EU CYBER DIRECT

ACCOUNTABILITY IN CYBERSPACE: THE HOLY GRAIL OF CYBER STABILITY?

Patryk Pawlak

ACCOUNTABILITY IN CYBERSPACE: THE HOLY GRAIL OF CYBER STABILITY?

Patryk Pawlak

March 2024

Suggested citation: Pawlak, Patryk (2024) *Accountability in Cyberspace: The Holy Grail of Cyber Stability?* Policy brief, EU Cyber Direct, March 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: Jason Hawke/Unsplash

Implementing organisations:

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

Funded by the European Union

Contents

KEY TAKE-AWAYS 7
1. INTRODUCTION 8
2. NETWORKED ACCOUNTABILITY IN CYBERSPACE 11
2.1 Who is accountable to whom? 13
2.2 Who is accountable for what? 18
3. DIFFERENT TYPES OF ACCOUNTABILITY 23
3.1 Hierarchical accountability 23
3.2 Supervisory accountability 26
3.3 Electoral accountability 27
3.4 Fiscal accountability 28
3.5 Legal accountability 29
3.6 Market accountability 30
3.7 Participatory accountability 32
3.8 Public reputational accountability 33
4. LAYERS OF ACCOUNTABILITY 35
4.1 Standards 35
4.2 Information 38
4.3 Monitoring and verification 40
4.4 Sanctions 40
5. CYBER ACCOUNTABILITY ACROSS POLICY REGIMES 44
5.1 International security: the case of the UNSC 44
5.2 International criminal justice: the case of the International Criminal Court 46
5.3 Trade and investment: the case of investor–state dispute settlement 48
5.4 Development assistance: the case of the World Bank Inspection Panel 49
5.5 Human rights: the case of the European Court of Human Rights 50
5.6 Internet governance: the case of ICANN 52
6. MOVING FORWARD: THREE OPTIONS FOR A CYBER ACCOUNTABILITY SYSTEM 53
6.1 A new accountability mechanism at the UN 53
6.2 A 'whole-of-UN approach' to accountability based on the existing institutions 55
6.3 An accountability system beyond the UN 58
ABOUT THE AUTHOR 61
ABOUT EU CYBER DIRECT 62

Key take-aways

1. The road to accountability in cyberspace is uneven and subject to **two major conceptual roadblocks**. First, the conversation was hijacked by a **state-centric version of accountability**, whereby only governments were accountable to each other. Second, since accountability is directly linked to mechanisms within the international security regime, it has largely **ignored other potential institutional choices within international regimes** such as human rights, criminal justice, international trade and internet governance.

2. The question of accountability is ultimately about **attributing responsibility**. Given the multi-stakeholder nature of governance in cyberspace, this paper **abandons the unitary and state-centric approaches** that treat 'the state' and 'the government' as black boxes and the sole units of accountability in cyberspace. Without **a complex and holistic approach to accountability in cyberspace**, the existing power imbalances – between states or among big tech companies and states – will be exacerbated and accountability deficits more marked.

3. Opening the black box of state brings to the fore a more suitable concept of a **networked accountability** involving multiple relationships, capacities, tools and mechanisms that different groups of stakeholders bring to the accountability table. To better grasp the complexity of the accountability debates, the paper also introduces the concepts of **primary and secondary accountability holders, negative and positive accountability,** as well as **anticipatory and material accountability**.

4. All types of accountability **share four features**: standards; information; monitoring and verification; and sanctions. There must be some provision for interrogation as to whether an actor upholds certain agreed **standards**; access to **information** that allows others to verify the claims of compliance or violation of the agreed standards; **monitoring and verification**, which play an important role in verifying whether the available information is accurate; and some means by which the accountability holder can impose **sanctions**.

5. In light of the upcoming negotiations of the Pact for the Future and the Global Digital Compact, the paper presents **three potential non-exclusionary solutions to strengthen the pursuit of accountability**: 1) a new mechanism under the UN umbrella, 2) a 'whole-of-UN' approach based on the existing institutions within the UN system, and 3) an accountability system beyond the UN.

1. Introduction[1]

> *'As responsible states that uphold the international rules-based order, we recognize our role in safeguarding the benefits of a free, open, and secure cyberspace for future generations. When necessary, we will work together on a voluntary basis to hold states accountable when they act contrary to this framework, including by taking measures that are transparent and consistent with international law. There must be consequences for bad behavior in cyberspace. We call on all states to support the evolving framework and to join with us to ensure greater accountability and stability in cyberspace.'*[2]

The pursual of accountability in cyberspace is a story of the Holy Grail eagerly searched for *by* the international cyber-policy community. Accountability – narrowly understood by the cyber elites as the capacity to impose consequences on actors for their malicious and/or illegal behaviour in cyberspace – is seen as a potentially strong deterrent. But the limited effects of the current practices – such as joint attribution statements or targeted sanctions – have raised questions about whether anyone at all is held accountable and to what effect.

Accountability as a goal of cyber diplomacy is on the lips of many policymakers but almost entirely absent from the hundreds of pages of statements delivered by government representatives in different international settings, including the United Nations and the G7. While states reference the UN framework of responsible state behaviour (FRSB), any explicit mentions of accountability are banished from the consensus reports – including the annual progress reports – produced by the UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG).[3] By contrast, government officials are more outspoken and comfortable with referring to accountability in informal discussions and conversations outside of the UN chambers. This is not surprising if one considers the voluntary and non-binding nature of norms and principles in cyberspace, except for those resulting from international law.

The overemphasis on attribution and sanctions as the key elements of accountability has further excluded from the conversation about accountability countries in the Global South, whose capacities in these two areas are less advanced or who take different view

[1] The author would like to thank Allison Pytlak, Xymena Kurowska and Dennis Broeders for their comments on earlier versions of this paper. Any mistakes and omissions are those of the author alone.

[2] US Department of State. *Joint Statement on Advancing Responsible State Behavior in Cyberspace* signed by Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom and the United States. 23 September 2019.

[3] The OEWG report mentions accountability only once, in reference to accountability of the cyber capacity-building initiatives.

on the use of tools such as 'unilateral coercive measures'. This de facto contributed to alienating the broader international community sensitive to power imbalances within world politics and the application of double standards in terms of holding the powerful states accountable.

This paper aims to address some of the weaknesses in the debates about accountability in cyberspace with the primary aim of proposing a system approach to accountability and a potential solution to the accountability deficit in cyberspace. The paper focuses on the following questions:

1. Who are accountable to whom in cyberspace, and for what?
2. How do standards, information, monitoring and participation, and sanctions impact accountability in cyberspace?
3. What processes exist in other cyber-related regimes that could strengthen cyber accountability?

While the problem of accountability has been extensively explored in relation to domestic and international policymaking[4], the debates about accountability in cyberspace remain atheoretical and ignore the richness of those explorations. This paper builds on Keohane's concept of the accountability system, defined as 'the set of accountability mechanisms, and their interactions that characterise a given governance system, from the relationship between the electorate (if any) to the highest political officials, all the way to the relationship between a working-level bureau and its clients'.[5]

The question of accountability is ultimately about attributing responsibility. Given the multi-stakeholder nature of governance in cyberspace, this paper abandons the unitary and state-centric approaches that treat 'the state' and 'the government' as black boxes and the sole units of accountability in cyberspace. This allows for a more holistic approach to accountability in cyberspace whereby accountability claims and politics exist between different actors and at different levels, including individuals, companies, international and regional organisations, and specialised agencies within the UN system.[6] **Without a complex and holistic approach to accountability in cyberspace, the existing power imbalances – between states or among big tech companies and states – will be exacerbated and accountability deficits more marked.** Therefore, the

[4] Mark Bovens, Robert Goodin and Thomas Schillemans (eds.) (2014) *The Oxford Handbook of Public Accountability*, Oxford University Press. Available at: https://academic.oup.com/edited-volume/28191; Mathias Koenig-Archibugi (2010) "Accountability in transnational relations: how distinctive is it?", *West European Politics* 33(5): 1142-64. Available at: https://doi.org/10.1080/01402382.2010.486142.

[5] Robert O. Keohane (2003) "The concept of accountability in world politics and the use of force", *Michigan Journal of International Law* 24(4): 1121–41: 1127. Available at: https://repository.law.umich.edu/mjil/vol24/iss4/9.

[6] See for instance: Robert Wolfe (2015) "An anatomy of accountability at the WTO", *Global Policy* 6(1): 13-23. Available at: https://doi.org/10.1111/1758-5899.12160; Ngaire Woods and Amrita Narlikar (2001) "Governance and the limits of accountability: the WTO, the IMF, and the World Bank", *International Social Science Journal* 53(170): 569-83. Available at: https://doi.org/10.1111/1468-2451.00345.

way forward is not to ignore the questions around accountability in cyberspace but rather to study more rigorously how accountability relationships clash with each other.

A system approach views accountability as a mechanism that allows for a more comprehensive and effective discussion about who is responsible for what and to whom in cyberspace, according to whose standards and with what potential sanctioning mechanisms in place. The observations presented in this paper are based on analysis of the official documents (e.g. submissions and positions expressed by stakeholders at the UN OEWG), participant observation in various international debates (including at the UN) and analysis of secondary sources.

Finally, as this paper argues, the discussion about accountability at the UN does not need to involve conversation about attribution. On the contrary, by avoiding the 'attribution curse' altogether, there are multiple options for the UN to add value in the ongoing efforts to strengthen accountability in cyberspace.

2. Networked accountability in cyberspace

The road to accountability in cyberspace is uneven and subject to two major conceptual roadblocks. First, since the issue was introduced in the UN General Assembly (UNGA) First Committee on Disarmament, the conversation was hijacked by a state-centric version of accountability, whereby only governments were accountable to each other. However, as the past 20 years have proved, such a view is too limiting as it underestimates an important role that the private sector and civil society organisations play in the process. Although deliberations of the OEWG have been opened to non-state actors through formal accreditations and informal consultations, these decisions were motivated not by a desire for more accountability but rather by a more calculated aspiration for creating issue-based alliances with non-governmental groups.

The state-centric approach to accountability leads to another problem. Since accountability is directly linked to mechanisms within the international security regime, it has largely ignored other potential institutional choices within international regimes such as human rights, criminal justice, international trade and internet governance. This is unfortunate given the more advanced maturity of those regimes and well-established mechanisms for norms enforcement they developed over time, for instance the World Trade Organization (WTO) Dispute Resolution Mechanism or the Human Rights Council.

As in the policy debates, the tone of the research about accountability in cyberspace has been set by scholars interested primarily in the international security dimension, with the questions of attribution,[7] responsibility[8] and potential consequences for actors violating agreed norms and international law at its core.[9] Surprisingly, these discussions – perhaps with the exception of the legal scholarship – have remained largely atheoretical and detached from the existing scholarship on accountability across disciplines, including international relations, internet governance and public administration. For instance, very little has been written about the performative practices of states holding other states accountable and their own compliance with the agreed standards of responsible state behaviour in cyberspace.

The question of accountability has been explored in international relations scholarship, which provides insights into its definition and key elements. Although some authors have

[7] Rebecca Crootof (2018) "International cybertorts: expanding state accountability in cyberspace", *Cornell Law Review* 103(3). Available at: https://scholarship.law.cornell.edu/clr/vol10 3/iss3/2; Andreas Kuehn, Debra Decker and Kathryn Rauhut (2023) "Whodunit in cyberspace: the rocky road from attribution to accountability", Issue Brief, *Stimson*, 12 December 2023. Available at: https://www.stimson.org/2023/whodunit-in-cyberspace-from-attribution-to-accountability/.

[8] Russell Buchan and Nicholas Tsagourias (2016) "Special Issue: Non-state actors and responsibility in cyberspace: state responsibility, individual criminal responsibility and issues of evidence", *Journal of Conflict & Security Law* 21(3): 377–81. Available at: https://scholarship.law.cornell.edu/clr/vol103/iss3/2; Antoni Coco and Talita de Souza Dias (2021) "'Cyber due diligence': a patchwork of protective obligations in international law", *European Journal of International Law* 32(3): 771–806. See also Francois Delerue (2020) *Cyber operations and international law*, Cambridge: Cambridge University Press.

[9] James A. Lewis (2022) *Creating accountability for global cyber norms*, Washington, DC: Center for Strategic and International Studies.

questioned the utility of this concept at a global level in the absence of a global public[10] or given the undemocratic nature of international organisations,[11] others have stressed the urgency to find 'innovative ways to hold the abusers of power, at a global level, to account'.[12] This paper builds on the work of Robert Keohane and conceptualises accountability, providing a particularly useful framework to unpack the concept of accountability beyond inter-state relations.

Opening the black box of state brings to the fore a more suitable concept of a networked accountability involving multiple relationships, capacities, tools and mechanisms that different groups of stakeholders bring to the accountability table. Building on Keohane's work, this paper defines accountability as a 'power relationship' whereby a person, an organisation or a state (power-wielders) is accountable to someone else (accountability holders), i.e. there is another person, organisation, state that can constrain the powers and decisions of the former.[13] As argued by Keohane, 'a relationship of accountability can only exist if the accountability holder can exercise some degree of influence over the power-wielder'.[14] Consequently, accountability 'implies that some actors have the right to hold other actors to a set of standards, to judge whether they have fulfilled their responsibilities in light of these standards, and to impose sanctions if they determine that these responsibilities have not been met'.[15]

Recognising that the cyberspace governance regime is becoming increasingly dense and complex,[16] this paper adapts Keohane's accountability system[17] to better reflect organisational overlaps and supplement existing notions and mechanisms of accountability with an additional way of achieving accountability.[18] It does so in two ways.

First, to better grasp the complexity of the accountability debates, the paper introduces the concepts of **primary and secondary accountability holders**. Primary accountability holders are those whose role has been directly recognised by power-wielders. In the context of international security, these are mostly the states that can hold other states accountable for violations of norms or international law. It could also be a private sector company recognising the authority of an arbitration body or an external oversight board. However, often the agreed cyber norms create indirect accountability claims from those directly affected by abuses, violations or simply mismanagement. They are secondary

[10] David Held (2004) *Global covenant: the social democratic alternative to the Washington Consensus*, London: Polity Press.
[11] R.A. Dahl (1999) "Can international organizations be democratic? A sceptic's view", in: I. Shapiro and C. Hacker-Cordon (eds), *Democracy's edge*, Cambridge: Cambridge University Press, 19–36.
[12] Robert O. Keohane (2006) "Accountability in world politics", *Scandinavian Political Studies* 29(2): 75–87: 78. Available at: https://doi.org/10.1111/j.1467-9477.2006.00143.x.
[13] According to Keohane, an accountability holder is a person or entity to whom someone else or another entity is accountable. A power-wielder is a person or entity that gives another person or entity the right to hold them accountable.
[14] Keohane (2003): 1125.
[15] Ruth W. Grant and Robert O. Keohane (2005) "Accountability and abuses of power in world politics", *American Political Science Review* 99(1): 29–43: 29. Available at: https://doi.org/10.1017/S0003055405051476.
[16] Stephanie Hofmann and Patryk Pawlak (2023) "Governing cyberspace: policy boundary politics across organizations", *Review of International Political Economy* 30(6): 2122–49. Available at: https://doi.org/10.1080/09692290.2023.2249002.
[17] Keohane (2003): 1127.
[18] Mette Eilstrup-Sangiovanni and Stephanie Hofmann (2024) "Accountability in densely institutionalized governance spaces", *Global Policy* 15(1): 103–13. Available at: https://doi.org/10.1111/1758-5899.13345.

accountability holders. For instance, although the norm prohibiting attacks against the critical infrastructure creates the rights of states to hold other states accountable, it also creates a group of secondary accountability holders among the operators of critical infrastructure or the users of the provided services who are affected by a cyberattack. In this scenario, while governments pursue accountability at international level, other entities can do so through domestic courts.

Second, the paper brings to the discussion the notions of **negative and positive accountability** in cyberspace,[19] which allow for broadening the scope of the discussion about accountability. Despite the general recognition that different groups of stakeholders (i.e. the private sector, civil society) are responsible for maintaining an open, free, safe and secure cyberspace, the state-centric and security-driven approaches to accountability have excluded from the discussion the need to hold all stakeholders accountable. While negative accountability focuses on the actors who undertake malicious or illegal activities, positive accountability looks at unintended adverse effects of actions by the private sector, civil society, development agencies and others, who may negatively impact citizens and businesses by changing the power structures in another country or weakening checks and balances. Such actions are not part of the current debates about accountability in cyberspace.

