a US Ambassador at Large for Cyberspace and Digital Policy, Nathaniel C. Fick.[40]

In Europe, there has been an acceleration in the number of states recognising and reacting to cyber risks and threats, with all 27 EU member states having developed a cyber strategy and some ten (Denmark, Sweden, Finland, Estonia, Netherlands, Germany, Poland, Czech Republic, France, Spain) and two non-members (UK, Switzerland) also appointing cyber ambassadors, envoys and representatives.[41] This article cannot, of course, provide a comprehensive review of all European states in relation to cyber diplomacy, but rather points to examples of how particular states and the EU have addressed this issue.[42] To this end, front-runners in Europe have included Estonia and Denmark. Drawing on the lessons of the Distributed Denial of Service (DDoS) attacks in 2007, Estonia produced its first cyber security strategy in 2008, ensuring the construction of a whole-of-government organisational and administrative structure for coordination of its cybersecurity approach.[43] In terms of its cyber diplomacy, the Estonian Ministry of Foreign Affairs (supported by a cyber diplomacy department established in 2019) engages and represents Estonia's positions internationally and Estonia appointed an Ambassador at Large for Cyber Diplomacy (Heli Tiirmaa-Klaar and, at the time of writing, Tanel Sepp) in 2018. Denmark appointed the first Tech Ambassador in 2017,[44] with a physical presence in Silicon Valley as part of its efforts to elevate tech diplomacy (technology and digitalisation) 'to a cross-cutting foreign and security policy priority of the Danish government' and to reshape 'traditional understanding of diplomatic representation'. Having published its

[38] Lilli and Painter, 2023.
[39] Office of the National Cyber Director, https://www.whitehouse.gov/oncd/
[40] Bureau of Cyberspace and Digital Policy: https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/#:~:text=The%20Bureau%20of%20Cyberspace%20and,and%20people%20everywhere%20can%20prosper.
[41] Tania Lațici, 'Understanding the EU's approach to cyber diplomacy and cyber defence', Briefing, EU Policies - Insights, European Parliamentary Research Service, May 2020.
[42] For trends in how other states in Europe and globally have developed their cyber capacity and diplomacy approaches, see: https://eucyberdirect.eu/atlas/country/
[43] Marina Kaljurand, 'Taking stock of Estonia's multistakeholder cyber diplomacy' in Ian Johnstone, Arun Sukumar & Joel Trachtman (Eds.), *Building an International Cybersecurity Regime: Multistakeholder Diplomacy*. Elgar International Law and Technology series. Edward Elgar Publishing, 2023.
[44] Robbie Gramer, 'Denmark Creates the World's First Ever Digital Ambassador: Diplomacy goes digital, Foreign Policy': https://foreignpolicy.com/2017/01/27/denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy/

first cyber security strategy in 2014 and most recent in 2022, its tech diplomacy approach was constructed to address significant and interlinked global borderless foreign policy challenges relating to the fourth industrial revolution that affect society. These include cybersecurity, artificial intelligence, the Internet of Things (IoT), cryptocurrency, multinational tech influence, the transformative power of new technologies and the rise of non-state actors and their effect on the evolving geopolitical order.[45]

The EU has developed a comprehensive system to address cyber security threats, including cyber diplomacy. Whilst it has stopped short of appointing a cyber czar or representative to project, negotiate and represent its positions on the global stage, in 2015 it sought to articulate and enhance specific cyber diplomacy goals (Council of Ministers 2015) and in 2017 established a cyber diplomacy toolbox. It also agreed to develop a framework for joint EU diplomatic response to malicious cyber activities, The EU cyber diplomacy toolbox makes 'full use of measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures' and that 'contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations'.[46] In May 2019, the EU established a general framework for its sanctions regime[47] and in the 2020 edition of its cyber security strategy (the first being published in 2013) there was a focus not only on internal capacity-building and cyber-resilience against cyber threats, but also on technological sovereignty, leadership and building international partnerships to 'strengthen the rules-based global order, promote international security and stability in cyberspace and protect human rights and fundamental freedoms online'. This includes not only the advancement of international norms for cyberspace but also external capacity-building and the creation of an 'EU Cyber Diplomacy Network around the world to promote its vision of cyberspace'.[48]

---

[45] Ministry of Foreign Affairs, Denmark, Office of the Tech Ambassador: https://techamb.um.dk/team/meet-the-ambassador

