STIMSON

EU CYBER DIRECT

CYBER ACCOUNTABILITY BUILDING

Andrea Calderaro

STIMSON

EU CYBER DIRECT

CYBER ACCOUNTABILITY BUILDING

Andrea Calderaro

July 2024

Suggested citation: Calderaro, Andrea (2024) *Cyber accountability building* Policy brief, EU Cyber Direct, July 2024.

This publication has been produced in the context of the EU Cyber Direct – EU Cyber Diplomacy Initiative project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

Cover image credits: Esteban Chinchilla/Unsplash

Implementing organisations:

EU Institute for Security Studies
Carnegie Endowment for International Peace
Leiden University

Funded by the European Union

Contents

1. INTRODUCTION 7
2. CYBER CAPACITY BUILDING (CCB) AND ACCOUNTABILITY 9
3. FRAMING ACCOUNTABILITY IN CYBERSECURITY 10
4. EXTERNAL ACCOUNTABILITY THROUGH CYBER DIPLOMACY CAPACITY BUILDING 11
4. CCB FOR ENHANCING DOMESTIC ACCOUNTABILITY 13
5. CONCLUSION 15
ABOUT THE AUTHOR 17
ABOUT EU CYBER DIRECT 18

1. Introduction

The transnational nature of connectivity infrastructure and the borderless routing of data increasingly highlight the critical role that international cooperation plays in strengthening the safety and stability of the cyber domain. Beyond initiatives aimed at enhancing national capacities to protect critical information infrastructure from cyber threats, states increasingly engage transnationally in the governance of cybersecurity. Fostering trust in this global approach involves establishing accountable platforms and mechanisms. This can only be achieved if participants have both the capacity to negotiate accountability frameworks and the ability to adhere to them. In this context, cyber capacity building is crucial for enabling actors to play an active role in these key processes.

This is particularly critical due to the variety of actors and platforms involved in this endeavour. Notably, the United Nations Group of Governmental Experts (UNGGE) and the UN Open-Ended Working Group (OEWG) have emerged as significant efforts in this direction. These multiannual processes under the UN's auspices have facilitated dialogues among UN member states regarding norms and principles concerning the "security of and in the use of information and communications technologies". The initiatives underscore the importance of cooperative measures to address the complexities of cyber threats that transcend national borders.[1] In addition, the UN Ad Hoc Committee is spearheading negotiations on cybercrime, aiming to create a comprehensive international legal framework to combat cyber-related criminal activities.[2] Beyond the UN context, similar negotiations are occurring within the G7, where member countries discuss strategies to mitigate cyber risks and promote cyber resilience, and within the World Trade Organization (WTO) in the context of digital trade. Meanwhile, the International Telecommunication Union (ITU) is traditionally engaged in negotiations on the technical aspects concerning the functioning of the internet, highlighting the need for harmonized standards and protocols.

However, while the variety of international cooperation platforms can be welcomed as a means to consolidate a global effort to protect the various aspects of digital infrastructure's functioning, the lack of a consistent and comprehensive approach among these initiatives creates a vacuum of legitimacy. If the above-mentioned UN-led processes have a specific mandate to negotiate state-responsible behavior in cybersecurity, other initiatives address different aspects concerning the safety and stability of the cyber domain. Operating in silos with few formal tools to enhance a consistent and comprehensive approach results in a lack of legitimacy, raising critical

[1] "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 'Final Substantive Report.'" United Nations, 2021, accessed June 24, 2024, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Zero-Draft-19-01-2021.pdf.

[2] "Comprehensive Study on Cybercrime," United Nations: Office on Drugs and Crime, 2021, accessed June 27, 2024, https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html.

questions about what accountability in cybersecurity entails and, if relevant, how it could be achieved.