The following sections look at two key questions in the discussion about accountability: who is accountable to whom, and for what?

2.1 Who is accountable to whom?

Identifying who is accountable (power-wielders) to whom (accountability holders) is critical for advancing the implementation of a framework for responsible state behaviour in cyberspace and promoting broader accountability. The early dominance of the concept of deterrence in policy and academic debates about international security of cyberspace has set the direction for cyber diplomacy focused largely on states, leading to the emergence of national policies built on the concepts of deterrence by punishment and deterrence by denial.[20] Recently, this debate has been accompanied by new approaches to 'responsibility in cyberspace' with the emergence of new policies such as

[19] Patryk Pawlak (2024) "The pursuit of positive accountability in the cyber domain", *Global Policy* 15(1): 142–8. Available at: https://doi.org/10.1111/1758-5899.13302.

[20] See, for instance, Tim Stevens (2012) "A cyberwar of ideas? Deterrence and norms in cyberspace", *Contemporary Security Policy* 33(1): 148–70. Available at: https://doi.org/10.1080/13523260.2012.659597; Joseph S. Nye (2016) "Deterrence and dissuasion in cyberspace", *International Security* 41(3): 4–71. Available at: doi:10.1162/ISEC_a_00266; Chris Painter (2018) *Deterrence in cyberspace*, Canberra: Australian Strategic Policy Institute. Available at: https://www.aspi.org.au/report/deterrence-cyberspace; Maria Mälksoo (2021) "Ritual reverence to deterrence in cyberspace", *Directions Blog*, 15 February 2021. Available at: https://directionsblog.eu/ritual-reverence-to-deterrence-in-cyberspace/; Jacquelyn G. Schneider (2019) "*Deterrence in and through cyberspace*", in: Jon R. Lindsay and Erik Gartzke (eds), *Cross-domain deterrence: strategy in an era of complexity*, Oxford: Oxford University Press: 95–120.

'active cyber defence' and the increasing focus on accountability of states with confirmed offensive capabilities, such as the United States, the United Kingdom, China and Russia.[21]

In recent years, the accountability of states has been strengthened through changes in the formats of the UN discussions about stability in cyberspace. The expansion of membership within the UN Group of Governmental Experts and the subsequent transition from the GGE to the OEWG as the primary platform for deliberation about cyber affairs in the context of international security were important moves to end the Western monopoly on accountability in cyberspace and bring new voices to the discussion. 'Disadvantaged' actors – especially those from the Global South – may in time seek to alter or overturn the existing arrangements, if they consider they have sufficient political resources. The growing focus on cyber capacity-building (CCB) as an important enabler for the implementation of the FRSB is just one example. Similarly, the proposal by Russia for a new cyber treaty is a clear example of an effort to establish new power relations that significantly strengthen state sovereignty and focus the discussion about accountability on its traditional dimension of inter-state relations. A new legally binding instrument – Russia argues – is the only way to ensure 'more effective global implementation of commitments and a stronger basis for holding actors accountable for their actions'.[22]

Anticipatory and material approaches to accountability

How do states hold each other accountable and strengthen accountability? **'Deterrence by punishment' approaches emerged as one of the mechanisms for what could be described as anticipatory accountability**. They are constructed on the assumption that a credible threat of serious consequences imposed on a state conducting or linked to cyber operations would prevent that state from engaging in such activities out of the fear of being held accountable. This is different from material accountability, whereby states are de facto held accountable for their committed actions. The two concepts are very closely linked in that an effective anticipatory accountability benefits from or is undermined by how strong the material accountability measures are. The weakness and limited impact of material accountability measures on states' behaviour has been one of the key reasons for criticism of the existing approaches and why deterrence measures do not necessarily work. The sceptics argue that tools such as naming and shaming, collective attribution statements, targeted sanctions or offensive cyber operations rooted

[21] See for instance Max Smeets (2022) "Going the extra mile: what it takes to be a responsible cyber power", *Lawfare*, 11 May 2022. Available at: https://www.lawfaremedia.org/article/going-extra-mile-what-it-takes-be-responsible-cyber-power; Marcus Willett (2023) "Offensive cyber and the responsible use of cyber power", *Online Analysis*, IISS, 2 March. Available at: https://www.iiss.org/sv/online-analysis/online-analysis/2023/03/offensive-cyber-and-the-responsible-use-of-cyber-power/; Sven Herpig (2023) "Active cyber defence: toward operational norms", *Policy Brief SNV*, 21 November. Available at: https://www.stiftung-nv.de/de/publikation/active-cyber-defense-toward-operational-norms.

[22] United Nations (2020) *Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*: 5.

in defence forward and persistent engagement have very limited (if any) impact on state behaviour.[23] For instance, tools such as sanctions suffer from limited enforcement and have hardly any impact on individuals or entities whose activities are located exclusively in the territory of another state.

There are also numerous legal questions regarding state responsibility in the case of cyber operations, which complicate the use of tools with the potential to inflict more harm on the aggressors and influence their calculation, in particular the use of countermeasures. The insistence of Russia, China and other states on principles of state sovereignty and non-interference – including by calling into question the applicability of international humanitarian law in cyberspace – offers another example of how states attempt to avoid accountability for their actions in cyberspace.

Primary and secondary accountability of states

'Deterrence by denial' is another approach that emerged in response to increasing malicious cyber operations. Unlike 'deterrence by punishment', this approach focuses on strengthening one's own cyber resilience and building capabilities to increase the costs for the perpetrators of malicious attacks by making them more resource-intense. This implies improving threat analysis, detection and response capabilities by strengthening institutions, legal frameworks and human capabilities. The FRSB includes several positive obligations on states; however, their non-binding and voluntary nature means that they are often forgotten in discussions about accountability.

The primarily intra-state nature of cyber resilience and domestic capabilities initiatives, in combination with the focus on inter-state relations, means that accountability in the context of cyber resilience and capacity-building is often overlooked. There are several reasons why this neglect is relevant. In the context of inter-state relations, even though most attention goes to state responsibility for malicious actions, a state is also accountable for its negligence or failure to prevent undesired – but not necessarily malicious – cyber incidents with negative cascading effects beyond that state's own borders. In such cases, states are accountable to other states and their citizens based on the international rules regarding state liability. Similarly, the principle of due diligence obliges the states to do everything in their power to prevent undesired events from happening and to meet their international commitments. For instance, a state that fails to adopt adequate regulatory frameworks to counter cybercrime or establish basic institutional capabilities or standards aimed at preventing cyberattacks may be held accountable by other states or in some cases even by their citizens.[24] Finally, positive obligations that states undertake through international norms or domestic legislation

[23] Lewis (2022).

[24] Environmental law might offer inspiration to that effect. See for instance Pau de Vilchez and Annalisa Savaresi (2023) "The right to a healthy environment and climate litigation: a game changer?", *Yearbook of international environmental law* 32(1): 3–19.

make this state accountable to its own citizens, for whose safety and security governments are responsible. For instance, electoral processes give citizens the right to oust from power politicians and parties who fail to enact legislation or put in place an adequate institutional framework that protects them against cybercrime.

Primary and secondary accountability of non-state actors

The attention to cyber resilience opens the conversation about accountability in cyberspace to new groups of power-wielders, including international organisations, the private sector and the non-governmental organisations (NGOs).[25] All of them play an important role in influencing the international cybersecurity environment and shaping cyberspace.

The increasingly complex institutional environment in cyberspace comprising regional and international organisations with competences spanning diverse cyber-related policy areas such as trade (WTO, Organisation for Economic Cooperation and Development (OECD)), standards (International Telecommunication Union (ITU)) and crime (Council of Europe, Interpol) implies that those organisations play a role in holding their members accountable. For instance, WTO Dispute Settlement Body can create standards and strengthen accountability of states abusing the WTO security exception.[26] The Council of Europe, acting through its Council of Ministers, can decide to exclude a country from the organisation for violations of its statute. At the same time, regional and international organisations are also power-wielders. Although international relations scholars have researched various dimensions of accountability of international organisations.[27] There is very little scholarship that discusses this topic in the context of cyberspace and internet governance.[28] In addition, while multilateral institutions are supposed to help states hold each other accountable, they are usually ill-equipped to deal with abuses of power by the extremely powerful states that refuse to accept accountability, which undermines the global governance system amid accusations of double standards.[29]

Accountability of large multinational corporations in cyberspace is another critical aspect given the influence that those companies have on government policies and societies by

---

[25] See Jan Aart Scholte (2011) "Global governance, accountability and civil society", in: J.A. Scholte (ed.), *Building global democracy? Civil society and accountable global governance*, Cambridge: Cambridge University Press: 8–41.
[26] Wesley A. Cann (2001) "Creating standards and accountability for the use of the WTO security exception: reducing the role of power-based relations and establishing a new balance between sovereignty and multilateralism", *Yale Journal of International Law* 26(2): 413-86.
[27] See Jan Klabbers (2013) "Unity, diversity, accountability: the ambivalent concept of international organization", *Melbourne Journal of International Law* 14(1): 149–70. Available at: https://law.unimelb.edu.au/__data/assets/pdf_file/0006/1687443/06Klabbers1.pdf; Kristen E. Boon and Frédéric Mégret (2019) "New approaches to the accountability of international organizations", *International Organizations Law Review*, 16(2019): 1–10. Available at: https://brill.com/view/journals/iolr/16/1/article-p1_1.xml?language=en.
[28] For notable exceptions, see Jonathan G.S. Koppell (2005) "Pathologies of accountability: ICANN and the challenge of 'multiple accountabilities disorder'", *Public Administration Review* 65(1): 94–108. Available at: https://www.jstor.org/stable/3542585; Hortense Jongen and Jan Aart Scholte (2021) "Legitimacy in multistakeholder global governance at ICANN", *Global Governance* 27(2): 298–324. Available at: https://doi:10.1163/19426720-02702004.
[29] Keohane (2006).

shaping their preferences and behaviour. While internally accountable to their shareholders, private companies are not always subjected to scrutiny by governments or their peers,[30] who may not have similar resources (especially legal or financial) to pursue accountability. This is where the role of powerful regulators comes into play. For instance, the decisions by numerous governments to remove or block Chinese and Russian technology providers from their infrastructure is an accountability measure towards companies whose practices and actions are considered to pose significant risk. Similarly, regulators can use financial mechanisms such as fines against companies that fail to meet their legal obligations or voluntary commitments. The European Union's Digital Services Act (DSA) and General Data Protection Regulation (GDPR) both foresee fines on companies and entities that do not comply with the EU law to fight disinformation or strengthen data protection. Finally, certain efforts to pursue accountability were made through self-regulation. For instance, Siemens' Charter of Trust, Huawei's Cyber Security Transparency Centre and Kaspersky's Global Transparency Initiative all aimed at improving transparency around their practices, which would allow their users to assess their policies and make informed choices regarding the relationship they wish to establish. At the same time, close trade – and political – links between companies such as Microsoft, Huawei and Kaspersky and governments have led to increasing use of those companies as means for external accountability for other governments (e.g. bans on Huawei and Kaspersky products in the US and Europe).

Significant power imbalances among states, and the presence of influential multinational corporations with turnovers higher than national budgets, highlight the importance of non-governmental groups and civil society organisations in addressing accountability deficits. This role is clearly recognised by governments and international organisations, which increasingly open their deliberations to inputs – and oversight – from the civil society organisations. However, it might sometimes be contentious, as the controversy over the accreditation mechanisms to the OEWG and Ad Hoc Committee on cybercrime have demonstrated.

Civil society organisations have been particularly active in the field of human rights online. For years, the #KeepItOn campaign by Access Now has been raising awareness about the abuses and lack of accountability for internet shutdowns by governments. However, despite clearly identified responsibility for internet shutdowns and the overall agreement that such decisions undermine the open and free nature of cyberspace, there have been hardly any efforts to hold the states in question accountable. Similarly, Citizens Lab – in cooperation with different coalitions of actors – has exposed numerous violations of the existing norms and laws regulating the online environment. The most publicised recent investigation was on the use of commercial spyware Pegasus by governments across the world for surveillance of political opponents, journalists and human rights

[30] Admittedly, this is slowly changing, but within the context of domestic regulation more than international governance. For instance, the EU's Code of Conduct against Disinformation has become a valuable tool in strengthening peer accountability.

activists. The investigation resulted in an extensive audit at the European Parliament[31] and subsequently in the launch of a new Franco-British political initiative, the Pall Mall Process.[32]

2.2 Who is accountable for what?

The question 'who is accountable?' goes hand in hand with the question 'accountable for what?'. Most discussions focus on accountability of state actors for malicious or illegal activities in cyberspace that violate the agreed norms of responsible state behaviour or the existing international law.[33] At their centre is attention to the instruments and mechanisms that states and international organisations have at their disposal to discipline misbehaving states, and their effectiveness. This resulted in a much stronger focus on the application of existing international law – with emphasis on state responsibility and liability for malicious activities in cyberspace[34] – and compliance with the 11 norms proposed under the UN FRSB. What has received less attention is the accountability of different groups of stakeholders for activities that are not necessarily malicious or illegal but nonetheless may impact negatively on other countries, businesses or citizens. These two types of accountability are referred to as negative and positive accountability respectively.[35]

Negative accountability of states

The negative accountability debate is driven by two broad considerations grounded in the framework for responsible state behaviour in cyberspace: application of the existing law in cyberspace and compliance with the agreed norms, rules and principles. Each of them presents certain challenges. Regarding international law, although the international community has agreed that international law applies in cyberspace,[36] there is still no universal agreement on *how* the existing law applies. Although several states have published their national positions on the application of the existing international law,[37] such statements are still scarce. The provisions of international law are also seldom recalled in the statements issued by governments in relation to malicious cyber activities, raising questions about the

[31] See https://www.europarl.europa.eu/committees/en/pega/documents/latest-documents.
[32] See https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of.
[33] Chris Carpenter and Duncan Hollis (2023) "A victim's perspective on international law in cyberspace", *Lawfare*, 28 August. Available at: https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace.
[34] Rebecca Crootof (2018) "International cybertorts: expanding state accountability in cyberspace", *Cornell Law Review* 103(3), March. Available at: https://scholarship.law.cornell.edu/clr/vol103/iss3/2.
[35] Pawlak (2024).
[36] UN OEWG report.
[37] NATO Cooperative Cyber Defence Centre of Excellence (2024) *International law in practice: interactive toolkit*. Available at: https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

relevance of international law in strengthening accountability. While attribution statements recall the content of the agreed norms and principles, they usually avoid explicit references to the exact norms or international law. Such references are also absent from the decisions about measures of retorsion, including sanctions resulting in asset freezes or travel bans. Nonetheless, those decisions need to specify the reasons for which an individual or entity has been placed on the sanctions list, including the connection to a conducted or intended cyberattack.[38]

The limited application of international law in practice leads to criticism from both the supporters and the opponents of the view that the existing international law provides sufficient guarantees. While the supporters see the limited use of the existing international law to promote accountability as a major weakness, the opponents of this position question the suitability and applicability of the existing law itself. A group led by Russia argues that only a new binding international instrument would provide clear rules for cyberspace and consequently strengthen accountability. During the OEWG session in July 2023, Russia made it clear that it 'does not consider itself bound even by voluntary commitments stemming from those provisions of the report that contradict our legislation and national interests', which seriously undermines the future debate about pursuing accountability in cyberspace.[39] Similarly, while states refer to the catalogue of UN-agreed norms as an overall guidance for what states are allowed and forbidden to do in cyberspace, there are hardly any official declarations that would link states' actions and potential violations of these norms to accountability. Except for the general statement made by a group of like-minded countries in 2019,[40] hardly any references to accountability for the norm violations were made. This is primarily because the agreed norms and principles are non-binding and voluntary in nature and therefore are not supported by any concrete verification, monitoring or reporting mechanisms. The references and focus on the implementation of norms as well as proposals for mechanisms such as a national survey of implementation constitute a creative alternative to a formal monitoring mechanism. The potential of such mechanisms for 'ranking' or 'punishing' states was pointed out by Russia during the OEWG deliberations.[41]

Negative accountability of the private sector

Certain efforts to strengthen accountability in cyberspace have also been undertaken by the private sector and civil society organisations – either by stressing the importance of responsible state behaviour or by proposing specific commitments for their signatories.