[46] Council of Ministers, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")', 9916/17, Brussels, 7 June 2017. The cyber diplomacy toolbox includes measures to address all levels of the conflict spectrum: **Preventive measures** – cyber confidence and capacity building abroad, awareness raising activities of EU cyber policies; **cooperative measures** – political and thematic dialogues or EU diplomatic démarches; **stability measures** – official statements by EU leadership, Council conclusions, diplomatic engagements in international forums and démarches; **restrictive measures** (sanctions) – travel bans, arms embargos, freezing of assets; **EU support for Member States' lawful responses should they fall victim to a cyber act**: including in the case of invoking the EU's mutual assistance clause, Article 42 (7) TEU and the solidarity clause, Article 222 TFEU. NATO Allies can also invoke Article 5.

[47] The EU chose in May 2022 to extend its framework for restrictive measures against cyber-attacks threatening the EU and its member states until 18 May 2025. Sanctions currently apply to eight individuals and four entities and include an asset freeze and a travel ban. **See:** Council of the EU, 'Cyber attacks: Council extends sanctions regime until 2025', Press Release, 18 May 2023. Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States; Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

[48] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020) 16 final, 16 December

Cyber Diplomacy and Defence

This final section will focus on cyber defence and how cyber diplomacy can be used to prevent and react to the trend of increasing cyber incidents and the proliferation and use of cyber tools and weapons for malicious or strategic purposes in cyberspace. Cyber defence is more broadly defined than simply protecting military assets. There is an increasingly blurred line between the civilian and military spheres as both depend on a safe and secure cyberspace to protect supply chains, systems and critical infrastructure ranging from electricity grids to underwater cables, transport and communication. Penetration of critical infrastructures can have a variety of effects from paralysis and physical damage to disruption and catastrophe. There are also the issues that arise from the use of disruptive technologies such as AI in cyber defence. Of course, such disruptive technologies can be deployed to protect and defend against attacks and respond offensively, but they can also be used for malicious purposes.[49]

Cyber diplomacy can be used to establish internationally agreed guidelines on state and non-state actor behaviour in cyberspace. There are multiple elements to this: cyber warfare and to what extent a cyber-attack can be considered an armed attack; advancing responsible state behaviour through agreed norms[50] on what states should and should not be doing across a range of issues such as human rights and privacy, ensuring supply chain security, and not targeting critical infrastructure; issues connected to diplomacy for preventing the proliferation of a cyber arms race. Cyber diplomacy has a communicative function in engaging with relevant actors at different levels across these three elements; a preventative function in mitigating any negative consequences related to the actions of state and non-state actors; and a stabilising or transformative function in establishing a framework of acceptable and responsible behaviour that ensures, at minimum, the applicability of international law in cyberspace.

Let us take some examples to further illustrate the role and need of cyber diplomacy across the different elements outlined. The first relates to that of defining the rules and parameters for what constitutes an act of cyberwar. There have been multiple attempts to differentiate, through the first and second iterations of the *Tallinn Manual*,[51] 'between cyber attacks that do not constitute a use of force, attacks that do constitute a use of force but do not constitute an armed attack and attacks that amount to an

2020. On EU cyber diplomacy see also: Michael Reiterer, 'EU Cyber Diplomacy: Value – and Interest-Driven Foreign Policy with New Focus on the Indo-Pacific, on Gertjand Boulet, Michael Reiterer and Ramon P Pardo (eds), *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives,* New Security Challenges Series, Palgrave MacMillan, 2022; and Patryk Pawlak, 'Rebooting the EU's Cyber diplomacy', 8 November 2019, EU Cyber Direct. Available at: https://eucyberdirect.eu/research/rebooting-the-eus-cyberdiplomacy

[49] Lațici, 2020.