2. Cyber Capacity Building (CCB) and Accountability

Drawing from the available literature addressing accountability in global politics, the discussion proposed with this paper expands on how achieving accountability in cybersecurity necessitates enhancing inclusivity and bridging power inequalities in negotiating the mechanism and agendas on which accountability in a transnational governance approach to cybersecurity is grounded. By emphasizing this priority, this paper focuses on the role that Cyber Capacity Building (CCB) initiatives play in enhancing accountability in cybersecurity. Building on Slaughter's (2004) approach to accountability in the context of "Government of Networks", I examine Cyber Capacity Building for strengthening what the author frames as 'external' and 'domestic' accountability mechanisms.[3] According to this framework, if the equal distribution of cyber diplomacy capacity is critical to legitimizing multilateral approaches and strengthening 'external' accountability in cybersecurity, it is also pivotal that delegations are legitimized through the implementation of domestic accountability mechanisms. This is particularly relevant in the domain of cybersecurity, given that states have limited ownership of digital assets and broader limited control over the functioning of the internet. This approach enables better systematizing of CCB initiatives as a set of complementary instruments for empowering not only governments but also industry and civil society organizations to engage in inclusive dialogues among stakeholders to ensure comprehensive cybersecurity frameworks both nationally and transnationally. To better reflect the need to strengthen CCB beyond state actors, I refer to cyber capacity building "as the diffusion of technical, governance and diplomatic skills among relevant stakeholders, including government, industry and civil society actors, to ensure the development of sustainable connectivity".[4]

[3] Anne-Marie Slaughter, "The Accountability of Government Networks," Indiana Journal of Global Legal Studies 8, no. 2 (2021), accessed June 27, 2024, https://www.repository.law.indiana.edu/ijgls/vol8/iss2/5.

[4] Andrea Calderaro and Anthony J. S. Craig, "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building," Third World Quarterly 41, no. 6 (March 19, 2020): 920, https://doi.org/10.1080/01436597.2020.1729729.

3. Framing Accountability in Cybersecurity

Accountability is traditionally perceived as a critical aspect of global politics, and this applies to the discourse and practices on cybersecurity as well. Notably, accountability in international cooperation is established when power-wielders are held responsible for their actions through mechanisms that provide information and allow for actions, ensuring oversight and influence.[5] However, to establish accountability, it is critical to achieve a shared agreement within the international community regarding the norms and tools of relevance.[6] International negotiations on cybersecurity are not immune to this, and seeking accountability in the cybersecurity domain involves identifying the most accountable institutions and actors ensuring safety and stability in the cyber domain[7], in addition to agreeing on the norms and international legal obligations to which actors should be accountable.

The multifaceted nature of international cooperation in this field, where a variety of platforms are available to enhance dialogues between stakeholders beyond state actors, including industry and civil society organizations, aligns with what Slaughter frames as "Government Networks"[8]. Recognizing the role that Government Networks play in negotiating various aspects of the contemporary global order, Slaughter (2004) emphasizes the critical role that accountability plays in ensuring the legitimacy of these networks.[9] Notably, legitimacy can be achieved with transparency and inclusivity, avoiding the dominance of a limited number of actors.

Inclusivity does not merely consist of waiving restrictions to negotiating platforms but requires that state and non-governmental representatives from all regions of the world have the capacity to actively contribute to these negotiations. Without such active participation, these platforms are no much more than a means to impose hegemonic control by a limited number of actors over processes. This would weaken the credibility of negotiating accountability rules, jeopardizing the legitimacy of the institutional set-up. Although Slaughter (2004) refers to this priority as the concept of accountability in the broader context of global politics, this principle is similarly relevant to cybersecurity.[10]

[5] Robert O. Keohane, "The Concept of Accountability in World Politics and the Use of Force," Michigan Journal of International Law 24, no. 4 (2003): 1121–41, https://repository.law.umich.edu/mjil/vol24/iss4/9.

[6] August Reinisch, "Securing the Accountability of International Organizations," Global Governance 7, no. 2 (2001): 131–49.

[7] Patryk Pawlak, "Accountability in Cyberspace: The Holy Grail of Cyber Stability?," EU Cuber Direct, March 18, 2024. https://eucyberdirect.eu/research/accountability-in-cyberspace-the-holy-grail-of-cyber-stability

[8] Slaughter, "The Accountability of Government Networks."

[9] Anne-Marie Slaughter, "Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks," Government and Opposition 39, no. 2 (2002): 159–90.

[10] Slaughter, "Disaggregated Sovereignty: Towards the Public Accountability of Global Government Networks."

4. External Accountability through Cyber Diplomacy Capacity Building

Accountability in the context of global politics traditionally grounds itself on the role of the state (Goodhart 2014). Similarly, international cooperation in the cybersecurity domain relies on multilateral negotiations under the UN mandate, reflecting states' capacities to negotiate norms and be accountable to them. For this reason, initiatives aimed at supporting cyber capacity building strategies have consistently identified pathways to support states in developing and mastering their national cybersecurity framework. As a result, governments have been the main beneficiaries of CCB support for leading the implementation of a series of initiatives, including the launch of National Cybersecurity Strategies, the establishment of National Cybersecurity Agencies and Computer Emergency Response Teams (CERTs), the design of cybercrime legal frameworks, the promotion of public-private partnerships, and the enhancement of education and awareness. This approach is generally shared by the Oxford Cybersecurity Maturity Model,[11] the ITU Global Cybersecurity Index,[12] and the "Operational Guidance for the EUs International Cooperation on Cyber Capacity Building".[13] The combination of indicators and approaches to assess and implement national cyber capacity building has led to investments and supporting initiatives primarily aimed at reinforcing states' cyber capacity domestically.

Following years of implementation, the development of national cyber capacity has played a critical role in enhancing governments' abilities to strengthen resilience in cybersecurity. At the same time, the boost in international cooperation in the cybersecurity domain has called countries to enhance their capacity to engage in international cooperation dialogues. This priority became especially evident with the launch of the UN OEWG (2019-2021). Unlike the UN Group of Governmental Experts (GGE), which between 2004 and 2021 limited the number of state representatives to a maximum of 25 in its later versions,[14] the UN OEWG called upon all UN Member States to play an active role in negotiating rules and principles which states should be accountable. However, the first UN OEWG (2019-2021) agenda was mostly shaped by statements delivered by representatives from a limited number of countries from Europe and North America, in addition to notable contributions from China and Iran.[15] The limited engagement of most UN Member States from Africa, Asia, and Latin America highlighted the critical need to enhance cyber diplomacy capacity by empowering representatives from the Global South to engage in growing international cooperation efforts (Collett and Barmpaliou 2021). Cyber Diplomacy Capacity Building has therefore

[11] See for more: Oxford Global Cybersecurity Capacity Centre. 2021. "Cybersecurity Capacity Maturity Model for Nations." University of Oxford.

[12] See for more details: ITU. 2024. "Global Cybersecurity Index 2020." Geneva: International Telecommunication Union.

[13] European Commission. 2018. Operational Guidance for the EUs International Cooperation on Cyber Capacity Building. EU Institute for Security Studies. Brussels: European Commission.

[14] See more details about the evolution of the UNGGE on the "Developments in the field of information and telecommunications in the context of international security" here: https://disarmament.unoda.org/ict-security/

[15] List of statements available: https://disarmament.unoda.org/open-ended-working-group/

emerged as a critical aspect of the CCB framework, a priority that has been translated into investments, support, training, and fellowship programs (see, for example, the 'CyberDirect Fellowship Program', the 'Women and International Security in Cyberspace Fellowship', the EU CyberNet's training initiatives, and the Tallinn Summer School of Cyber Diplomacy, and the broader mission of the Global Forum on Cyber Expertise (GFCE). Although we are still far from bridging inequalities in cyber diplomacy, the more even distribution of statements regularly delivered in the context of the new UN OEWG cycle of negotiations (2021-2025) shows some positive progress.

4. CCB for Enhancing Domestic Accountability

Due to their multilateral nature that are clustered around states' negotiating capacity, international organizations often do not sufficiently take into account the role of non-governamental actors, missing the opportunity to fully implement accountability in global politics (Koenig-Archibugi 2010). As a result, the lack of legitimacy of some international organizations has pushed the debate toward the role of industry and civil society organizations in supporting accountability efforts (Scholte 2004). The relevance of implementing domestic accountability derives from the need to overcome this limitation and better reflect the concept of accountability in transnational governance.

Specifically in the cybersecurity domain where, as already emphasized, states do not own and control most aspects of connectivity, the lack of legitimacy of delegations to intervene in international negotiations concerning norms and accountability processes in the cybersecurity domain is even more evident. Notably, the protection of the cyber domain is a responsibility that states share with industry and civil society organizations. This means that states' representatives can better strengthen their accountability vis-a-vis transnational governance approaches to cybersecurity if domestic accountability mechanisms are in place too. Cyber Capacity Building is therefore also required to enhance other actors' capacity to engage in cybersecurity issues to strengthen domestic accountability, as suggested by Slaughter (2004).

CCB initiatives for enhancing domestic accountability usually consist of formalizing clear lines of dialogue between states and other stakeholders, notably those responsible for the functioning of the internet, including industry and civil society organizations. It is pivotal that CCB initiatives enhance effective inclusive governance models, fostering dialogue among these parties and ensuring a fruitful exchange of information to provide a comprehensive overview of the national cybersecurity framework. Through these mechanisms, delegations acting in international cooperation platforms can better represent domestic positions in international dialogues and have a full understanding of national cybersecurity frameworks. The formalization of these mechanisms, including the establishment of national public-private partnerships, the design of legislation ensuring efficient information sharing among parties, and the implementation of dedicated training and educational programs in cybersecurity, are some of the initiatives that are usually foreseen to enhance the government's capacity to engage domestically with non-governmental actors. However, to ensure their efficacy, it is critical that the actors invited to engage in these dialogues also have the capacity to do so. This condition should not be taken for granted, especially considering the cyber capacity inequalities across regions and countries worldwide.

To strengthen domestic accountability, CCB strategies should play a critical role in empowering actors beyond states to engage critically with cybersecurity-related issues. This can be achieved by increasing the number of CCB initiatives that bypass states as

the main beneficiaries and are specifically tailored for local civil society and industry, including human rights organizations, local industries, and telecom operators. When these actors, beyond the state, develop their CCB, countries will not only strengthen their cyber capacity to better reflect the distribution of responsibilities in the national cybersecurity framework but also enhance their accountability domestically and, consequently, externally.

5. Conclusion

Accountability in cybersecurity can be achieved when all actors engaged in a transnational governance approach to cybersecurity are, first, equally capable of negotiating the norms to which they must be accountable. Second, they must have the capacity to be accountable both externally and domestically. These conditions can be achieved by strengthening cyber capacity. Over the past few years, CCB efforts have been implemented for this purpose. However, state actors have consistently been perceived as the main responsible parties for ensuring these conditions and implementing these mechanisms. Consequently, state actors have been the primary beneficiaries of cyber capacity building support.

In order to better reflect the role of accountability in cybersecurity, this approach is, however, insufficient. There is a growing need to distribute CCB funds and efforts beyond state actors, directly targeting civil society organizations and industry. This would better support the implementation of domestic accountability mechanisms by enhancing the capacity of non-governamental actors to critically engage in the cybersecurity domain. The multidimensional nature of international cooperation in cybersecurity reflects this variety, and the UN OEWG was established to welcome contributions from non-governamental actors as a crucial aspect of gaining legitimacy and accountability. Otherwise, there is a risk that these initiatives could be perceived as reinforcing hegemonic power structures, potentially leading to the failure of these efforts.

About the author

Andrea Calderaro is Reader/Associate Professor in International Relations at Cardiff University and a Robert Schuman Center for Advanced Studies Fellow at the European University Institute, where he also obtained his PhD in Social and Political Sciences. His research centers on the intersection of International Relations and Technology, with a focus on cybersecurity, cyber diplomacy, transnational governance of emerging technologies, cyber capacity building, and EU Foreign Policy.

His publications include "Internet Diplomacy: Shaping the Global Politics of Cyberspace" (Roman and Littlefield, 2022), and articles in "European Security", "Third World Quarterly", among others. He has conducted research and supported cyber capacity building initiatives in Africa, Asia, the Middle East, and Latin America, and he regularly serves on advisory boards for International Organizations and governments, including the Global Forum of Cyber Expertise (GFCE), the UK FCDO, the European Commission, UNESCO, and the United Nations.

He has held visiting fellowships and worked at the California Institute of Technology (CalTech), Humboldt University, LUISS, University La Sapienza, University of Oslo, and the Fundação Getulio Vargas (FGV) Rio de Janeiro.

About EU Cyber Direct

EU Cyber Direct – EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen rules-based order in cyberspace and build cyber resilient societies. To that aim, we conduct research, support capacity building in partner countries, and promote multistakeholder cooperation. Through research and events, EU Cyber Direct regularly engages in the discussions about the future of international cooperation to fight cybercrime and strengthen criminal justice systems globally.