[38] Council of the European Union (2023) Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, version dated 29 November 2023. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019D0797-20231129.
[39] United Nations (2023) *Statement by the Russian interagency delegation at the fifth session of the UN Open-Ended Working Group on security of and in the use of ICTs 2021–2025*, 28 July.
[40] See footnote 1.
[41] UN OEWG fifth substantive session, July 2023.

The Cybersecurity Tech Accord commits its over 100 signatories to 'act responsibly, to protect and empower our users and customers' through the implementation of eight specific principles. Although the Tech Accord signatories commit to publishing regular reports on the progress that strengthens transparency of this initiative, these documents hardly provide a mechanism for strengthening accountability: they provide a summary of certain activities rather than a monitoring mechanism for the implementation of specific commitments.[42] Such reports provide little insight into concrete achievements towards protecting 'all users and customers from cyberattacks' or how individual signatories have implemented the commitments made.

Another example of the private sector arrangement is the Charter of Trust – an alliance of the leading global companies and organisations to strengthen cybersecurity through the implementation of 10 concrete principles around security by default, user-centricity or cyber resilience through conformity and certification.[43] Although the Charter does not mention any reporting mechanism, the information about implementation of the principles is illustrated with specific examples provided by individual signatories.[44] Neither the Tech Accord nor the Charter of Trust clarifies what specific mechanisms are used to monitor the progress towards their implementation or how potential violations or non-compliance would be remedied. They do, however, create specific groups of responsibility-wielders (i.e. companies, governments) and accountability holders (i.e. customers, organisations and citizens). A good illustration of initiatives that emerged from the cooperation between private sector actors is a multi-stakeholder blueprint on the cyber-mercenary market presented by a group of actors at the Paris Peace Forum in November 2023.[45]

An important aspect of private sector accountability is security and safety of the products and services that private sector entities put on the market and how those impact their consumers and end-users. Following large-scale attacks like NotPetya, WannaCry, SolarWinds and Log4Shell, the technical and policy community invested in policy solutions for coordinated vulnerability disclosure (CVD) processes that allow the vulnerability finders (e.g. hackers) to share such information with relevant stakeholders such as vendors and ICT infrastructure owners.[46] The case of WannaCry was particularly instructive regarding the obligations of state agencies in terms of sharing information about vulnerabilities they discover as opposed to keeping them secret with the goal of potential weaponisation at a later stage. Microsoft was quick to acknowledge its own responsibility but also pointed a finger at the US government by comparing the leaks of

[42] Cybersecurity Tech Accord website. Available at: https://cybertechaccord.org/.
[43] Charter of Trust website. Available at: https://www.charteroftrust.com/.
[44] Ibid.
[45] Paris Call Working Group on Unpacking the Cyber Mercenaries Phenomenon (2023) *Taming the cyber mercenary market: a multistakeholder blueprint towards increased transparency and cyber stability*, Paris Peace Forum, November. Available at: https://parispeaceforum.org/publications/paris-call-taming-the-cyber-mercenary-market/.
[46] European Union Agency for Cybersecurity (2022) *Coordinated vulnerability disclosure policies in the EU*, 13 April. Available at: https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

exploits from the government to the US military having some of its Tomahawk missiles stolen.[47] Conversely, threat intelligence and cybersecurity experts also point out problems with services and products being released on the market without sufficient testing and consequently creating opportunities for cybercriminals or other malicious actors.[48] In such cases, it is usually the market, through customer choices, that provides an accountability mechanism (i.e. customers choose different products and services). However, recognising that citizens may not always have alternatives and depend on a limited number of providers, governments decided that intervention in the market may be necessary through certification and labelling mechanisms such as the US Cyber Trust Mark[49] or the EU's certification scheme, and specific security and safety measure for hardware and software products with digital elements[50].

Recognising the power of big tech companies, government agencies and politicians are increasingly looking to provide oversight and ensure that those companies are accountable. Following reports of a Chinese espionage campaign against the US government in 2023, the Chairman of the US Senate Committee on Finance, Ron Wyden, sent a letter to the Cybersecurity and Infrastructure Security Agency (CISA), the Attorney General and the Chair of the Federal Trade Commission, requesting them to hold Microsoft 'responsible for its negligent cybersecurity practices'.[51] Another example of government intervention is bans of certain products or services, including Kaspersky, Huawei, ZTE or TikTok, taken by some governments concerned about the role of these companies in facilitating malicious activities by other states. Such interventions into the market are also one of the mechanisms through which governments hold each other accountable.

Positive accountability

Finally, there is the often-neglected case of positive accountability in relation to activities in cyberspace that are neither malicious nor illegal but might have concrete adverse implications for their targets, such as CCB.[52] This form of accountability is particularly relevant in the context of activities undertaken by international or regional organisations

[47] Brad Smith (2017) "The need for urgent collective action to keep people safe online: lessons from last week's cyberattack", *Microsoft on the Issues*, 14 May. Available at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.
[48] Sergiu Gatlan (2023) "Microsoft fixes flaw after being called irresponsible by Tenable CEO", *Bleeping Computer*, 4 August. Available at: https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-flaw-after-being-called-irresponsible-by-tenable-ceo/.
[49] The White House (2023) "Biden-Harris administration announces cybersecurity labeling program for smart devices to protect American consumers", 18 July. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/.
[50] European Commission (2022) *Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020*, COM(2022) 454 final, 15 September. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454.
[51] United States Senate (2023) "A letter from Ron Wyden to Jen Easterly, Merrick B. Garland and Lina Khan regarding Microsoft's negligent cybersecurity practices", 27 July. Available at: https://www.wyden.senate.gov/imo/media/doc/wyden_letter_to_cisa_doj_ftc_re_2023_microsoft_breach.pdf.
[52] Pawlak (2024).

(e.g. World Bank, ITU, Council of Europe) or non-governmental stakeholders in the cyber domain.

The international community operates on the assumption that international CCB initiatives have an overall positive impact and neglects the need for transparency, reporting and sanctions mechanisms in case of adverse effects. However, international relations scholars have pointed out significant problems of a conceptual and methodological nature linked to resilience or capacity-building.[53] CCB initiatives may have a significant impact on the power structure between stakeholders, reshape a legal system that may not be adequate, or create ineffective institutions. Although not explicitly linking it to accountability in cyberspace, the international community has increasingly highlighted the need for a principles-based approach to CCB[54] that is grounded in development cooperation and human rights.[55] The 2021 OEWG report in the CCB section speaks of concrete principles such as the need for the CCB activities to be 'evidence-based, politically neutral, transparent, accountable, and without conditions' and to 'respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory'. However, like in other OEWG areas, such provisions lack clear monitoring and enforcement mechanisms. As a consequence, the principle of accountability remains underdeveloped.[56]

[53] David Chandler (2014) "Beyond neoliberalism: resilience, the new art of governing complexity", *Resilience: International Policies, Practices and Discourses* 2(1): 47–63. Available at: https://doi.org/10.1080/21693293.2013.878544.
[54] Patryk Pawlak and Nayia Barmpaliou (2017) "Politics of cybersecurity capacity building: conundrum and opportunity", *Journal of Cyber Policy* 2(1): 123–44. Available at: https://doi.org/10.1080/23738871.2017.1294610.
[55] 2021 OEWG Final Report, A/75/816, paragraph 56.
[56] Pawlak (2023).

3. Different types of accountability

Due to a rather narrow understanding of who is accountable and for what in cyberspace, the debate about different forms of accountability has overstated the importance of sanctions and their implementation as a necessary condition for accountability. This has led to a rather narrow conceptualisation of accountability in international cyber policies. To broaden the discussion and offer new perspectives, this paper introduces Keohane's **eight types of accountability** (see Figure 1) and adapts them to the cyberspace context.[57] These accountability mechanisms are not in competition with each other but rather overlap and complement each other, contributing to the emergence of a more comprehensive accountability system.

3.1 Hierarchical accountability

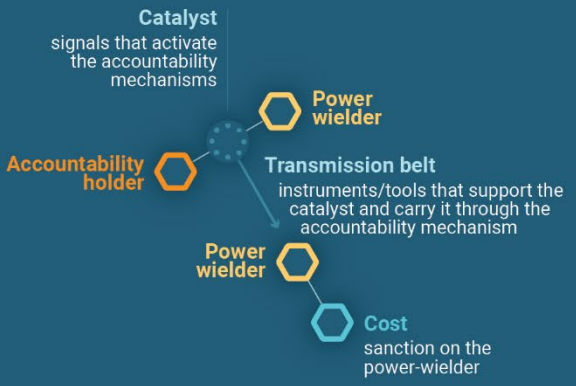
Hierarchical accountability is typical of bureaucracies and large organisations where superiors exercise control over their subordinates. Although it is one of the most straightforward forms of accountability, this type of accountability is ignored in cyber discussions despite the clear impact it might have on cultural change and raising awareness about the importance of cyber standards among the political leadership, across organisations and in the national policymaking and decision-making systems. For instance, individuals in the positions of cyber ambassadors or coordinators, or heads of national cybersecurity agencies or intelligence agencies, are subjected to hierarchical accountability for any decisions or advice they provide. If their decisions violate laws or do not comply with the standards provided by the agreed norms of responsible state behaviour, national and international law or other professional standards established through diplomatic practice, they may be held accountable by their superiors on the basis of the applicable specific or general rules of procedure, staff regulations or professional codes of conduct. In other words, cyber ambassadors, the UN Tech Envoy or the Chair of the OEWG are all accountable to those who appoint them (e.g. Ministers of Foreign Affairs, UN Secretary General, UN General Assembly). For instance, the appointment of Chilean diplomat Fabrizio Hochschild as the UN Tech Envoy was withdrawn by the UN Secretary General after an investigation into his conduct. In the specific cyber context, the chair of the OEWG is accountable to the Secretary General, to whom he is expected to present a report from the deliberations and to the General Assembly on the performance of their mandate, as established by the UNGA resolutions.

[57] Keohane (2003).

Chemistry of accountability

Mechanisms in the cyberspace accountability system

The pursuit of accountability is like a chemical reaction whereby the reactants – power-wielder and accountability holder – are changed resulting in different products. In the context of the accountability discussion, catalysts are signals that activate the accountability mechanisms, transmission belts are instruments/tools that support the catalyst and carry it through the accountability mechanism, and the cost is a sanction on the power-wielder.



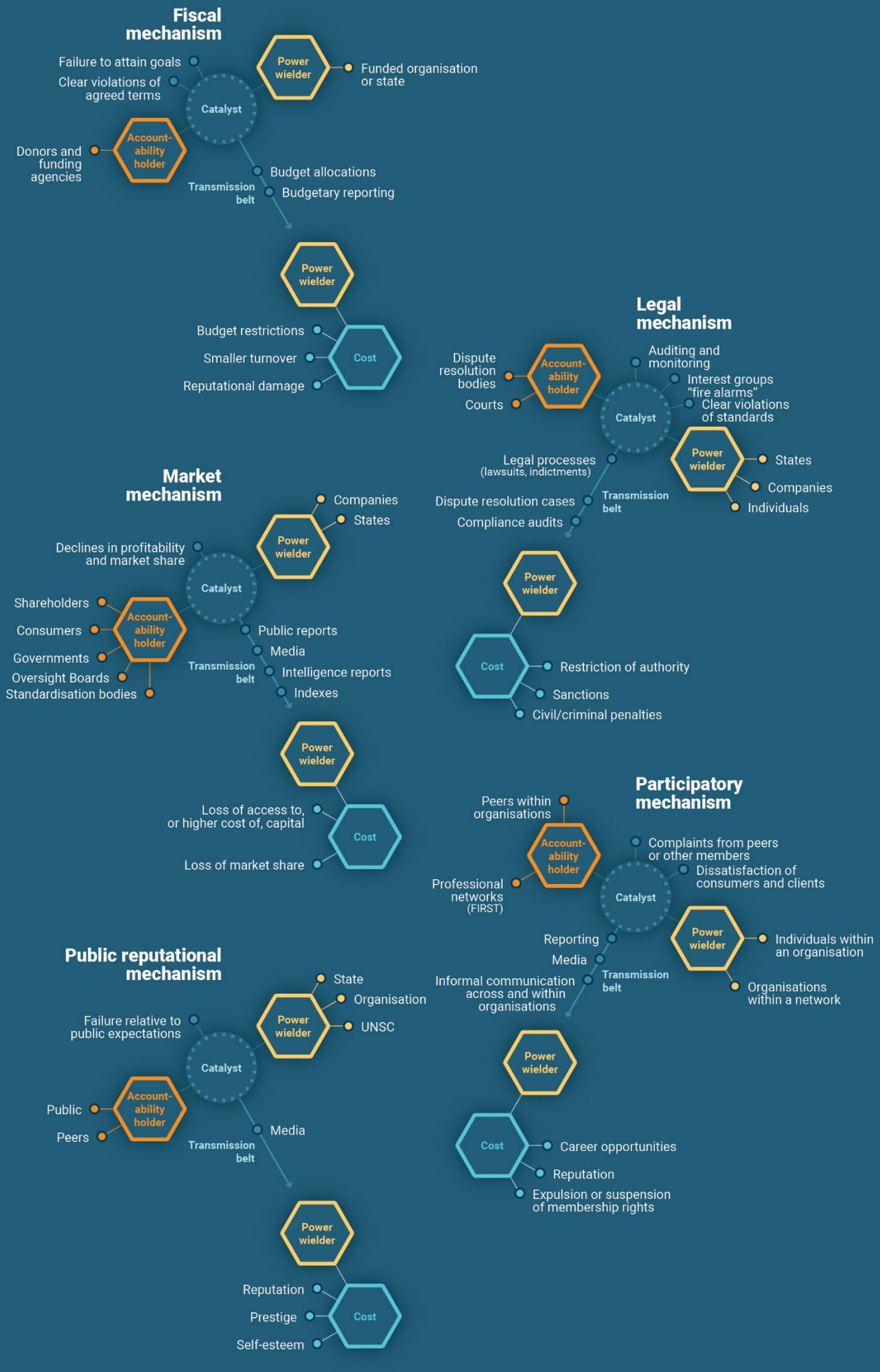

Fiscal mechanism
Failure to attain goals
Clear violations of agreed terms
Power wielder
Funded organisation or state
Catalyst
Account-ability holder
Donors and funding agencies
Budget allocations
Transmission belt
Budgetary reporting
Power wielder
Budget restrictions
Smaller turnover
Reputational damage
Cost
Legal mechanism
Dispute resolution bodies
Courts
Account-ability holder
Auditing and monitoring
Interest groups "fire alarms"
Clear violations of standards
Catalyst
Power wielder
States
Companies
Individuals
Legal processes (lawsuits, indictments)
Dispute resolution cases
Compliance audits
Transmission belt
Power wielder
Cost
Restriction of authority
Sanctions
Civil/criminal penalties
Market mechanism
Companies
States
Power wielder
Declines in profitability and market share
Catalyst
Shareholders
Consumers
Governments
Oversight Boards
Standardisation bodies
Account-ability holder
Public reports
Media
Intelligence reports
Indexes
Transmission belt
Power wielder
Loss of access to, or higher cost of, capital
Loss of market share
Cost
Participatory mechanism
Peers within organisations
Account-ability holder
Professional networks (FIRST)
Complaints from peers or other members
Dissatisfaction of consumers and clients
Catalyst
Power wielder
Individuals within an organisation
Organisations within a network
Reporting
Media
Informal communication across and within organisations
Transmission belt
Power wielder
Cost
Career opportunities
Reputation
Expulsion or suspension of membership rights
Public reputational mechanism
State
Organisation
UNSC
Power wielder
Failure relative to public expectations
Catalyst
Public
Peers
Account-ability holder
Media
Transmission belt
Power wielder
Reputation
Prestige
Self-esteem
Cost

Figure 1 (on pages 24-25): Accountability mechanisms in cyberspace (based on Keohane, 2003)

An important contribution to the discussion about hierarchical accountability comes from the United Kingdom, whose National Cyber Strategy 2022 introduced the concept of responsible cyber power, with very concrete accountability mechanisms. For instance, the activities of the UK's National Cyber Force (NCF) are subject to approval by ministers, judicial oversight and parliamentary scrutiny of the Intelligence and Security Committee. The Secretary of State for Foreign, Commonwealth and Development Affairs and the Secretary of State for Defence are jointly accountable for NCF activities. Cyber operations are also subject to review by the Investigatory Powers Commissioner and potentially the Investigatory Powers Tribunal, an independent specialist tribunal with unique statutory powers.[58]

3.2 Supervisory accountability

Supervisory accountability comes into play when a specific group is authorised to act as the accountability holder in respect of specified power-wielders. For instance, in representative democracies the legislative branch exercises control over the executive branch. In the cyber context, member states exercise a supervisory role over the secretariat of regional or international organisations to which they belong or the UN Secretary General exercises this role over specialised agencies such as the UN Office on Drugs and Crime (UNODC) or the UN Institute for Disarmament Research (UNIDIR). The question of supervisory accountability – even though not framed in these terms – plays an important role in the context of international security in cyberspace, where states have been very reluctant to relinquish any power over their national competence or create new bodies that could provide more accountability. For instance, the Microsoft proposal to establish a public/private international body on attribution of cyberattacks and to validate whether norms are being adhered to has received significant pushback from governments.[59]

[58] UK National Cyber Force (2023) *Guidance: Responsible cyber power in practice*, 4 April. Available at: https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html.
[59] Scott Charney (2016) "Cybersecurity norms for nation-states and the global ICT industry", *Microsoft on the Issues*, 23 June. Available at: https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/.