[50] On the implementation of such norms agreed at UN level, see: https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[51] https://guides.ll.georgetown.edu/cyberspace/cyber-conflicts

armed attack'.[52] Despite proportionality being baked into the manual, such distinctions are important as they determine how one state can retaliate against another, with the risk of a kinetic attack in response to a cyber incident. Any such escalation, if we are to view this from a security dilemma perspective, might also harm any deterrence efforts. Cyber diplomacy through bilateral and multilateral channels is important in this context, with the caveat that it must be accepted by all the major players in cyberspace. As noted by Barrinha and Renard, the exclusion of 'non-liberal-minded' states in the construction and agreement of the Tallinn manuals[53] has led to a lack of credibility and legitimacy in those states marginalised from the process. It also points to the need for the Western like-minded states to play to the rules. If this is not the case then it creates an environment where Western disregard for the rules (for example, Snowden or Stuxnet) are used for justification for exceptional actions by other states.[54]

This is not to say that cyber diplomacy cannot work in cyberspace and we have seen this in numerous bilateral agreements, including the short-lived US-China Cyber agreement of 2015 concerning hacking and espionage activities. Normative commitments to abstain from cyber attacks against each other have also been penned between the US and Russia (2013), China and Russia (2015), the US and Japan (2019),[55] and states in the Shanghai Cooperation Organisation (SCO) coming together to negotiate, agree and communicate their collective view on information security and cyber sovereignty in cyberspace at the United Nations (e.g., International Code of Conduct for Information Security 2011, revised 2015). It can also be argued that within the UN process, the United Nations Governmental Group of Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGE) came to broad agreement and consensus in 2010, 2013 and 2015 on principles for the applicability of international law in cyberspace (UNGGE Report 2015); and that subsequent negotiations in the UNGGE and the Open Ending Working Group (OEWG, led by Russia and formed in 2018) led to consensual reports being published in May and March 2021 respectively. UN General Assembly Resolution 75/240 also established a new five-year Open Ended Working Group (2021 to 2025) on security and the use of information and communications technologies.[56] In addition, UN member states agreed a Programme of Action 'to advance responsible State behaviour in the use of information and communications technologies in the context of international security' with a focus on implementing previously agreed frameworks (UNGGE and OEWG) at national and regional levels through an open, transparent and action-oriented

[52] Riordan 2019, p71.
[53] Note that one Chinese international law expert was included in the expert group that produced Tallin 2.0 but no Russian experts. See Milton Mueller, 'Against Sovereignty in Cyberspace', International Studies Review, 22, pp.779-801, 2020, p.786.
[54] Riordan, 2019, p.76. See also Jarrin and Riordan, 2023 for further discussion on cyber diplomacy and the Law of Armed Conflict, and attribution in cyberspace. See also Izycki et al, 2023 for discussions on cyber diplomacy and capacity building, Confidence Building Measures (CBMs) and attribution.
[55] Patryk Pawlak and Thomas Biersteker. 'Guardians of the Galaxy: EU Cyber Sanctions and Norms in Cyberspace', Challoit Paper/155, October 2019.
[56] UN Office for Disarmament Affairs. https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021#:~:text=Show%20more-,Background,and%20communications%20technologies%202021%E2%80%932025.

process.[57] Such developments come with a note of caution as much work still needs to be done to determine what this means for stability in practice and implementation when it comes to state behaviour in cyberspace. This, in particular, given the differing interpretations of core principles and rules of international law that exist in times of war and peace and the essence of the UN mechanism that should exist to implement them.[58]

Cyber diplomacy is thus a necessity because, as Riordan suggests, 'Good enough, even if flawed, is better than nothing – in cyberspace, a bad agreement is better than no agreement'.[59] This is taken further with the work of Renard on EU bilateral cyber strategic dialogues. He concludes that effects must be understood beyond the material notion of impact (how effective an actor is in fulfilling cyber diplomatic goals) to include symbolic and discursive effects.[60] Such effects are important in assessing diplomatic performance in the bilateral, multilateral and multi-stakeholder processes of cybersecurity as they: ensure critical issues remain on the table; facilitate communication on such issues and ensure that, for example, important norms and rules remain visible as a guide to state and non-state behaviour, even if interpreted differently by the actors involved; help to reduce misunderstandings and mitigate the likelihood of a cyber arms race; and provide the foundations for the creation of a cyber diplomatic community of practice (COP) that can mitigate the risk of escalation in cyberspace.[61]

The UN GGE and OEWG are prime examples of the intricacies and difficulties of diplomacy in cyberspace. Dialogue within these processes can contribute to the implementation of agreed norms and new bilateral mechanisms of cooperation if consensus is found and can put them at risk if a consensus is not reached.[62] There are also other salient examples of incidents and events that point to the need for cyber diplomacy in cyber defence to reduce risk and mitigate the effects of cyber incidents and episodes, whether state-on-state or involving the private sector and other actors. Huawei's role in the provision and implementation of 5G mobile technology provides multiple lessons for cyber diplomacy both in the preventative sense and in terms of future diplomacy. Provision by Huawei was first framed as a threat to 'national security', with the lead protagonist being the US which imposed sanctions on Huawei and banned them from their networks. The UK followed in 2020 and stipulated that UK 5G networks would be Huawei-free by 2027. What has followed is a variety of state approaches towards such Chinese technologies, from outright bans to proportionate

[57] On this, see: Statement on the Cyber Programme of Action, Cyber Peace Institute, July 2023 https://cyberpeaceinstitute.org/news/statement-cyber-programme-of-action/#:~:text=Scope%20of%20the%20Programme%20of,further%20build%20upon%20this%20work.
[58] Lousie Marie Hurel, Avoiding Deadlock Ahead of Future UN Cyber Security Negotiations, Commentary, RUSI, 31 August 2023; Aleksi Kajander, 'Unnecessary Repetition: Russia's Latest Attempt at a New UN Convention on Cyberspace', and 'A Tale of Two Draft Resolutions: A Report on the Polarizing International Law Discussions at the 2023 OEWG Substantive Session', NATO CCD COE, 2023. Available at: https://ccdcoe.org/library/publications/
[59] Riordan 2019, p.73.
[60] Thomas Renard, 'EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain', *European Politics and Society*, 19 (3), p.321-337.
[61] Riordan 2019, p.73.
[62] Hurel, 2023.

risk assessment of technologies and products. This is not the only issue, however, that has needed diplomatic attention. As Riordan and Jarrin point out, having left mobile telephony standard-setting to technicians and officials from telecoms ministries who did not fully understand the geopolitical or security implications of China's increased attention, role and significance there are implications for how such standards need to be negotiated in the future by cyber diplomats.[63]

More recently we have seen the increased role of private actors in the Ukraine conflict through the deployment of AI and other technologies. Here, the case of Palantir raises both ethical and normative questions about whether the rules and laws of war are being stretched at best and ignored at worst; questions no doubt that diplomats in the cyber domain will need to address to ensure the applicability of international law and the appropriate and proportionate use of new technologies in times of war and peace.[64] Similarly, the use of facial recognition software such as Clearview AI, 'engulfed by claims of privacy violations and banned by several governments', has been used by the Ukraine government to counter Russian propaganda. This is controversial for many digital rights activists who have claimed its use can be interpreted as a violation of the Geneva Convention.[65] It thus raises important questions for cyber diplomats who are seeking to construct and establish laws and rules on the use of technologies such as AI in offensive information war strategies. Finally, the export of dual-use technologies has vexed cyber diplomats, in particular in relation to authoritarian states but also the war in Ukraine. The EU, for example, has imposed sanctions on Russia over dual-use goods and 'has sharpened and extended export controls on dual-use goods to target sensitive sectors in Russia's military-industrial complex and limit Russia's access to crucial advanced technology'.[66] These include drones and their software, software for encryption devices, semiconductors and advanced electronics. For its 13th package of sanctions in February 2024, the EU also proposed export bans on companies that are suspected of helping Russia to evade sanctions on technological goods, which would not mean an asset freeze, but rather be 'entity-non-grata for dual-use exporters inside the bloc'.[67]

[63] Riordan and Jarrin, Cyber diplomacy, 2020.
[64] Vera Bergengruen, How Tech Giants Turned Ukraine into an AI War Lab, Time, 8 February 2024.
[65] Maya Sobchuk, 'How Ukraine Uses AI To Fight Russian Information Operations', Commentary, Global Governance Institute, 12 February 2024. Available at: https://www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations
[66] European Commission, 'EU Solidarity with Ukraine': https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine/sanctions-dual-use-goods_en
[67] Nicholas Vinocur, Brussels Playbook, Politico, 15 February 2024. It is important to not here, though, that the credibility of any such sanctions and controls has been undermined in the past because many of the sales of such dual-use technologies to authoritarian states come from the very states in the West that seek to impose sanctions; see, for example, Ross James Gildea and Federica D'Alessandra, 'We Need International Agreement on How to Handle These Dangerous Technologies', 7 March 2022, Slate.com.