Similar ideas for a new cyber-attribution institution were explored in academic security policy[60] and international law[61] circles. However, calls for independent bodies that might limit states' full control over their national security were rejected, especially regarding attribution where attribution decisions reflect national intelligence assessments and political priorities. The proposal for a new UN convention on ensuring international information security – an initiative spearheaded by Russia – mentions a verification mechanism that would operate under UN auspices 'while respecting the principles of its Charter, including, above all, the sovereign equality of States'.[62] It proposes a permanent body with the participation of all states that join the convention and regular review conferences. In terms of international security, the UN Charter gives the Security Council and General Assembly certain supervisory accountability tools (i.e. resolutions); however, as the experience of past years has demonstrated, their political polarisation has significantly reduced their usefulness.

3.3 Electoral accountability

Electoral accountability is another type of democratic accountability. It is less straightforward in the context of cyber governance. No government has so far lost elections because of its position on cyber issues, and such topics are rarely part of an electoral campaign unless presented as significant for national security or the rule of law. This was the case with the hack against the Democratic National Committee in 2015 and 2016: one of the factors that contributed to Hillary Clinton losing the US presidential election. Press and civil society reports about the government's use of spyware against the political opposition, journalists or civil society organisations have attracted a lot of attention, including investigations by parliamentary bodies such as the European Parliament[63] and the Polish Senate investigation into Pegasus hacking.

This does not mean, however, that politicians are not concerned about the impact that a lack of action or wrong decisions in relation to cyberspace might have on their political standing. Amid growing concerns about Chinese cyber-espionage operations in the US, President Obama raised the issue with his counterparts in Beijing, leading to a short-lived agreement that such attacks would be stopped.

---

[60] Milton Mueller, Karl Grindal, Brenden Kuerbis and Farzaneh Badiei (2019) "Cyber attribution: can a new institution achieve transnational credibility?", *Cyber Defence Review* 4(1): 107–21. Available at: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1830029/cyber-attribution-can-a-new-institution-achieve-transnational-credibility/.

[61] Yuval Shany and Michael N. Schmitt (2020) "An international attribution mechanism for hostile cyber operations", *International Law Studies* 96: 196–222. Available at: https://digital-commons.usnwc.edu/ils/vol96/iss1/8/.

[62] Permanent Mission of the Russian Federation to the UN (2023) *Updated concept of the convention of the United Nations on ensuring international information security*. Available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf.

[63] European Parliament (2023) *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, 23 May. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

Cases of clear electoral accountability for illegal or questionable use of cyberspace, however, are hard to find. Electoral accountability plays an important role also in the case of officials elected to leadership positions in international or regional organisations: for instance the Secretary General of the ITU, who is elected by all members. Similarly, the governing bodies of the Internet Governance Forum are appointed through a broad multi-stakeholder community.

3.4 Fiscal accountability

Fiscal accountability refers to mechanisms that regulate relationships between funders and recipients of funding. In cyberspace, this is particularly relevant in the context of funding for digital infrastructure and CCB. In fact, the only mention of accountability in the 2021 OEWG report relates to CCB.

Fiscal accountability plays out at several levels. First, states, international donor agencies and multinational development banks that provide funding to other actors become accountability holders with relatively straightforward and prescribed monitoring and reporting mechanisms about where and how the money is spent. Should the donors be unsatisfied with the results or the processes, they can deploy various sanctioning mechanisms, including ending the financial support for any violations of the agreed terms.

Second, states that enter into cooperation agreements with international donors where the power arrangement favours those holding the purse, or their citizens, should also be able to hold the donors accountable for any negative effects of their interventions. For instance, citizens who suffer from the abuse of power by a government whose cyber-surveillance capacity was strengthened through an external actor should be able to hold that donor accountable. To reduce any risks from inappropriate use of resources, several organisations have proposed elaborating clear guidance for principles-based approach in a broad development context[64] and in a more specific cyber context. The OECD's Development Assistance Committee (DAC)[65], for instance, adopts concrete standards for the largest providers of aid, including on enabling civil society or good pledging practice[66]. Although not cyber-specific, these standards should be also applicable for the financial support provided in the cyber domain.

Finally, any donor providing assistance to other countries or organisations and using public funding or the budgets provided by the organisation's members or contributors is also accountable for how taxpayers' money is spent. For instance, aid ineffectiveness

[64] Busan Declaration. Available at: https://www.oecd.org/dac/effectiveness/busanpartnership.htm.
[65] Development Assistance Committee (DAC). Available at: https://www.oecd.org/dac/development-assistance-committee/.
[66] DAC standards. Available at: https://www.oecd.org/dac/dac-instruments-and-standards.htm.

and limited results have pushed certain donors to significantly limit their contributions to international cooperation.

3.5 Legal accountability

Legal accountability addresses compliance – or lack thereof – with formal rules and/or specific contractual provisions. The most straightforward example of legal accountability is states' compliance with general international law and other legal commitments undertaken through bilateral and/or multilateral international agreements. Although states agree that the existing international law applies in cyberspace, there are differences in how they interpret specific legal provisions in the context of cyberspace, which in turn may create conflict and complicate the pursuit of accountability. The number of countries that presented their national positions regarding how the existing international law applies in cyberspace is still relatively small. Other than a possible lack of capacity to formulate such positions, this can be explained by the unwillingness of states to subject themselves to any forms of external accountability. This is also the reason why many of the published statements remain vague in their language and commitments.[67]

Critics of the traditional state-to-state approaches to accountability argue that the reluctance of states to rely on the full spectrum of instruments provided by international law and the difficulties in ensuring that such instruments are enforced have significantly weakened accountability in cyberspace. In addition, the reliance on mechanisms such as retorsions and countermeasures is in itself subject to legal accountability. For instance, the Court of Justice of the European Union has set very clear rules regarding the rights of individuals or entities who are subject to the EU's sanctions regime – including cyber sanctions – that if not properly implemented might lead to invalidation of the adopted measures.

This does not mean, however, that courts have remained silent in terms of shaping cyberspace and promoting accountability through jurisprudence. The existing case law in the fields of data protection and the right to privacy suggests that legal accountability of states often involves the need to balance different policy goals, especially the protection of human rights and national security. In early 2024, the European Court of Human Rights issued a judgment in which it disagreed with the approach presented by Russia's Federal Security Service (FSB) that required messaging service Telegram to provide technical information to assist the decryption of a user's communication. The Court found that 'the contested legislation providing for the retention of all internet communications of all users, the security services' direct access to the data stored without

[67] NATO Cooperative Cyber Defence Centre of Excellence (2024) *International law in practice: interactive toolkit*. Available at: https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society'.[68] It remains to be seen whether increasing recognition of the need for protection of human rights online will result in growing involvement of the courts, including the European Court of Human Rights.

In addition, legal accountability is relevant for ensuring that non-state actors such as tech companies, critical infrastructure operators or other relevant entities comply with national laws and international agreed standards. In such cases, the monitoring, reporting and other transparency mechanisms are usually defined by the law and enforced through specific institutions such as the courts, consumer organisations or other designated agencies. Recognising that strengthening cyber resilience requires cooperation across different levels of government and the involvement of different stakeholder groups, governments started adopting regulation that clearly prescribes specific roles and responsibilities of different stakeholders. The enforcement of such measures is ensured through various forms of reporting and sanctioning mechanisms such as fines. For instance, in December 2023 the European Commission opened formal proceedings to assess whether X may have breached the Digital Services Act (DSA) in areas linked to risk management, content moderation, dark patterns, advertising transparency and data access for researchers.[69]

3.6 Market accountability

Various stakeholder groups can exercise influence on others through markets, which creates **market accountability**. This means that through their choices and decisions, governments, customers and end-users can all hold economic actors accountable for their actions. This role can be executed by investors and stakeholders who decide about the direction of the company's evolution by providing funding for investments or loan guarantees, or exercise influence through other mechanisms. In some cases this may also lead to establishment of specific bodies that enhance companies' accountability. For instance, Facebook's Oversight Board was created to help the company ensure the protection of freedom of expression online. The binding nature of the Board's decisions to uphold or reverse Facebook's content decisions means that Facebook has to implement them, unless doing so could violate the law.

Where market mechanisms seem to fail, governments can resort to regulation to intervene in the markets out of security concerns and to mitigate risks associated, for

[68] European Court of Human Rights (2024) *Case of Podchasov v. Russia*, 13 February 2024. Available at: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}.
[69] European Commission (2023) "Commission opens formal proceedings against X under the Digital Services Act", 18 December. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-x-under-digital-services-act.

instance, with the presence in the market of untrustworthy suppliers. Other than introducing specific standards and requirements to enhance security of supply chains or the internet of things, governments have resorted to restricting access to markets on security grounds. For instance, the US and several other Western countries have banned Chinese or Russian companies from their markets on the grounds of potential risks that companies such as Huawei, ZTE or Kaspersky carry for national internet infrastructure and their citizens. The focus on geopolitical competition that these decisions triggered led to new political concepts such as 'decoupling' and 'strategic economy'. Concerns about governments abusing national security exceptions in market access decisions and digital trade[70] have also strengthened the importance of other types of accountability, such as legal accountability through the WTO Dispute Settlement Body.[71] In an attempt to address market failures, governments have also moved to introduce standardisation and labelling schemes as a tool to increase transparency and hold the tech companies accountable. In this context, the role of consumer organisations as accountability holders remains under-explored in the field of cybersecurity.

Market accountability has emerged as a potentially key mechanism to curb the growing market in commercial cyber-surveillance technologies and vulnerabilities.[72] The reports of commercial spyware used by governments against political opposition, journalists and other groups have triggered not only public criticism but also calls for regulatory action[73] to shape the market for such technology, such as export controls.[74] Despite these steps, however, highly sophisticated exploits and mercenary spyware continue to be used against civil society organisations, for example.[75] The risks to societies and international security posed by the proliferation of these technologies[76] have resulted in calls for more concerted effort at the international level. The Pall Mall Process launched by France and the UK in February 2024 aims to establish market accountability mechanisms for irresponsible use of commercial cyber-intrusion capabilities. It lists accountability as one

[70] Henry Gao (2018) "Digital or trade? The contrasting approaches of China and US to digital trade", *Journal of International Economic Law* 21: 297-321; Robert K. Knake (2020) "Weaponizing digital trade. Creating a digital trade zone to promote online freedom and cybersecurity", *Council Special Report* No. 88, Council on Foreign Relations, September 2020.
[71] Susan Ariel Aaronson and Patrick Leblond (2018) "Another digital divide: the rise of data realms and its implications for the WTO", *Journal of International Economic Law* 21: 245-72.
[72] Steven Feldstein and Brian Kot (2023) *Why does the global spyware industry continue to thrive? Trends, explanations, and responses*, Carnegie Endowment for International Peace, 14 March. Available at: https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.
[73] European Parliament (2023) *Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware,* 2022/2077(INI), Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, 22 May. Available at: https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.
[74] *Official Journal of the EU* (2021) "*Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)"*, L 206, 11 June. Available at: https://eur-lex.europa.eu/eli/reg/2021/821/oj.
[75] See for instance the Pegasus archives by The Citizen Lab. Available at: https://citizenlab.ca/tag/pegasus/.
[76] National Cyber Security Centre (2023) *The threat from commercial cyber proliferation*, 19 April. Available at: https://www.ncsc.gov.uk/report/commercial-cyber-proliferation-assessment.

of the pillars to frame our future engagement involving states, industry, civil society and academia representatives.[77]

3.7 Participatory accountability

Participatory accountability emerges through demands for explanation of professional performance or action. This specific type of accountability aims to strengthen accountability within organisations by assigning the role of accountability holders to professional associations, networks or individuals within organisations who can hold others accountable for their actions. In that sense, participatory accountability resembles a peer review mechanism whereby power-wielders are not hierarchically superior to accountability holders. For instance, in 2020 the ICT4Peace Foundation proposed the establishment of a States Cyber Peer Review Mechanism for state-conducted foreign cyber operations to strengthen compliance with the agreed UN norms of responsible state behaviour in cyberspace.[78]

In the cyber domain, where trust-based mechanisms are the foundation for information sharing and cooperation, this type of accountability is particularly relevant and may be effective in promoting and enforcing specific norms, rules and principles of behaviour. For instance, the Forum of Incident Response and Security Teams (FIRST) is a *peer-to-peer network that provides platforms, means and tools for incident responders. In 2020, FIRST published EthicsfIRST*: Ethics for Incident Response and Security Teams, which sets expectations for FIRST teams and provides guidance to incident response teams worldwide. The FIRST Board of Directors can decide to suspend the membership of organisations, but one of the drawbacks of this process is that such decisions are not always dictated by objective factors. For instance, in March 2022 the Board decided to temporarily suspend all member organisations from Russia and Belarus until the full implications of the issued US government sanctions were assessed.[79] Earlier, in 2019, FIRST was also forced to suspend the memberships of Huawei, Duhau and Hikvision in response to changes made to the US Export Administration Regulations (EAR).[80] However, FIRST made it clear that those decisions result more from the need to comply with US laws than from a loss of trust in those companies.

Participatory accountability is also important in the context of the fight against cybercrime, intelligence-sharing or military cooperation, where adherence to strictly

[77] Ministry of Foreign Affairs of France (2024) *The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of.
[78] ICT for Peace Foundation (2020) *"ICT4Peace proposed "States Cyber Peer Review Mechanism" for state-conducted foreign cyber operations"*, 1 March. Available at: https://ict4peace.org/wp-content/uploads/2020/03/ICT4Peace-Proposed-States-Cyber-Peer-Review-3.pdf.
[79] FIRST (2022) "Teams suspension from FIRST", 25 March. Available at: https://www.first.org/newsroom/releases/20220325.
[80] FIRST (2019) "Statement regarding Huawei's suspension from the Forum of Incident Response and Security Teams (FIRST)", 18 September 2019. Available at: https://www.first.org/newsroom/releases/20190918.

defined professional standards (e.g. regarding confidentiality of information, technical standards for information sharing, adherence to the rule of law) is critical for the effectiveness of cooperation. In such cases, any violation of or negligence regarding the agreed rules might result in suspension of cooperation. These standards are often defined in bilateral or multilateral cooperation arrangements. The existence of such standards, monitoring mechanisms and sanctions is particularly important in the context of the private–private partnerships whereby the performance of public functions is sometimes delegated to a private company, which may not be subject to the same rules of transparency or sanctioning as public entities. The case of Microsoft support to the Albanian government following a series of cyberattacks helps to illustrate this point.[81]

Finally, in the specific context of international security, the participation of non-governmental actors in the usually intergovernmental discussions at the UN – whether in the OEWG or the Ad Hoc Committee on Cybercrime – can be considered a mechanism to ensure participatory accountability. The opening of such discussion to participation of civil society organisations and the private sector implies that those organisations become secondary accountability holders in relation to the states. For instance, in the context of the OEWG, some of the submissions by civil society organisations have criticised governments for attacks against healthcare institutions.[82] Organisations such as the ICRC have also pointed out the obligations of states to respect international humanitarian law in cyberspace.[83]

3.8 Public reputational accountability

Public reputational accountability applies to situations in which 'reputation, widely and publicly known, provides a mechanism for accountability even in the absence of other mechanisms'.[84] This includes, among others, international organisations such as the UN Security Council (UNSC), UN Human Rights Council and International Court of Justice. In these cases, external scrutiny from legal scholars and other judges is the primary mechanism for ensuring accountability. With regard to cyber policies, this is particularly relevant in the context of the international standardisation bodies or associations dealing with the technological layer of cyberspace, such as the Internet Engineering Task Force (IETF). In most cases, the origin of these organisations dates back to when the basic aspects of internet infrastructure and functioning were established, and many of them

[81] Microsoft (2022) "Microsoft investigates Iranian attacks against the Albanian government", 8 September. Available at: https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.
[82] CyberPeace Institute (2021) "Online or offline, attacking healthcare is attacking people", 9 March. Available at: https://cyberpeaceinstitute.org/news/online-or-offline-attacking-healthcare-is-attacking-people/.
[83] ICRC (2022) "ICRC statement on International Law in the second session of the OEWG on security of and in the use of information and communications technologies", 1 April. Available at: https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations.
[84] Keohane (2003): 1134.

became public trust institutions. For instance, the Internet Society – an organisation established to support and promote the development of the internet as a global technical infrastructure – was subjected to public reputational accountability when it attempted to sell the '.org' top-level internet domain to the private equity firm Ethos Capital. Access Now together with a group of other NGOs criticised the deal, which in their view did not consider 'the human rights impacts of the business deal' or 'the sale's deleterious effects on the governance of the open and free internet'.[85] Eventually, ICANN – a multistakeholder, internationally organised, non-profit corporation established to provide a technical coordination function – blocked the sale[86] after receiving letters from at least 30 groups opposing it. In fact, ICANN's decision in the case of the .org sale was also influenced by an intervention from the California Attorney General, who recalled the organisation's commitment to work 'for the benefit of the Internet community as a whole'.[87]

[85] Access Now (2019) "Access Now calls on Internet Society to halt the sale of .ORG", 27 November. Available at: https://www.accessnow.org/press-release/access-now-calls-on-icann-and-internet-society-to-halt-the-sale-of-org/.
[86] ICANN (2020) "Approved Board resolutions", Special Meeting of the ICANN Board, 30 April. Available at: https://www.icann.org/en/board-activities-and-meetings/materials/approved-resolutions-special-meeting-of-the-icann-board-30-04-2020-en.
[87] Timothy B. Lee (2020) "ICANN blocks controversial sale of .org domain to a private equity firm", *Ars Technica*, 5 January. Available at: https://arstechnica.com/tech-policy/2020/05/icann-blocks-controversial-sale-of-org-domain-to-a-private-equity-firm/.

4. Layers of accountability

All types of accountability share four features: standards; information; monitoring and verification; and sanctions. There must be some provision for interrogation as to whether an actor upholds certain agreed **standards**; access to **information** that allows others to verify the claims of compliance or violation of the agreed standards; **monitoring and verification**, which play an important role in verifying whether the available information is accurate; and some means by which the accountability holder can impose **sanctions** on the power-wielder. Each of these elements impacts the discussions about accountability in cyberspace and makes it more or less challenging.

Figure 2. Accountability stack across four layers

4.1 Standards

There are several approaches to defining standards for cyberspace, depending on the policy area (e.g. crime, diplomacy, defence, human rights), the policy community concerned (e.g. technical, policy) and the type of stakeholder (e.g. public, private, civil society). Standards are expected to provide an objective reference point within a community. Standards established by the International Organization for Standardization (ISO) are generally recognised as the baseline for network security among the technical community (e.g. ISO 27001). The development community operates with clearly prescribed principles embedded, among others, in the Busan Partnership for Effective

Development Cooperation, which constitute a standard for external assistance. The principles of legality, proportionality and necessity constitute a golden standard in the international fight against cybercrime for law enforcement agencies, legislators and criminal justice actors.

This does not mean, however, that there are no differences in how these principles are interpreted in different regions or countries. In fact, those differences are sometimes the reason why certain countries do not cooperate. In the field of international criminal justice[88] and law enforcement cooperation, differences in interpretation of a proportionate response may result in overcriminalisation of certain acts (e.g. illegal content online) and other states' refusal to cooperate through mutual law enforcement and extradition agreements. There are also no precise standards when it comes to strengthening cyber resilience, since many of those efforts depend on the local context, institutional preferences and numerous other factors. Instead, actors refer to good practices as a proxy for standards. In the context of international security, the discussion about standards is a particularly thorny issue. As mentioned in previous sections, the overall standards are established in the UN FRSB that emerged through deliberations in the UN GGE and UN OEWG. Although the final reports have been approved by the UNGA, the exact content is still subject to interpretation and debate.

Against the background of discussions about norm contestation[89], the UN GGE 2021 report is particularly noteworthy as it provides more extensive discussion of each norm proposed as part of the FRSB.[90] At the macro level, countries such as Russia and China question whether such a 'framework' exists at all and call for a continued discussion and possible development of new norms. The 'framework-believers' call for more focus on consolidating the achievements to date and the implementation of commitments already made. At the micro level, there is an ongoing debate about what specific norms or principles mean in the absence of standards that would allow for their universal interpretation. This is where the connections between the FRSB and other international policy regimes (e.g. human rights, criminal justice, trade) play an important role. For instance, there is no single definition of critical infrastructure, no single institutional model for a computer emergency response team, and no universal procedure for attributing cyberattacks. The 2021 GGE report and the OEWG submissions aimed to further clarify these terms or called for the development of a common vocabulary to facilitate the conversation (e.g. UNIDIR developed a taxonomy of malicious ICT incidents[91]). Countries also use the OEWG discussion to introduce new concepts that would add further nuance to the debates. Egypt, for instance, proposed including in the discussion about CCB the concept of Common but Differentiated Responsibility (CBDR),

[88] Adam Bower (2019) "Contesting the International Criminal Court: Bashir, Kenyatta, and the status of nonimpunity norm in world politics", *Journal of Global Security Studies* 4(1): 88-104. Available at: https://doi.org/10.1093/jogss/ogy037.
[89] Wayne Sandholtz (2019) "Norm contestation, robustness, and replacement", *Journal of Global Security Studies* 4(1): 139-46. Available at: https://doi.org/10.1093/jogss/ogy042.
[90] United Nations (2021) *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the context of international security*, A/76/135, 14 July. Available at: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf.
[91] Samuele Dominioni and Giacomo Persi Paoli (2022) *A taxonomy of malicious ICT incidents*, UNIDIR. Available at: https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/.

borrowed from the field of environmental protection, which would make a country's responsibility in cyberspace (and hence accountability) conditional on its level of economic development, among other things.

One standard that is particularly relevant to the discussions about accountability in cyberspace is that of attribution of malicious cyber activities. Attribution is a multilayered process involving technical, legal and policy communities – each with their own standards of attribution.[92] International law scholars, for instance, have developed concrete methodologies and determinants that are used for attributing malicious cyber activities and taking decisions about state responsibility.[93] The technical community has also identified standards and procedures for investigating cyberattacks and identifying who is behind a specific attack or cyber operation.[94] Political attribution is a more complex process whereby 'attribution is what states make of it'.[95] This is one of the reasons why the UN norm concerning attribution and states' obligation to take account of all available information has been debated.

With the progress in technical capabilities for identification of perpetrators and the shift in thinking about attribution processes, the discussion about accountability also became more nuanced. The requirement of absolute certainty has been increasingly replaced by new formulas (e.g. attribution with 'strong confidence') allowing for more flexible approaches and more room for action. Given the political nature of the attribution processes, it became acceptable that holding a state accountable does not require full certainty, and the legal and political risks associated with attribution – including accountability for a mistaken attribution – shift onto the state that make the attribution decision. It needs to be noted that the capacity to attribute an attack does not automatically translate into decisions about political attribution. Challenges associated with the decisions to attribute are clearly visible in the EU's guidelines for the implementation of the cyber diplomacy toolbox.[96]

[92] Dennis Broeders, Els De Busser and Patryk Pawlak (2020) "Three tales of attribution in cyberspace: criminal law, international law and policy debates", The Hague Program for Cyber Norms Policy Brief, 4 June. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3589139.

[93] See for instance Nicholas Tsagourias and Michael Farrell (2020) "Cyber attribution: technical and legal approaches and challenges", *European Journal of International Law* 31(3): 941–67. Available at: https://doi.org/10.1093/ejil/chaa057; Kristen Eichensehr (2020) "Cyberattack attribution and international law", *Just Security*, 24 July. Available at: https://www.justsecurity.org/71640/cyberattack-attribution-and-international-law/.

[94] See for instance Andraz Kastelic *(2022) Non-escalatory attribution of international cyber incidents: facts, international law and politics*, UNIDIR. Available at: https://unidir.org/publication/non-escalatory-attribution-of-international-cyber-incidents-facts-international-law-and-politics/; Delbert Tran (2018) "The law of attribution: rules for attributing the source of a cyber-attack" *Yale Journal of Law and Technology* 20(376): 376–441. Available at: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7830/DelbertTranTheLawofAttrib.pdf?sequence=2.

[95] Thomas Rid and Ben Buchanan (2015) "Attributing cyber attacks", *Journal of Strategic Studies* 38(1–2): 4–37. Available at: https://doi.org/10.1080/01402390.2014.977382.

[96] Council of the EU (2023) *Revised implementing guidelines of the Cyber Diplomacy Toolbox*, Brussels, 8 June. Available at: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

4.2 Information

To perform their functions, accountability mechanisms require information. Information constitutes the basis for verification of compliance with the agreed and accepted standards. It is the glue that holds together accountability holders and power-wielders. This is why the procedures and rules for access to information and transparency play an important role in promoting accountability in cyberspace. Such mechanisms or tools can be used to explain specific procedures that an actor adopted and follows, clarify exceptions to these procedures, or share concrete information about activities undertaken in cyberspace.

In this context, confidence- and transparency-building measures agreed among states are an important – although neglected – element of the accountability puzzle. Due to their primary function, defined as reducing the risks of conflict in cyberspace resulting from misperceptions or misunderstandings, the role of confidence-building measures (CBMs) in strengthening accountability has been underestimated even though several such measures are aimed at improving access to and quality of information about actions undertaken in cyberspace by states. A measure promoting exchange of information among states regarding their national cybersecurity strategies and doctrines gives accountability holders additional context for defining accountability standards and establishing responsibility of individual actors if their acts are contrary to standards and principles established through their domestic processes. Similarly, the public announcement of the US doctrines of 'persistent engagement' and 'defend forward' allows the broader international community to assess legitimacy of such operations but also whether the procedures defined by the US government are respected.

Due to their missions and roles within the cyber ecosystem, different stakeholder groups vary in their approaches to transparency and information-sharing rules. Development agencies, private sector actors and the intelligence community have different missions that prescribe their transparency and information-sharing standards. It is unrealistic to expect that a national intelligence or cybersecurity agency responsible for national security will apply the same rules for information sharing and transparency that are required from a development agency responsible for implementation of a CCB project in another country. This is also context-specific. Democratic societies require that even intelligence agencies be subjected to certain rules and procedures that can be verified by national parliaments or other purpose-specific bodies at the national level.[97] At the same time, development agencies may be subjected to extraordinary scrutiny when they are involved in projects that might have implications for human rights in another country or contribute to significantly strengthening the powers of law enforcement agencies or other security sector actors to the detriment of civil society organisations.

Information sharing between intelligence or national cybersecurity agencies plays a particularly important role in the context of negative accountability, whereby decisions

[97] Dennis Broeders and Camino Kavanagh (2023) *Shades of grey: cyber intelligence and (inter)national security*, EU Cyber Direct, 16 October 2023. Available at: https://eucyberdirect.eu/research/shades-of-grey-cyber-intelligence-and-inter-national-security.

about a proportionate and lawful response are conditioned by the quality of the available information. However, such information is usually kept away from public eyes and shared within well-defined channels. The limited availability of official information about cyber operations is the Achilles heel of accountability. Given that political attribution procedures rely primarily on information from intelligence agencies, the secrecy surrounding such evidence also undermines the credibility of decisions about attribution and ultimately allows the perpetrators to deny any involvement until the concrete evidence of their involvement is presented. Russia, for instance, has insisted in the past on seeing the intelligence that other countries have gathered as proof of its involvement in malicious cyber operations. Such release of intelligence would also mean giving a potential perpetrator insights into methods, techniques and tools used by the victims to identify and defend against the attackers.

However, there are also instances when states decide to share such information about the attacks that they have identified or prevented, either to pursue accountability or simply to signal to the perpetrators their capabilities or to garner support for policy decisions from a broader public. The Dutch Military Intelligence and Security Service published in 2018 a report in which it described the details of a disrupted cyber operation carried out by a Russian military intelligence (GRU) team against the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.[98] Interestingly, such moves are also increasingly made by countries such China that are usually accused of conducting attacks. In August 2023, China accused the US of a cyberattacks against the Wuhan Earthquake Monitoring Centre and suggested that it was performed using a complex malware previously deployed by the US intelligence agencies.[99]

The requirement of transparency and information sharing is also linked to the accountability mechanism whereby specific reporting or information-sharing mechanisms may be defined by law, regulation or policies. Such mechanisms have been introduced, for instance, in case of the breach notification obligations or vulnerability disclosure mentioned earlier. Different accountability mechanisms have different thresholds regarding the amount and quality of information required. Consumers and end-users depend on the information about the products provided by the companies. Since information about levels of security is not always available or shared by the producers, regulators have moved to introduce certification and labelling schemes to improve the quality of information about the products and services available to consumers. Where information is unavailable, hidden and not shared, accountability is difficult to pursue or requires creating additional channels for acquiring information, including from third parties such as civil society organisations or media.

[98] Ministry of Defence of the Netherlands (2018) "Russian cyber operation, remarks Minister of Defence, 4 October in the Hague". Available at: https://english.defensie.nl/topics/cyber-security/documents/publications/2018/10/04/remarks-minister-of-defense-4-october-in-the-hague.
[99] Yuan Hong (2023) "Wuhan Earthquake Monitoring Center suffers cyberattack from the US; investigation underway", *Global Times*, 26 July 2023. Available at: https://www.globaltimes.cn/page/202307/1295064.shtml.

4.3 Monitoring and verification

Like information sharing, monitoring plays an important role in the enforcement of the agreed standards. But it is equally problematic, as it depends on the existence of adequate verification mechanisms, which in turn rely on available information. Because such information is not always public or accessible, verification, too, becomes difficult. Limited availability of information was one of the main arguments against establishing a cyber-arms control mechanism[100] that would curb the development of offensive capabilities.[101] It is also one of the main arguments raised against a proposal for a legally binding international instrument regulating state behaviour in cyberspace, given that monitoring and verification of such a cyber treaty would be extremely difficult, if not impossible.[102]

Some accountability processes may have clearly defined verification mechanisms, whereas others rely on more informal structures and tools. In the case of hierarchical or supervisory accountability, for instance, mechanisms for verification are provided for by law or internal procedures: ministers of foreign affairs or heads of national cybersecurity agencies are obliged to report and provide information to their parliaments, which in turn may request additional sources for verification. Similarly, actions or interventions by government officials can be verified based on meeting reports, minutes or other official documents that are required by internal reporting procedures and subject to transparency and access to information regulations. Companies are required to submit annual reports to their boards and shareholders, but there are hardly any examples of such reports mentioning cyber matters, let alone any decisions that were taken to hold people accountable for violations of good practices and exposing consumers to external risks. Some of the accountability mechanisms deployed by the companies are regular third-party audits such as certification of the data management systems in accordance with existing standards (e.g. ISO 27001) or source code reviews. In certain cases when information is limited or kept secret, investigative journalism or work conducted by civil society organisations is the only way to provide a monitoring and verification mechanism, which in turn stresses the importance of public reputational accountability.

4.4 Sanctions

The final element of the puzzle is sanctions. It is generally believed that for any accountability mechanism to perform its function, there needs to be a form of penalty or cost for those who violate the agreed standards and cause harm. Despite the large

[100] Andrew Futter (2020) "What does cyber arms control look like? Four principles for managing cyber risk", *Global Security Policy Brief*, European Leadership Network, June. Available at: https://www.europeanleadershipnetwork.org/wp-content/uploads/2020/06/Cyber-arms-control.pdf.
[101] Erica D. Borghard and Shawn W. Lonergan (2018) "Why are there no cyber arms control agreements?", Council on Foreign Relations, 16 January. Available at: https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.
[102] Scott Neuman and Greg Myre (2021) "Hacks are prompting calls for a cyber agreement, but reaching one would be tough", *NPR*, 2 July. Available at: https://www.npr.org/2021/07/02/1009925791/hacks-are-prompting-calls-for-a-cyber-agreement-but-reaching-one-would-be-tough.

volume of activities undertaken by all groups of stakeholders – including governments, international organisations, the private sector and civil society organisations – there has been hardly any debate around the desirability of sanctions, their purpose, their types or even the cost to those imposing them, all of which are traditionally addressed in the context of sanctions.

One of the most developed aspects is sanctions for violations of the standards set in the UN FRSB. Several countries – including the US, the UK, Australia and South Korea – and the EU have introduced targeted sanctions against individuals or entities associated with concrete cyber operations. Limited existing scholarship on cyber sanctions has attempted to provide some answers – including about the effectiveness of sanctions.[103] Critics of the current approach, which relies heavily on targeted sanctions (e.g. travel bans, asset freezes) point out their limited reach and mostly symbolic nature.[104] In their view, any instrument that aims to strengthen accountability and end impunity in cyberspace should have a visible impact. Because malicious actors usually act as proxies for their client-states, the argument goes, the sanctioning mechanisms need to carry the cost, especially for the states.[105]

Sanctioning mechanisms are also provided in the form of civil or penal court proceedings. In this context, the measures adopted in the criminal justice system to fight cybercrime provide the main point of reference. However, in the absence of a global and universal definition of cybercrime, international cooperation in this domain is often difficult due to concerns about over- or under-criminalisation of certain behaviours. The risk that cybercrime laws will be abused by authoritarian regimes to curb freedom of speech or other civil liberties has brought to the fore the question of what acts should be criminalised and how to ensure that the principles of necessity and proportionality are respected. An interesting example of a sanction in this context is take-downs of bots operating across multiple jurisdictions. Such operations usually involve extensive international cooperation between private companies and government agencies given that the computers that are being 'arrested' are in different countries.[106] In February 2024, law enforcement agencies in the US, the UK and several other countries disrupted LockBit's operations by seizing numerous public-facing websites used by LockBit to connect to the organisation's infrastructure and seizing control of their servers.[107]

Another category is sanctions that governments may impose on companies or organisations that fail to comply or implement laws and regulation that aim to strengthen cyber resilience, target cybercriminals or strengthen the open, safe and secure nature of

[103] Patryk Pawlak and Thomas Biersteker (2019) "Guardian of the galaxy: EU cyber sanctions and norms in cyberspace", Chaillot Paper, No. 155, EU Institute for Security Studies. Available at: https://op.europa.eu/en/publication-detail/-/publication/f65d51c1-0435-11ea-8c1f-01aa75ed71a1/language-en.
[104] Iryna Bogdanova and María Vásquez Callo-Müller (2021) "Unilateral economic sanctions to deter and punish cyber-attacks: are they here to stay?", *EJIL:Talk!*, 7 December. Available at: https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/.
[105] Stefan Soesanto (2021) "After a year of silence, are EU cyber sanctions dead?", *Lawfare*, 26 October 2021. Available at: https://www.lawfaremedia.org/article/after-year-silence-are-eu-cyber-sanctions-dead.
[106] Europol (2023) "288 dark web vendors arrested in major marketplace seizure", 2 May. Available at: https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure.
[107] US Department of Justice (2024) "US and UK disrupt LockBit ransomware variant", 20 February. Available at: https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant.

cyberspace more broadly. In the EU, specific laws have been put in place to promote cyber risk management and mitigation models among private companies,[108] to introduce cybersecurity standards,[109] to prevent unsafe and insecure products from entering the market[110] or to ensure adequate levels of data protection with concrete reporting and sanctioning mechanisms.[111] The question of compliance is linked to the nature of regulation itself and a broader political context within which it is adopted. EU laws and regulation are criticised for interfering with market mechanisms, undermining innovation or creating additional burdens for companies that become less competitive globally.[112] However, in China, for instance, the question of compliance with (Chinese) regulation is more problematic considering the potential implications for human rights, trade-related concerns or security implications and the use of state institutions by the government to force companies to comply or face penalties.[113]

In addition, in recent years states have increasingly resorted to regulatory tools and bans on specific technology provided by high-risk companies in an effort to eliminate or at least reduce their exposure to such vendors. The example of Chinese companies Huawei and ZTE is the most publicised and scrutinised. While such approaches provide a certain form of government-steered accountability targeting private companies with close ties to governments with questionable records in cyberspace, they neglect a similar role that market mechanisms could play. In those cases, it would be up to consumers and end-users to take decisions about which technologies to use. Any doubts or problems associated with specific vendors would then possibly translate into falling sales or consumer boycotts. For instance, Samsung – the world's largest smartphone maker – was forced to discontinue and recall 2.5 million Galaxy Note 7 devices on grounds of safety, which cost the company USD5.3 billion.

Finally, an issue that has received hardly any attention is sanctions in cases of positive accountability. This is based on a very simple assumption within the cyber community that 'good deeds' such as CCB support provided to other countries – for instance, in the form of capacity-building – aim to achieve positive effects in the partner country. As such,

---

[108] *Official Journal of the European Union* (2022) "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)", 27 December. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[109] *Official Journal of the European Union* (2019) "Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)", 7 June 2019. Available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[110] European Commission (2022) *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)*, 15 September. Available at: https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf.

[111] *Official Journal of the European Union* (2016) "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", 4 May. Available at: https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf.

[112] Jacques Pelkmans and Andrea Renda (2014) *How can EU legislation enable and/or disable innovation*, European Commission. Available at: https://ec.europa.eu/futurium/en/system/files/ged/39-how_can_eu_legislation_enable_and-or_disable_innovation.pdf; Carmelo Cennamo and D. Daniel Sokol (2021) "Can the EU regulate platforms without stifling innovation?", *Harvard Business Review*, 1 March. Available at: https://hbr.org/2021/03/can-the-eu-regulate-platforms-without-stifling-innovation.

[113] Joe McDonald (2023) "Foreign companies in China face growing scrutiny, pressure", *Associated Press*, 28 April. Available at: https://apnews.com/article/china-foreign-business-corruption-investigation-technology-113adfa55788aabb11896d8b059b32bc.

they are subjected to limited scrutiny that results either from monitoring and evaluation mechanisms or reporting on the indicators. In the case of donor agencies, such as the European Commission, the sanctioning mechanisms come from the scrutiny provided by the European Parliament for political actions as well as the Court of Auditors and Anti-Fraud Office for financial aspects. In addition, partner countries that engage with donor agencies can sanction their donors by withdrawing or suspending cooperation in cases where they feel that the cooperation mechanisms are damaging their national interests or the objectives of the project. It might happen that such sanctions are also used to exercise political pressure on a donor.

The opposite is also true: several donor agencies have suspended their activities in Uganda following the adoption of a law criminalising homosexuality.[114] Similar mechanisms can be used in relations between international financial institutions such as the World Bank or the European Investment Bank and their clients. In addition, these institutions can be sanctioned by their board of directors, on one hand, and their funders on the other. Such sanctions can take the form of more hands-on political steering or fewer resources for conducting activities. Sanctioning by limiting the budgets of international organisations is a generally used practice by donors and funders unsatisfied with the direction in which the organisations are moving with their operations.[115]

[114] World Bank Group (2023) "Statement on Uganda", 8 August. Available at: https://www.worldbank.org/en/news/statement/2023/08/08/world-bank-group-statement-on-uganda.
[115] Susan Cornwell (2011) "US halts UNESCO funding over Palestinian vote", *Reuters*, 31 October. Available at: https://www.reuters.com/article/idUSTRE79U5ED/.

5. Cyber accountability across policy regimes

Different views on accountability in cyberspace have focused on cyber-specific institutions and over-emphasised the importance of sanctions as a necessary condition for accountability. In the current geopolitical climate, the question of accountability is challenging not only in the cyber domain but in many other regimes, including trade, disarmament, climate and human rights. Challenges linked to the implementation of the existing international treaties, the lack of national compliance with the judgments of international courts and the overall crisis of international institutions pose a broader problem for global governance. Nonetheless, there have also been positive developments. The progressing digitalisation and its impact across many other international regimes – including trade, human rights and international criminal justice – mean that international institutions increasingly expand the scope of their activities and need to address accountability in cyberspace as part of their mandate. The following sections discuss how some of these developments can support strengthening accountability in cyberspace.

5.1 International security: the case of the UNSC

The UNSC is a body established by the Charter of the UN with primary responsibility for the maintenance of international peace and security.[116] It is the main body tasked to determine the existence of a threat to the peace or an act of aggression. Through its resolutions, it can also call on states to settle their disputes by peaceful means or impose sanctions and authorise the use of force to maintain or restore international peace and security. The UNSC's decisions are binding on all UN member states and require an affirmative vote of nine members, including the concurring votes of the permanent members. Even though some argue that the UNSC was built to be unfair,[117] many criticise it for its ineffectiveness in dealing with ongoing conflicts and call for the reform of its memberships and powers[118] to minimise the impact of great power politics and disagreements among its members.[119]

The impact of information and communication technologies on international security and stability is undeniable, as evidenced by several UN processes: the UN GGE, the OEWG and the effort to establish the Programme of Action (PoA) as a permanent structure, all of which focus on international security and responsible state behaviour in cyberspace.

[116] Article 24 of the UN Charter; also Chapters VI, VII, VIII and XII of the UN Charter.
[117] Mark Mazower (2013) *Governing the world: the history of an idea, 1815 to the present*, London: Penguin Random House.
[118] United States Institute of Peace (2023) "The U.N. Security Council was designed for deadlock — can it change?", 1 March. Available at: https://www.usip.org/publications/2023/03/un-security-council-was-designed-deadlock-can-it-change.
[119] Stewart Patrick, Sithembile Mbete, Matias Spektor, Zhang Guihong, Alexandra Novosseloff, Christoph Heusgen, Rohan Mukherjee, Phillip Y. Lipscy, Miguel Ruiz Cabañas Izquierdo, Adekeye Adebajo, Andrey Kolosovskiy, Joel Ng, Priyal Singh, Barçin Yinanç, Richard Gowan and Anjali Dayal (2023) *UN Security Council reform: what the world thinks*, Carnegie Endowment for International Peace, 28 June 2023. Available at: https://carnegieendowment.org/2023/06/28/un-security-council-reform-what-world-thinks-pub-90032.

Although the UNSC has touched upon various dimensions of cybersecurity in the context of international security,[120] it was not until the Estonian presidency in 2021 that a formal, high-level open debate on cybersecurity took place.[121] Before that, various aspects of cybersecurity were discussed in informal settings, including large-scale cyberattacks against Georgia in 2019 and two Arria-formula meetings on 'cyber stability, conflict prevention and capacity building' (organised by Estonia)[122] and 'cyber-attacks against critical infrastructure' (organised by Indonesia).[123] Since 2021, several other Arria-formula meetings devoted to stability of cyberspace were organised in the UNSC, including on 'the impact of emerging technologies on international peace and security'[124] convened by China, on 'addressing and countering hate speech and preventing incitement to discrimination, hostility, and violence on social media'[125] by Kenya, and on 'preventing civilian impact of malicious cyber activities'[126] by Estonia and the UK. Although Arria-formula meetings provide an opportunity for exchange of views with individuals, organisations or institutions on matters within the competence of the UNSC, they cannot constitute an alternative to formal sessions in the long term. They usually have no records and no outcomes. Nonetheless, the Arria-formula meetings with top UN officials provide an opportunity to receive briefings when no agreement can be reached in the formal meeting.

The role of the UNSC as the ultimate arbiter in relations between states and existing divisions among its members Council have seriously undermined its position in terms of promoting accountability in cyberspace. The use of vetoes by the permanent members of the UNSC who are also among those most frequently accused of malicious and illegal cyber operations has meant for a long time that the UNSC could not be realistically considered a viable option for strengthening accountability in cyberspace. However, UNGA resolution 76/262 adopted in 2022,[127] aimed at holding the five permanent UNSC members accountable for use of veto, may change the situation. According to the resolution tabled by Liechtenstein and co-sponsored by 83 member states, the President of the UNGA shall convene a formal meeting within 10 working days of the casting of a

[120] Security Council Report (2019) *In hindsight: the Security Council and cyber threats*, 23 December. Available at: https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.
[121] Security Council Report (2022) "In hindsight: the Security Council and cyber threats, an update", 21 January. Available at: https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php.
[122] Security Council Report (2020) "Arria-formula meeting: cyber stability, conflict prevention and capacity building", 21 May. Available at: https://www.securitycouncilreport.org/whatsinblue/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php.
[123] Security Council Report (2020) "Arria-formula meeting on cyber-attacks against critical infrastructure", 15 August. Available at: https://www.securitycouncilreport.org/whatsinblue/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.
[124] Security Council Report (2021) "Arria-formula meeting on the impact of emerging technologies on international peace and security", 14 May. Available at: https://www.securitycouncilreport.org/whatsinblue/2021/05/arria-formula-meeting-on-the-impact-of-emerging-technologies-on-international-peace-and-security.php.
[125] Security Council Report (2021) "Arria-formula meeting on hate speech and social media", 27 October. Available at: https://www.securitycouncilreport.org/whatsinblue/2021/10/ria-formula-meeting-on-hate-speech-and-social-media.php.
[126] Security Council Report (2021) "Arria-formula meeting on 'preventing civilian impact of malicious cyber activities'", 19 December. Available at: https://www.securitycouncilreport.org/whatsinblue/2021/12/arria-formula-meeting-on-preventing-civilian-impact-of-malicious-cyber-activities.php.
[127] United Nations (2022) *Standing mandate for a General Assembly debate when a veto is cast in the Security Council*, A/RES/76/262, 28 April. Available at: https://digitallibrary.un.org/record/3972149?ln=en.

veto and hold a debate on the situation as to which the veto was cast, provided that the UNGA does not meet in an emergency special session on the same situation.

> ***Implications for accountability in cyberspace:*** *The adoption of resolution 76/262 means that should a resolution on cyber-related issues be introduced and vetoed in the UNSC, all members of the UN will have a chance to express their views on a situation through a vote and therefore overcome the political obstacles in the UNSC.*

5.2 International criminal justice: the case of the International Criminal Court

The International Criminal Court (ICC) was established to hold accountable those responsible for the gravest crimes of concern to the international community.[128] The crimes falling under its jurisdiction are genocide, crimes against humanity, war crimes and the crime of aggression.[129] Situations that might fall under the jurisdiction of the Court are examined, investigated and prosecuted by the Office of the Prosecutor (OTP). Interestingly, the Rome Statute gives the Prosecutor General the mandate to decide which situations to investigate within the scope of the Statute. The ICC has a clear competence to investigate natural persons for attacks directed against any civilian population, including grave breaches of the Geneva Conventions and other serious violations of the laws and customs applicable in international armed conflict and in armed conflicts not of an international character. Specifically, the ICC may investigate, among others, intentional attacks against the civilian population not taking direct part in hostilities and attacks targeting civilian objects that are not military objectives. Several types of cyberattacks may fall within these categories, which potentially opens the door for ICC's jurisdiction.

Information on alleged or potential ICC crimes can be sent to the OTP by any individual, group, or organisation and the ICC prosecutor is then responsible for determining whether a situation meets the legal criteria laid out by the Rome Statute.[130] In 2021, a Council of Advisers on the Application of the Rome Statute to Cyberwarfare produced a report discussing how different forms of cyber operations fit into the Rome Statute system and other international legal frameworks.[131] Following the Russian war of aggression against Ukraine, in March 2023, the Human Rights Center at University of

[128] Article 1 of the Rome Statute.
[129] Article 5 of the Rome Statute.
[130] International Criminal Court (2016) *Policy paper on case selection and prioritisation*, 15 September. Available at: https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf.
[131] Permanent Mission of Liechtenstein to the UN (2021) *The Council of Advisers' report on the application of the Rome Statute of the International Criminal Court to cyberwarfare*. Available at: https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.

California (UC) Berkeley School of Law filed an 'article 15 communication'[132] with the ICC Prosecutor in which it focuses on attacks carried out against Ukraine by a Russian group known as Sandworm that many link to Russia's GRU military intelligence agency. The submission lists numerous instances of attacks on civilian critical infrastructure such as Ukraine's power grid, deployment of data-destroying Not-Petya malware, and more recent attacks on the Viasat satellite modem network.[133]

Although for a long time the ICC has remained silent on the question of potential harm, recently the Prosecutor General, Karim Khan, published a piece in which he made it clear that he intended to investigate and prosecute any hacking crimes that violate existing international law, in particular those against critical infrastructure such as medical facilities or control systems for power generation that may have consequences for a civilian population.[134] One of the issues that will need to be resolved in specific cases is what constitutes an attack, object or military objective in cyberspace.[135] The precondition for such cases is that they be 'sufficiently grave', meaning that not all cyberattacks with consequences for a civilian population will be automatically prosecuted.[136] The submission from UC Berkeley provides a blueprint for how such cases could be argued and names concrete individuals: Vladimir Putin, Sergei Shoigu, Valery Gerasimov, Igor Kostyukov, Vladimir Alexeyev, Sergey Gizunov and Aleksandr Osadchuk.

> ***Implications for accountability in cyberspace:*** *The case of cyberattacks against Ukraine provides an opportunity for the ICC to strengthen the pursuit of accountability for violations of international law and the protection of civilians in armed conflicts conducted with the use of new technologies. But it also opens the door for investigating cases of grave cyberattacks against a civilian population outside of an international conflict. The ICC's engagement in the cyber domain even at the stage of information collection and investigation would contribute to further refinement of the FRSB in cyberspace.*

[132] Article 15 of the Rome Statute.
[133] Lindsay Freeman, Amanda Ghahremani and Sophie Lombardo (2023) "The gravity of Russia's cyberwar against Ukraine", *Opinio Juris*, 19 April. Available at: https://opiniojuris.org/2023/04/19/the-gravity-of-russias-cyberwar-against-ukraine/.
[134] Karim A.A. Khan (2023) "Technology will not exceed our humanity", *Digital Front Lines*, 20 August. Available at: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/.
[135] Lindsay Freeman (2023) "Ukraine symposium – accountability for cyber war crimes", *Articles of War*, 14 April. Available at: https://lieber.westpoint.edu/accountability-cyber-war-crimes/.
[136] Andy Greenberg (2023) "The International Criminal Court will now prosecute cyberwar crimes", *Wired*, 7 September. Available at: https://www.wired.com/story/icc-cyberwar-crimes/.

5.3 Trade and investment: the case of investor–state dispute settlement

Investor–state dispute settlement (ISDS) clauses are introduced in trade and investment agreements to ensure corporate accountability for violations of human rights.[137] ISDS is a mechanism in a free trade agreement (FTA) or investment treaty that provides foreign investors with the right to access an international tribunal to resolve investment disputes. The ISDS clauses in the investment agreements give businesses the right to sue a state should it decide to introduce a new regulation that has adverse effects on the company's profits. As such, ISDS clauses can prevent governments from introducing new laws, even if such regulation is in the broader public interest and strengthens corporate accountability. They may also undermine the ability of states to realise their duty to respect human rights, as laid out in the UN Guiding Principles.[138] Some notable examples of cases include the lawsuit by tobacco giant Philip Morris against Australia for introducing plain packaging on cigarettes[139] and that by German coal company RWE against the Dutch government for its decision to phase out fossil fuel consumption[140].

The ISDS clauses often affect the freedom of countries to introduce standards and laws that may be beneficial to their people and environment. This is particularly relevant in the context of increased efforts by the international community to strengthen capacities of numerous countries – especially developing countries – in the field of cyber resilience and cybercrime. Should a country wish to adopt new laws that require companies to comply with specific cybersecurity standards or meet concrete reporting obligations that create additional cost for them, those companies could potentially use the ISDS clauses in the existing trade and investment agreements. Such a development would undoubtedly have a significant deterring effect on governments who have limited resources and could adversely impact global efforts aimed at reducing cyber vulnerabilities and protecting citizens from cyber harm by regulating the behaviour of international corporations. The same is true for protection of human rights online. Two trends are relevant in this context: the increase in the number of countries that reject or modify ISDS clauses[141] and the growing focus on corporations undertaking human rights and environmental due diligence.[142]

---

[137] See the Business and Human Rights Resource Centre. Available at: https://www.business-humanrights.org/en/.
[138] United Nations Human Rights Office of the High Commissioner (2011) *Guiding principles on business and human rights. implementing the United Nations 'Protect, respect and remedy' framework*. Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.
[139] Business and Human Rights Resource Centre (2016) *Philip Morris international arbitration (re. Australian plain packaging law)*, 24 May. Available at: https://www.business-humanrights.org/en/latest-news/philip-morris-international-arbitration-re-australian-plain-packaging-law/.
[140] Kira Taylor (2021) "Germany's RWE uses Energy Charter Treaty to challenge Dutch coal phase-out", *Euractiv*, 5 February. Available at: https://www.euractiv.com/section/energy/news/germanys-rwe-uses-energy-charter-treaty-to-challenge-dutch-coal-phase-out/.
[141] Ben van der Merwe (2021) "What do trade deals mean for FDI?", *Investment Monitor*, 12 February.
[142] Business and Human Rights Resource Centre (2023) "Towards an EU mandatory due diligence and corporate accountability law", 15 December. Available at: https://www.business-humanrights.org/en/latest-news/eu-towards-a-mandatory-due-diligence-corporate-accountability-law/.

Implications for accountability in cyberspace: *As in the case of human rights due diligence that promises to hold companies responsible for their social and environmental impact,*[143] *greater regulation of corporations regarding cyber resilience could oblige them to implement concrete security standards across their whole supply chain. This is, for instance, the rationale behind recently adopted or proposed EU legislative acts (e.g. the Network Information Security Directive, certification schemes set out by the Cybersecurity Act and the Cyber Resilience Act) or policy documents such as the Council Conclusions on ICT supply chain security.*[144]

5.4 Development assistance: the case of the World Bank Inspection Panel

To ensure that people and communities affected adversely by projects funded by the World Bank have access to an independent body to seek recourse, the Board of Executive Directors created the Inspection Panel as an independent complaints mechanism. The Panel is an impartial fact-finding body reporting directly to the Board with the aim of promoting accountability at the World Bank. It is a non-judicial body that acts independently, impartially and objectively in evaluating the processes followed by the Bank that were put in place to provide social and economic benefits and avoid harm to people or to the environment. As such, it performs oversight and accountability functions. In September 2020, the Board approved a resolution establishing the World Bank Accountability Mechanism (AM), which houses the Panel, and established a new Dispute Resolution Service, which will give complainants another way to have their concerns addressed. The Panel has a mandate to review projects funded by the World Bank through the International Bank for Reconstruction and Development (IBRD) and the International Development Association (IDA). It assesses allegations of harm linked, for instance, to risks to people and the environment related to dam safety, use of pesticides and other indirect effects of investments or adverse effects on natural habitats. The complaints can be filed by different actors, including an organisation, association, society or other group of individuals in the country where the Bank-financed project is located who believe their rights or interests have been, or are likely to be, adversely affected in a direct and material way.

[143] See the Business and Human Rights Resource Centre, "Mandatory Due Diligence" section. Available at: https://www.business-humanrights.org/en/big-issues/mandatory-due-diligence/.
[144] Council of the EU (2022) *Council conclusions on ICT supply chain security*, 13664/22, 17 October. Available at: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf.

Implications for accountability in cyberspace: *The growing investment by the World Bank in digital transformation projects or critical infrastructure projects with significant digital components opens the door for the Inspection Panel to be used to strengthen positive accountability in the cyber domain, in particular in the context of CCB projects. The Bank's Multi-Donor Trust Fund was developed as an associated trust fund under the broader Digital Development Partnership (DDP) umbrella to better define, understand, articulate, structure and roll out the cybersecurity development agenda. The Fund aims, among others things, to provide practical and technical analysis on the threats, risks and opportunities of emerging technology, fund effectively coordinated tailored CCB activities, and lay the cybersecurity foundation in low- and middle-income countries.*[145]

5.5 Human rights: the case of the European Court of Human Rights

The human rights regime has probably the most advanced legal accountability system, with different regional organisations and treaties having established specific peer review mechanisms and bodies to deal with human rights violations. Each of the core international human rights treaties has a 'treaty body' of experts that monitors implementation of its provisions.[146] In addition to the universal instruments, regional instruments such as the European Convention on Human Rights (ECHR) have established their own bodies. The European Court of Human Rights (ECtHR) monitors respect for human rights in the 46 Council of Europe member states that have ratified the ECHR, including the right to respect for private and family life,[147] freedom of thought, conscience and religion[148] and freedom of expression.[149]

With the expansion of human activities online, the human rights regime has played an important role in promoting accountability in cyberspace. ECtHR has delivered several judgments that play a critical role in ensuring that people enjoy the same level of protection of their rights online and offline. In the case *Cengiz and Others v. Turkey*, the Court acknowledged that 'the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest'.[150] Over the years, the ECtHR

[145] See the World Bank's Cybersecurity Multi-Donor Trust Fund. Available at: https://www.worldbank.org/en/programs/cybersecurity-trust-fund.
[146] United Nations Human Rights Office of the High Commissioner (2013) *Individual complaint procedures under the United Nations Human Rights Treaties*, Fact Sheet No. 7, Rev. 2. Available at: https://www.ohchr.org/sites/default/files/Documents/Publications/FactSheet7Rev.2.pdf.
[147] Article 8 of the ECHR.
[148] Article 9 of the ECHR.
[149] Article 10 of the ECHR.
[150] §§ 49 and 52.

has taken a stand in numerous cases concerning measures blocking access to the internet, restrictions placed on prisoners' access to certain internet sites such as legal advice or educational information,[151] and data protection.[152] In the cases of *Big Brother Watch and others v. the United Kingdom*[153] and W*ieder and Guarnieri v. the United Kingdom*,[154] the ECtHR found that government bulk collection of personal data for surveillance purposes constituted a violation of Article 8 of the ECHR. The most recent addition to this extensive list is the judgment in the case of *Podchasov v. Russia* concerning end-to-end encryption of communication, whereby the ECtHR took the position that 'the security services' direct access to the data stored without adequate safeguards against abuse and the requirement to decrypt encrypted communications, as applied to end-to-end encrypted communications, cannot be regarded as necessary in a democratic society'.[155]

> ***Implications for accountability in cyberspace:*** *The expanding case law of the ECtHR regarding the application of human rights online provides a valuable indication of what is and is not acceptable in cyberspace. It also provides a very concrete mechanism to hold states accountable for violations of the EHRC, which through the case law proves to be a living document and sets standards of accountability in the cyber domain. The public nature of the hearings and the detailed reasoning provided in the ECtHR judgments constitute an important source of information about government practices and strengthen transparency. One of the main challenges for the effectiveness of the ECtHR is the implementation of judgments by the national authorities – the process that is supervised by the Committee of Ministers, aided by the Department for the Execution of Judgments.*[156] *The most recent report on the implementation of the judgments of the ECtHR singled out Ukraine, Romania, Türkiye, Azerbaijan and Hungary as countries with the highest number of non-implemented ECtHR judgments, some of which have not been resolved for over 10 years.*[157]

[151] European Court of Human Rights (2022) "Access to Internet and freedom to receive and impart information and ideas", factsheet, September. Available at: https://www.echr.coe.int/documents/d/echr/FS_Access_Internet_ENG.
[152] European Court of Human Rights (2023) "Personal data protection", factsheet, November. Available at: https://www.echr.coe.int/documents/d/echr/fs_data_eng.
[153] European Court of Human Rights (2021) *Case of Big Brother Watch and others v. the United Kingdom*, 25 May. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}.
[154] European Court of Human Rights (2023) *Case of Wieder and Guarnieri v. the United Kingdom*, 12 September. Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-226468%22]}.
[155] European Court of Human Rights (2024) *Case of Podchasov v. Russia*, 13 February 2024. Available at: https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}.
[156] See Council of Europe (2023), "Implementation of ECHR judgments – Latest decisions by the Committee of Ministers", 10 March. Available at: https://www.coe.int/en/web/human-rights-rule-of-law/-/implementation-of-judgments-from-the-european-court-of-human-rights-latest-decisions-by-the-committee-of-ministers.
[157] Following its exclusion from the Council of Europe on 16 March 2022, the Russian Federation ceased to be a High Contracting Party to the European Convention on Human Rights on 16 September 2022. Nonetheless, the Committee of Ministers continues to supervise the execution of the judgments and friendly settlements concerned and the Russian Federation is required to implement them. See: https://rm.coe.int/implementation-of-the-judgments-of-the-european-court-of-human-rights-/1680aaaa60.

5.6 Internet governance: the case of ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) helps coordinate and support the maintenance of the domain name system (DNS) – a database of names and numbers that ensure the proper functioning of the global internet. Based in the US, ICANN has been under extensive scrutiny of its practices and the potential influence that the US government might have over its decisions. ICANN's position in the cyber ecosystem is peculiar and the organisation itself has been subject to a long debate about its accountability and transparency mechanisms.[158] In 2008, ICANN presented its own *Accountability and Transparency Frameworks and Principles*, which mention three types of accountability: public, corporate and legal, and participatory.[159] The organisation established several oversight and enforcement mechanisms, including an Independent Review Process (IRP) for independent third-party review of Board actions (or inactions) and an ICANN Ombudsman[160] whose role is to provide an independent internal evaluation of complaints by members of the ICANN community against the ICANN staff,[161] Board or an ICANN constituent body.[162] Two of the notable cases under the IRP concern string similarity review over the generic top-level-domain name (gTLD) '.hotels' filed by Booking.com,[163] claiming that ICANN violated the principles of transparency and fairness, and the submission by the Gulf Cooperation Council (GCC), which opposed the registration of gTLD '.persiangulf' as an international forum for people of Persian descent and heritage on the grounds of the use of the disputed geographical name.[164]

> ***Implications for accountability in cyberspace:*** *The transparency and accountability mechanisms adopted by ICANN play an important role in minimising any potential abuses of power or unequal treatment of different stakeholder groups, which is a precondition for ensuring that its bottom-up, multi-stakeholder model remains effective. They also guarantee stability and security of the internet infrastructure that the global community depends on. The access to those mechanisms enjoyed by members of different communities is a guarantee that no particular interests will have excessive influence over the governance of the internet.*

[158] Hortense Jongen and Jan Aart Scholte (2021) "Legitimacy in multistakeholder global governance at ICANN", in: *Global governance: a review of multilateralism and international organizations*, Leiden: Brill.
[159] ICANN (2008) *ICANN accountability and transparency frameworks and principles*. Available at: https://www.icann.org/en/system/files/files/acct-trans-frameworks-principles-10jan08-en.pdf.
[160] See ICANN Ombuds website: https://www.icann.org/ombuds.
[161] See "ICANN recommendations to improve staff accountability", 13 November 2017. Available at: https://www.icann.org/en/announcements/details/recommendations-to-improve-icann-staff-accountability-13-11-2017-en.
[162] See ICANN Accountability mechanisms. Available at: https://www.icann.org/resources/pages/mechanisms-2014-03-20-en.
[163] See "Booking.com v. ICANN (.HOTELS)". Available at: https://www.icann.org/resources/pages/booking-v-icann-2014-03-25-en.
[164] 'Persian Gulf' is the name used by Iran whereas several Arab states, including members of the GCC, use the name 'Arabian Gulf'.

6. Moving forward: three options for a cyber accountability system

UN Secretary General António Guterres called in 2023 for establishment of 'an independent multilateral accountability mechanism for malicious use of cyberspace by States to reduce incentives for such conduct'. [165] Such a mechanism, he argued, 'could enhance compliance with agreed norms and principles of responsible State behaviour'. In light of the upcoming negotiations of the Pact for the Future and the Global Digital Compact, the following sections of this paper discuss potential accountability mechanisms under the UN umbrella. Although the increasing importance of the UN as an orchestrating organisation for the international community[166] suggests that an accountability mechanism under the UN umbrella would be logical, there are several practical challenges – notably the question of attribution – that need to be addressed. At the same time, the increasing complexity of the challenges in cyberspace – in terms of both vulnerabilities and governance – requires strengthening of networked accountability that maximises an effective use of all stakeholders within the cyber ecosystem. At the same time, such a system needs to connect different layers in the accountability stock to minimise the risks of instrumentalisation and politicisation of such a mechanism.[167] The following sections discuss possible pathways for how this ambitious goal could be implemented in practice.

6.1 A new accountability mechanism at the UN

Any proposal for a new cyber accountability mechanism under the UN umbrella would need to answer at least two major questions: (1) what is the function of the proposed mechanism? and (2) what goals does it aim to achieve? The answers to these questions would then lead to discussions about its composition, modalities of work, and resources for its functioning.

There is an implicit assumption that any accountability mechanism needs to address the question of attribution, which states have consistently described as their exclusive competence while rejecting proposals of similar domestic or international accountability mechanisms.[168] Paradoxically, and contrary to the general expectation, for a UN-driven cyber-accountability mechanism to have any chance of success, it would need to exclude the attribution function from the very beginning. Such a choice would also imply that a new UN-based mechanism would need to give up on any sanctioning function for which

[165] United Nations (2023) "A new agenda for peace", Policy Brief No. 9. Available at: https://dppa.un.org/en/a-new-agenda-for-peace.
[166] Stephanie C. Hofmann and Patryk Pawlak (2023) "Governing cyberspace: policy boundary politics across organizations", *Review of International Political Economy* 30(6). Available at: https://doi.org/10.1080/09692290.2023.2249002.
[167] Hofmann and Pawlak (2023).
[168] Mueller et al. (2019).

attribution is a precondition. But this does not mean that the proposal makes no sense: on the contrary. With a large number of states still lacking basic capacities to attribute or assess the evidence related to specific cyberattacks, there is ample room for a UN accountability mechanism to play a role beyond the attribution and punitive functions. The opinions or reviews provided through such mechanisms could be used, for instance, to guide the investment decisions of large multilateral companies or multilateral donors and international financial institutions.

One option for the new accountability mechanism could be to perform a **deliberative function** with the aim of increasing the understanding of significant cyber incidents among the states. This mechanism could take the form of a Cyber Incident Review Board composed of both governmental and non-governmental technical experts appointed by the UN Secretary General. The Board not only could provide a general overview of the information obtained from various sources (including the state victim, private sector, etc.) and an assessment of its accuracy but also could issue concrete recommendations regarding how similar incidents might be avoided in the future and which national and international cyber capacities require further strengthening. In that sense, the Board could also serve as an information hub concerning specific incidents. The primary challenge in this respect would be to ensure that the composition of the Board reflected a broader UN membership and was not limited to a small group of well-resourced countries with advanced cyber capacities. The findings of the Board would provide a neutral assessment of concrete cyber incidents and could feed into broader political discussions at the UN, including the OEWG or the future Programme of Action. Similar bodies established at the national level – such as the Cyber Safety Review Board in the US[169] – illustrate how such a mechanism can be developed in practice.

A more ambitious alternative would be the establishment of a **special body** responsible for the implementation of and compliance with specific international commitments expressed in the form of a new binding cyber treaty, a code of conduct or a voluntary set of commitments. The idea of a new binding international instrument is very contentious and has been rejected by several states, mostly based on disagreement with the Sino-Russian proposal for a new treaty.[170] However, the call by the UN Secretary General for an accountability mechanism could be connected to another proposal made in the same Policy Brief regarding declaring the 'infrastructure essential for public services and to the functioning of society' as off-limits to malicious cyberactivity.[171] Although states made similar commitments in the UN GGE and OEWG, there has been little change in their behaviour and critical infrastructure continues to be one of the main targets of malicious cyber operations.

[169] For an example, see the CISA's Cyber Safety Review Board: https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb.
[170] It needs to be noted, however, that in recent years China has distanced itself from the proposals made by Russia. It has not joined in submitting the updated concept of the convention on ensuring international information security nor the concept paper on a permanent decision-making OEWG on security of and in the use of ICTs.
[171] United Nations (2023).

The new accountability mechanism could take two possible forms. It could be a formal body established to implement the provisions of a new legal document: a 'Critical Information Infrastructure Protection Treaty' (C2IP) or a 'Code of Conduct for Critical Information Infrastructure Protection' (3C2IP). Contrary to the arguments about potentially too broad a scope for negotiations of such a new instrument, the focus on the critical information infrastructure could build on the extensive body of national and international policy and regulatory instruments addressing this topic. There is also a significant acquis in the existing UN GGE and OEWG reports. If based on an internationally binding document, such an accountability mechanism could not only issue reports linked to specific incidents but be endowed with specific investigatory powers similar to those exercised by prosecutors or advocates general in the existing judicial bodies. A less ambitious alternative would be a Review Board established to deal with cases of attacks on critical information infostructure. This proposal is similar to the Cyber Incident Review Board discussed in the previous section.

These are of course just two ideas that ultimately may take completely different shape or not materialise at all. However, the main point here is that the discussion about accountability at the UN does not need to involve conversation about attribution. On the contrary, by avoiding the 'attribution curse' altogether, they offer multiple options for the UN to add value in the ongoing efforts to strengthen accountability in cyberspace.

6.2 A 'whole-of-UN approach' to accountability based on the existing institutions

An alternative – or complementary – approach to establishing a UN-driven cyber accountability mechanisms is to adopt a systems view whereby rather than creating a single body, the Secretary General strengthens the existing structures to benefit from their mandates, procedures, processes, resources and know-how developed over the decades dealing with different complex issues. Such an approach would not necessarily require a centralised body. Instead, it would rely on clearly prescribed expectations of each body within the UN system based on a mapping exercise of the accountability mechanisms conducted by the UN Joint Inspection Unit (JIU).[172] A similar review has been undertaken by the JIU to take stock of cybersecurity in the UN system organisations.[173] Given the highly political nature of this debate, such mapping could be accompanied by an internal reflection conducted under the leadership of the UN Under-Secretary-General for Political and Peacebuilding Affairs and the High Representative for Disarmament Affairs. The mapping exercise would allow for a clear identification of the added value that different bodies within the UN system bring to the promotion of accountability,

[172] See United Nations Joint Inspection Unit of the United Nations System: https://www.unjiu.org/.
[173] Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy (2021) *Cybersecurity in the United Nations system organizations*, Report of the Joint Inspection Unit, March. Available at: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf.

including ITU or international complaint mechanisms established under international human rights treaties.[174]

The 'whole-of-UN approach' to cyber accountability could be expanded to include other organisations with which the UN has concluded cooperation agreements. The UN and World Bank concluded a cooperation agreement that identifies the Bank as a specialised agency as defined by the Charter of the United Nations.[175] The agreement states that 'the United Nations and the Bank shall consult together and exchange views on matters of mutual interest', which could include accountability in cyberspace. As discussed earlier, the World Bank Inspection Panel might play an important role in strengthening positive accountability in cases of projects focused on CCB. Interestingly, the agreement also authorises the Bank to request advisory opinions of the International Court of Justice on any legal questions 'arising within the scope of the Bank's activities other than questions relating to the relationship between the Bank and the United Nations or any specialized agency'.[176] The UN has also concluded a Relationship Agreement with the ICC,[177] which in light of the recent declarations of the Prosecutor opens the possibility for a deeper engagement in the context of cyber accountability.

The 'whole-of-UN approach' resulting from the engagement across the UN system is no doubt a less elegant solution than the establishment of a new mechanism. However, its reliance on the existing structure that member states are familiar with and know how to navigate offers a clear advantage and allows avoidance of debates about the need for a new mechanism altogether. The advantages of such an approach are also the existing mechanisms for multistakeholder cooperation and engagement that have been developed and practised, without necessarily embarking on difficult discussions about the modalities for involving the private sector or civil society organisations.

[174] United Nations Human Rights Office of the High Commissioner (2013).
[175] See "International Bank for Reconstruction and Development Agreement between the United Nations and the International Bank for Reconstruction and Development". Available at: https://thedocs.worldbank.org/en/doc/877831508427688702-0290022017/render/AgreeementbetweentheUnitedNationsandIBRD1947.pdf.
[176] International Bank for Reconstruction and Development Agreement.
[177] See "Negotiated relationship agreement between the International Criminal Court and the United Nations". Available at: https://legal.un.org/ola/media/UN-ICC_Cooperation/UN-ICC Relationship Agreement.pdf; *Best practices manual for United Nations – International Criminal Court Cooperation*. Available at: https://legal.un.org/ola/UNICCCooperation.aspx.

Figure 3. Accountability within the UN system

6.3 An accountability system beyond the UN

The most comprehensive accountability system is one that combines different mechanisms across various overlapping policy regimes that together constitute a cyber regime complex.[178] Bringing several accountability elements and mechanisms from different policy areas has clear advantages. It allows for flexibility in the use of different mechanisms and as such addresses political sensitivities associated with accountability debates.

Many of those issues can be also pursued simultaneously through different regimes: human rights, trade, security. This approach would be the most inclusive and open in terms of engagement with the multi-stakeholder community and would benefit from the role that the private sector and other actors play as accountability holders. For instance, in the case of grave violations of human rights online, flexibility within the system gives any state the choice of instruments such as debate in the Human Rights Council as opposed to a fully fledged investigation. Violations of the framework of responsible state behaviour can be addressed through ad-hoc coalitions of actors or brought for debate at the UNSC. States also recognise the role of the WTO as the only legitimate forum to clarify and resolve trade-related disputes, including a potential role of cybersecurity strategies as a technical barrier to trade.[179]

However, the complexity of this system is its clear disadvantage, as it may require significant investment of resources, both human and financial, or lead to accountability and legitimacy debates.[180] Some states – especially the less resourced ones – are already criticising the multiplication of venues for debates about cyber matters, which makes it difficult for them to contribute. Nonetheless, opening up the black box of accountability in cyberspace allows for more creative thinking about accountability and exploring options beyond the UN-mandated solutions. For instance, members of the African Union may decide to reduce their political dialogue with the EU or any other actor should they consider its policies harmful for their states and citizens. Sending a political signal undoubtedly constitutes a form of sanction and pursual of accountability: one that is unavailable if accountability is conceptualised too narrowly.

[178] Hofmann and Pawlak (2023).
[179] See for instance: WTO (2017) Members debate cyber security and chemicals at technical barriers to trade committee, 14-15 June 2017. Available at: https://www.wto.org/english/news_e/news17_e/tbt_20jun17_e.htm; WTO (2018) Communication from the United States "Measures adopted and under development by China relating to its cybersecurity law", S/C/W/376, 23 February 2018. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=243365,243385,243363.
[180] Julia Black (2008) "Constructing and contesting legitimacy and accountability in polycentric regulatory regimes", *Regulation & Governance* 2: 137-64. Available at: https://doi.org/10.1111/j.1748-5991.2008.00034.x.

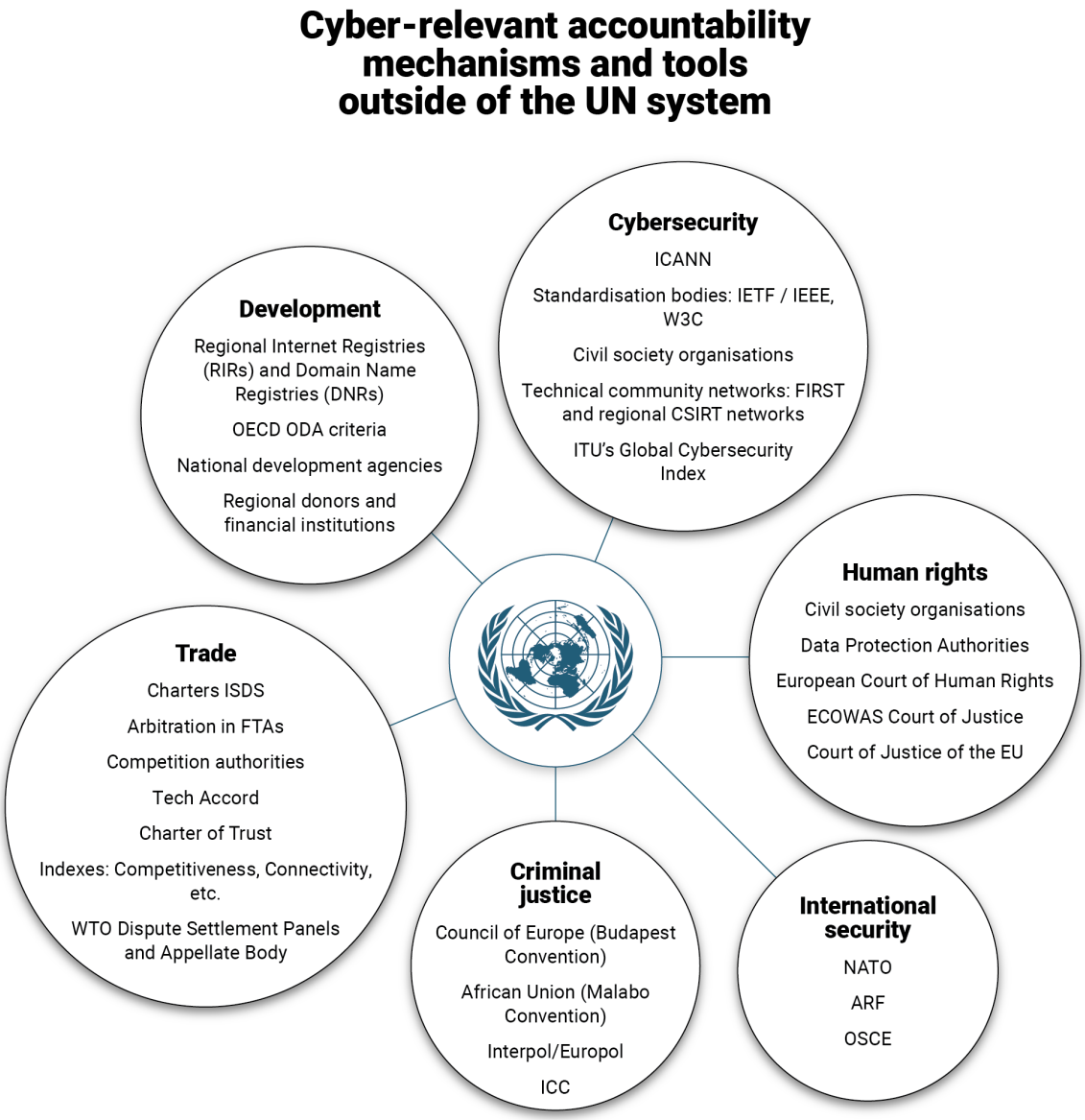


Figure 4. Accountability mechanisms and tools outside of the UN system

About the author

Patryk Pawlak is a visiting scholar at Carnegie Europe and a part-time professor at the Robert Schuman Centre for Advanced Studies at the European University Institute in Florence. He is also project director of the Global Initiative on the Future of the Internet funded by the European Union. In December 2023, Pawlak was appointed to the UN Advisory Board on Disarmament Matters and the UNIDIR Board of Trustees.

Prior to joining Carnegie Europe, Pawlak worked for the EU Institute for Security Studies where he headed the Brussels office and coordinated cyber and digital activities. Until December 2022, Pawlak was the project director of EU Cyber Direct, an EU-funded initiative to support the bloc's engagement on cyber diplomacy and digital policies worldwide. In this capacity, he ideated and coordinated the European Cyber Diplomacy Dialogue, bringing together senior government officials and scholars.

Dr Pawlak's fields of expertise include global governance of cyberspace, cyber capacity building, the impact of technology on foreign and security policy, and the EU's cyber and digital diplomacy.

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.