Conclusions

This article has provided an overview of how cyber diplomacy has evolved, its definition, how it has developed and how it has been performed in relation to critical issues of cyber security and cyber defence. The central debates and trends identified have illuminated the need for further government and governance adaptation to develop, integrate and constitute cyber diplomatic practices within the foreign policies of governments and ROs and towards the increasing importance of the role of cyber diplomats in times of war and peace whether related to preventative, cooperative, restrictive or reactive measures in response to the increased sophistication and complexity of incidents and the use of new technologies. It has also pointed to the need for cyber diplomacy to build coalitions and alliances to bridge the ideological gap that exists over important issues of cyber security.

Whilst the article relies on a handful of Western-centric examples, states in the global south have also become more active in cyber diplomacy.[68] There is also no doubt that the cyber diplomacy landscape has become more challenging geopolitically and concerning new trends and developments in disruptive technologies (AI,[69] 5G/6G, cloud and quantum computing and IoT). This has not only increased the complexity of the issues related to the governance of cyberspace (physical, logic, data and social[70]) but also of the multiple stakeholders needed to reach effective outcomes.

Cyber diplomats will need to adapt and evolve to address the trends of the increased digitalisation of society and the use of offensive cyber weapons in cyberspace, find solutions to issues of privacy and data protection and address cybercrime, resilience, attribution and rules of engagement and adherence to international law in cyberspace. This will entail not only that foreign ministries in the global north and south continue to build capacity and integrate issues of internet governance and cybersecurity into their foreign and security policy structures and strategies, but also that adequate training is provided for cyber diplomats to acquire the knowledge and skills required to undertake their roles effectively. The evolution of a cyber diplomacy 'COP will be essential for cyber diplomats to manage, communicate and negotiate their relationships effectively with other state and non-state actors in the global cyberspace milieu' with such a COP only being advantageous if there is a clear cost to not being a member of such a community.[71]

That cyber diplomacy is essential to the defence of cyberspace is no longer disputed in policy and academic circles. More work must be done to refine, define, explain and

[68] Such as, for example, in the United Nations Group of Governmental Experts and the Open-Ended Working Group that seek to reach agreement on cyber norms for responsible state behaviour in cyberspace. On this, see Louise Marie Hurel, Avoiding Deadlock Ahead of Future UN Cyber Security Negotiations, RUSI Commentary, 31 August 2023. See also Eduardo Izycki, Bret van Niekerk and Trishana Ramluckan, 'Cyber Diplomacy: NATO/EU Engaging with the Global South', 15th International Conference on Cyber Conflict, NATO CCD COE, 2023; Barrinha and Raymond, (forthcoming, 2025).
[69] On AI and cyber (public) diplomacy see: Alina Bârgăoanu and Bianca-Florentina Cheregi, 'Artificial Intelligence: The New Tool for Cyber Diplomacy: The Case of the European Union', in F. Roumate (ed.), *Artificial Intelligence and Digital Diplomacy*, Switzerland: Springer Nature, 2021.
[70] Klimburg, 2017.
[71] Jarrin and Riordan, Ciber diplomacy, 2020.

understand what cyber diplomacy is and does, who does it and how and where it can be most effectively used to work towards reducing risks, addressing threats and achieving stability in cyberspace. Progressing a cyber diplomacy COP will be important to such work and will be reflective of how, by whom and where cyber diplomacy is practised in addressing real-world cyber issues going forward. Its development can also be facilitated through integrating cyber diplomacy into cyber security exercises and scenarios in and beyond Europe,[72] providing opportunities for state and non-state actors to learn and build trust through testing potential diplomatic as well as legal, tactical and strategic responses to cyber security challenges.

[72] See, for example, Dessy P Saputri, Srryanto D.W., and Helda Risman, Indonesian Cyber Diplomacy: Asean-Japan Online Cyber Exercise, *Technum Social Sciences Journal*, 9, 453-464, July 2020. On lessons and challenges related to NATO cyber exercises see: Amy Ertan, Veronika Datzer, Aurimas Kuprys and Lisa Schauss, NATO Cyber Exercises: Moving Ahead, CyCon 2022 Workshop Summary, NATO CCD COE, December 2022. Cyber diplomacy injects could also be explored in the annual Locked Shields cyber defence exercises organised by NATO CCD COE (https://ccdcoe.org/exercises/locked-shields/), and also the cyber exercises organised by the European Union Agency for Cybersecurity (ENISA): https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises