Check for updates

Received: 27 June 2023 | Revised: 17 October 2023 | Accepted: 24 October 2023

DOI: 10.1111/1758-5899.13302

SPECIAL SECTION

The pursuit of positive accountability in the cyber domain

Patryk Pawlak

European University Institute, Fiesole, Italy

Correspondence
Patryk Pawlak, Robert Schuman Centre for Advanced Studies, European University Institute, Via dei Roccettini, 9 50016 San Domenico di Fiesole, Italy.
Email: patryk.pawlak@eui.eu

Abstract

Debates about accountability in cyberspace are dominated by state-centric and security-driven approaches that disregard the complexity of the institutional ecosystem in cyberspace and the diverse ways through which different stakeholder groups may pursue accountability. Such an approach has contributed to a flawed interpretation of accountability in cyberspace as applicable solely to malicious actors who need to be punished for their actions. Despite greater policy and research attention to this line of reasoning, holding states accountable for their behaviour has yielded limited results due to the legal, political and technical complexities. At the same time, the non-malicious activities in cyberspace that might have unintended negative effects remain exempted from scrutiny. Cyber capacity-building activities, which aim at supporting governments and societies in strengthening their cyber resilience, illustrate this point well. This article introduces the concept of positive accountability to describe accountability for actions that are not malicious in their intent. It argues that the anticipatory potential of mechanisms like deliberation, joint problem-solving, interactive learning and competition plays an important role in strengthening accountability by eliminating or minimising any unintended or undesired spillovers. It concludes with a proposal that broadly defined capacity building might also be considered a form of anticipatory and deliberative accountability mechanism.

1 | A MISSING PIECE: POSITIVE ACCOUNTABILITY IN CYBERSPACE

Is accountability in cyberspace attainable? What are the accountability standards, sanctioning mechanisms and enforcement tools in the cyber domain? Diplomats and researchers raise these questions primarily in relation to malicious cyber operations launched by one state against another: Chinese cyber espionage operations in the United States, Russian attacks on critical infrastructure in Ukraine, or North Korean ransomware campaigns launched to evade international sanctions. All of these are united by the state-victim feeling of injustice and the desire of the international community to end the impunity of the attackers.

Consequently, most research and policy analysis on the topic remain rather state-centric and focus on accountability for malicious actions that violate the agreed norms of responsible state behaviour or existing international law. In this article, imposing consequences for wrongdoing and violations of agreed standards is referred to as negative accountability. Driven by the legal debates about state responsibility in cyberspace (Buchan & Tsagourias, 2016) and limitations of the self-help mechanisms stemming from the challenge of attribution (Crootof, 2018), the existing state-centric research leaves us convinced that negative accountability is all that matters but is ineffective without sustained engagement and imposition of consequences (Lewis, 2022). Most analysis remains silent about the fact that while governments may call for more accountability in cyberspace, they avoid any clear references to accountability for their actions given the primarily voluntary and non-binding nature of current commitments. One would be hard-pressed to find any references to accountability mechanisms in national statements or UN reports on cyber issues.

The problem with the prevailing state-centric and security-driven approach to accountability in cyberspace is that it disregards the institutional complexity of the cyber

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2023 The Authors. *Global Policy* published by Durham University and John Wiley & Sons Ltd.

ecosystem, which also includes the private sector, multilateral donor institutions and international and regional organisations (Wolfe, 2015; Woods & Narlikar, 2001), and diverse ways through which different stakeholder groups may pursue accountability (Buchanan & Keohane, 2006; Grant & Keohane, 2005). Such negligence has contributed to a flawed interpretation of accountability, whereby only malicious actors should be held accountable for their actions. Consequently, most policy and academic debates have focused on accountability for bad behaviour, albeit without satisfactory results.

The focus on negative accountability is in contrast with an almost absolute silence regarding accountability of different actors for actions that are not malicious but nonetheless have unintended adverse effects on other countries, institutions or groups. This article argues that such actions and behaviour should not be excluded from scrutiny and introduces a new concept of positive accountability as the way to differentiate from malicious actions. For instance, traditional development agencies (e.g., USAID and JAICO), specialised UN agencies (e.g., ITU), regional organisations (e.g., EU, Council of Europe, African Union and RECs, ASEAN and OAS), and numerous private sector and non-governmental organisations are involved in cyber capacity-building (CCB) initiatives to strengthen legal, institutional or human capacities of countries with inadequate cyber resources. Although well-intended, these activities may have significant effects on national power structures, legal frameworks and societies at large. Currently, the accountability of the funders or implementors in such cases is rarely discussed. For instance, the support provided to a country to develop new cybercrime legislation may give more powers to law enforcement but without strengthening checks and balances mechanisms that would protect civil society organisations or human rights defenders.

The absence of the debate about positive accountability is unfortunate, given the overall importance of properly designed and implemented CCB initiatives. A more rigorous pursuit of positive accountability offers a twofold benefit. On the one hand, more effective positive accountability in CCB contributes to strengthening cyber resilience and reduces vulnerabilities in cyberspace. As a matter of fact, the only time when the UN reports explicitly refer to accountability is in the section on cyber capacity building (United Nations, 2021). On the other hand, stronger cyber resilience achieved thanks to more disciplined approach to positive accountability of the funders and implementors for their CCB actions ultimately increases the costs of engaging in malicious activities by state actors or their proxies who need to invest additional resources in more sophisticated tools to be effective. In that sense, the focus on positive accountability might be seen as a way to overcome some of the challenges associated with the pursuit of negative accountability.

Identifying new approaches to accountability in cyber capacity building is important for many reasons. First, funding for such projects and initiatives is increasing and comes from many—sometimes competing—sources. This raises questions about the efficient use of the resources, the sustainability of the undertaken actions and the real motivations of the funders (Pawlak, 2016). Second, the differences in policy objectives and approaches of the 'capacity-builders' turn the CCB engagements into yet another domain for competition that is driven by the funders' individual interests rather than the long-term benefits for those whose capacities are being built. Finally, the evolving nature of cyber threat landscape means that there is no one clear standard for cybersecurity. While there are certain good practices and technical benchmarks, donors usually have very little control over the off-the-shelf technology that is provided by the private sector. There is also no one-size-fits-all regulatory or institutional set-up. This raises questions about the donors' accountability for the solutions proposed as part of their CCB initiatives.

Against this background, the question of *who* is accountable *to whom* and *for what* in cyberspace requires a more dynamic and differentiated approach. Building on the theoretical foundations and proposals by Eilstrup-Sangiovanni and Hofmann in the opening to the Special Section, this article focuses on positive accountability in an institutionally dense governance setting of cyber capacity building. In contrast to the existing research focused on negative accountability of states, it looks at the roles of other actors in this domain, especially development agencies, regional organisations or international bodies. The article argues that the anticipatory potential of mechanisms like deliberation, joint problem-solving, interactive learning and competition plays an important role in strengthening accountability by eliminating or minimising any unintended or undesired spillovers. The article concludes with a proposal that broadly defined capacity building might also be considered a form of anticipatory and deliberative accountability mechanism.

2 | ACCOUNTABILITY GAPS IN A DENSE CYBER INSTITUTIONAL ENVIRONMENT

The almost exclusive focus on accountability in cyberspace through the prism of international security fails to capture the dynamic ecosystem of stakeholders involved in the governance of cyberspace (Decker et al., 2023). Different policy communities and organisations acknowledge the need to strengthen the institutional environment, regulatory frameworks and human capacities to address negative externalities resulting from the progressing digital transformation and connectivity, including the fight against cybercrime or strengthening

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

cyber resilience structures and mechanisms. The lack of capacities in certain countries to effectively address cybersecurity challenges provides an impulse for the growth in technical assistance and capacity building in this domain. Progressively, specialised organisations (Interpol, International Telecommunication Union—ITU, UN Office on Drugs and Crime—UNODC), regional organisations (e.g., Council of Europe—CoE, European —EU, Organization of American States—OAS, Economic Community of West African States—ECOWAS) and multistakeholder platforms (e.g., Global Forum on Cyber Expertise—GFCE) have become critical actors for the design and implementation of CCB programs.

The field of cyber capacity building has grown significantly over the past 20 years in terms of the number of initiatives (more than 1000 projects), participating organisations (over 657) and policy communities involved (Collett & Barmpaliou, 2021a). At the core of this dense institutional environment are the 'parent communities' specialised in justice, incident management, foreign policy, human rights and development (Collett & Barmpaliou, 2021b). To respond to the growing phenomenon of cybercrime and prevent the emergence of safe havens for cybercriminals, Interpol, UNODC, CoE, OECD and G8 have gradually embraced CCB as part of their mandates. The development community introduced CCB as an element of a de-risking strategy for their digital transformation programs (World Bank, 2016). Some notable examples include the adaptations in the World Bank's Digital Development Partnership Fund or the EU's Digital for Development Hub initiative. The diplomatic community has also invested resources in improving states' capacities to meet their commitments under the UN framework for responsible state behaviour, including the implementation of the agreed norms, rules and principles.

As Eilstrup-Sangiovanni and Hofmann observe, in such a complex institutional environment, determining who is accountable to whom, for what and according to what standards becomes difficult. But a failure to scrutinise actions of individual organisations despite this density and complexity carries serious implications for accountability that is diffused among many organisations and dispersed at many organisational layers (Pawlak & Barmpaliou, 2017). First, the CCB interventions undertaken by external actors have wide-ranging legal, institutional, political and societal effects on the domestic audiences and power structures. A CCB initiative focused on strengthening institutional capacities of an intelligence agency or a ministry of defence might adversely affect power structures between civilian and military actors. A legislative reform that does not include human rights safeguards might lead to unjustified indiscriminate online surveillance. A training programme provided to law enforcement agencies without equivalent attention to reinforcing the independence of the judiciary branch might adversely affect the rule of law in that country. The promotion of specific technological solutions without adequate investment in strengthening human capacities through training might ultimately make a society more vulnerable by creating negative security externalities. The reliance of the donor agencies and institutions on external contractors and consultants with different motivation, including the private sector, methods and working modalities without proper monitoring mechanisms creates additional risks.

Second, since its introduction on the policy agenda, CCB has evolved from a neutral tool of international development cooperation to a strategically deployed instrument of foreign and security policy (Pawlak, 2016). The expanding number of IOs involved in CCB has created opportunities for states and other stakeholders to engage in forum shopping or regime shifting in the search of a venue that best serves their policy goals. For instance, the EU prefers to partner with the Council of Europe for cybercrime initiatives due to the higher human rights and rule of law standards that the CoE promotes, including through the Budapest Convention. Since the establishment of the EU-funded Global Action on Cybercrime (GLACY) initiative, the Council of Europe's engagement in CCB increased significantly, and its international standing improved in comparison with other organisations like ITU or UNODC. Russia and China, on the contrary, prefer to promote UN agencies as the primary vehicle for CCB initiatives, which strengthens the state-centric model of cyberspace governance. Both were the main drivers behind the ITU's Global Cybersecurity Agenda (GCA) as a platform for partnerships with other IOs, such as INTERPOL, ECOWAS or UNODC. The ITU's capacity-building assistance—offered without any conditionality (Ma, 2020)—makes it more difficult for the EU and other donors to link CCB to human rights protection or anti-corruption (Milanovic, 2021). To limit dependence on Western financial institutions, China also launched the Digital Silk Road initiative and created the Asian Infrastructure Development Bank (AIDB) to fund it its digital investment projects.

Third, the increasing geopolitical polarisation has translated into the political instrumentalisation of cyber capacity building, to the detriment of well-established principles adopted to ensure the effectiveness of international development cooperation (e.g., the Busan Partnership for Effective Development Cooperation and the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building). Clashes over the competing visions of cyberspace, such as the sovereign rights of states in governing their cyberspace or the role of non-governmental stakeholders in that respect, have adversely impacted the commitment to principles such as inclusive partnerships, sustainability or transparency. Driven by political considerations, donors tend to favour some countries over others, leading to new

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

digital divides. For instance, in the last 2 years, several donor countries have shifted their funding towards Ukraine and limited their engagement in other parts of the world. The lack of coordination and competition among donors has also resulted in duplication of efforts and inefficient use of resources for donors, which in turn creates absorption challenges for recipient countries. For instance, 16 different actors have been responsible for 42 projects implemented in Ghana, with several of them focusing on cybercrime, crisis management or cyber diplomacy (Global Forum on Cyber Expertise, 2023). The efforts undertaken to remedy the situation might also have adverse effects. Tools like the ITU's Global Cybersecurity Index or the Cyber Maturity Model (CMM) for needs assessment by the Oxford University might be instrumentalised by governments to legitimise politically driven institutional reforms or policy adaptations. In both cases, the information generated for the purpose of the assessment is often kept away from the public eye, which complicates scrutiny and accountability. For instance, limited transparency of the CMM-based maturity assessments makes it impossible to scrutinise the landing decisions of the World Bank, who relies on this tool when considering its engagement options with client countries.

Against this background, the utility of traditional accountability mechanisms for standard-setting, monitoring and sanctioning in CCB is weak. Firstly, there is no universal standard for different actors to follow; there is no single definition of what a successful CBB initiative looks like. Instead, development actors define a theory of change behind their CCB engagements and provide the parameters to the project implementors. However, because a desired impact can rarely be achieved and attributed to a single intervention, both donors and implementors can ultimately avoid accountability. Secondly, the absence of proper monitoring mechanisms may lead to divergent or conflicting outcomes, even when the overall objectives of different interventions are similar. For instance, the Global Action on Cybercrime Extended (GLACY+) by the Council of Europe defines its desired impact as strengthening the capacities of states worldwide 'to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area' (Council of Europe, 2022). The standard applied by the CoE is provided by the Budapest Convention on Cybercrime. However, some of the GLACY+ priority countries—Benin, Cabo Verde, Ghana and Senegal—have also ratified the Malabo Convention of the African Union, which provides a lower standard in the same policy domain (Council of Europe, 2016). Finally, the sanctioning possibilities are weakener when the pool of possible project implementors is limited or when the implementors are large international organisations. For instance, the EU-funded HIPSSA and HIPCAR projects implemented by the ITU in the Sub-Saharan Africa and the Caribbean have developed cybercrime model laws in clear contradiction to the provisions of the Budapest Convention (ITU, 2012; ITU, 2013) and the objectives of the GLACY project. Despite that, the options for the EU to hold ITU accountable—or for others to hold the EU accountable for undermining its own policies—were very limited.

3 | THE PROMISE OF PLURALIST ACCOUNTABILITY MECHANISMS

States acknowledge that CCB should be 'evidence-based, politically neutral, transparent, accountable, and without conditions' (United Nations, 2021), but there is not yet consensus on what implementing these principles would mean in practice. This is due to the fact—as noted by Eilstrup-Sangiovanni and Hofmann—that organisations in governance complexes do not operate in isolation, and their performance needs to be assessed considering a broader environment and relationships. Consequently, understanding pluralistic models of accountability in CCB is critical.

In a highly polarised international environment, the competition for resources, visibility and authority turns IOs into the venues where existing standards are being contested, defended or new ones are developed. The overlapping competences of the IOs are used as vehicles for diffusing such (rival) standards. The set of confidence-building measures in cyberspace, first developed at the regional level by the OSCE, was subsequently adopted at the United Nations, making them a global standard referred to by other IOs like the OAS or the ASEAN. The Code of Conduct developed by the Shanghai Cooperation Organization as a blueprint for a new UN cyber treaty was less successful in promoting concrete standards but was useful in promoting the need for new legal standards as opposed to existing international law. To counter this narrative and to defend the existing standard, several individual donors (e.g., Australia, Canada, Netherlands, Switzerland and Singapore) and regional organisations (e.g., EU, OAS and ASEAN) use trainings and workshops on the application of the existing international law in cyberspace.

A dense institutional environment also makes monitoring more complicated. The example of HIPSSA and HIPCAR projects shows clearly how the lack of proper monitoring mechanisms and the lack of self-monitoring by the EU have led to conflicting outcomes and undermined the EU's own position on the Budapest Convention. The challenge for monitoring CCB initiatives is the limited transparency and information-sharing in this field. Cybil Portal—an online repository for international CBB projects launched by the GFCE—is a good illustration of the problem. Cybil Portal currently contains 868 projects involving 858 actors globally. However, incomplete information provided by different actors makes proper monitoring and

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

pursuit of accountability very difficult. For instance, of the eight projects listed under the Solomon Islands, none contains information about the amount of funding or the standards against which these initiatives will be assessed. The situation with defence-oriented CCB actions in Moldova, Georgia or Ukraine is even more problematic.

Finally, sanctioning in complex settings of CCB is equally difficult. As mentioned earlier, the presence of several donors in the same country makes assigning responsibility difficult and gives donors and implementors operating in a specific context an opportunity to shift the blame. In the case of Samoa Islands, the involvement of the ITU and the Commonwealth Telecommunications Organization gives them an opportunity to blame each other for a failure in delivering promised outcomes. In the context of CCB where international donors rely on a limited number of implementors with the desirable expertise and resources, the risks of one organisation sanctioning another are very low. Despite the adverse effects of the project implemented by ITU, the EU continues to use the organisation for the implementation of its digital and cyber-related projects. Therefore, the 'exit' possibilities are more limited in the context of policy areas where despite institutional density, the specific expertise is scarce and distributed among a limited number of organisations. In such cases, the reliance on public forms of accountability becomes crucial.

Given these limitations, can pluralist mechanisms yield better results for positive accountability or at least unlock the dormant potential of certain existing processes in the cyber domain?

The multiplication of venues for discussing commitments and responsibilities of different stakeholders in the cyber domain—including multistakeholder initiatives like the Paris Call for Trust and Security in Cyberspace or the private sector-driven Tech Accord—has made accountability through deliberation particularly attractive. In the UN context, the establishment of the Open-Ended Working Group (OEWG) dealing with cyber issues has not only democratised the debate but also provided opportunities for states to call out violations of the framework of responsible state behaviour in cyberspace. The shift from a closed setting of the UN Group of Governmental Experts (GGE) to an open platform for deliberation among all UN members and with the involvement of the non-governmental actors has significantly improved transparency. Even though explicit references to accountability are rarely made in the OEWG meetings, it has become a platform used by governments, the private sector and civil society organisations to debate standards and communicate their expectations regarding accountability. For instance, Russia insists on agreeing 'a comprehensive universal list of rules, norms and principles of responsible behavior and make them legally binding' (United Nations, 2023a). Following the adoption of the Annual Progress Report in July 2022, Russia stated that it 'does not consider itself bound even by voluntary commitments stemming from those provisions of the report that contradict [their] legislation and national interests' (United Nations, 2023b). On other occasions, in an effort to clearly link a state's level of cyber capacities to its international obligations and accountability, Egypt and Venezuela have proposed the concept of 'shared but differentiated responsibility' used so far in the environmental protection domain. In some cases, these expectations are incorporated in the OEWG consensus report, which in the past laid down specific principles and goals for cyber capacity building (UN, 2021). The involvement of international and regional organisations (e.g., EU, OAS, OSCE, ASEAN and ICRC) in the UN debates has resulted in proliferation of the accountability standards beyond the UN. For instance, OSCE, G7, AU, OAS and ASEAN have all committed to support the implementation of the UN norms. As such, the OEWG is an example of joint standard-setting and harmonisation of rules for responsible state behaviour in cyberspace based on deliberation and mutual transparency.

Interactive learning is another promising avenue for strengthening positive accountability, especially in the context of cyber capacity building. With standards of cyber capacity building clearly depending on the national policy context, local ownership and sustainability of the implemented actions, sharing good practices and lessons learned related to needs assessments, risk management or specific regulatory and institutional solutions has proven to be particularly relevant. For instance, OAS, EU and ITU have all produced guides with best practices and lessons learned concerning the development of the national cybersecurity strategies or establishment of the Computer Emergency Response Teams (CERT). In addition, different IOs and coalitions of states are engaged in exercises aimed at strengthening their preparedness to deal with cyber crisis. Around 40 like-minded countries regularly engage in tabletop exercises and scenario-based discussions aimed at improving their collective capability to act jointly, including issuing attribution statements to make perpetrators accountable (EEAS, 2021). The post-exercise reports and lessons learned are used to monitor progress. Indirectly, such initiatives may serve to hold states accountable for negligence or the lack of implementation of international commitments. Accountability through mutual learning and more transparency can be also achieved with technocratic processes such as the establishment of repositories of capacity-building needs proposed by Brazil in the context of the UN negotiations of a new cybercrime convention, the national survey for the implementation of the UN framework of responsible state behaviour proposed by Australia and Mexico, or different indexes and rankings such as the ITU's Global Cybersecurity Index or the Estonian National Cyber Security Index.

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Finally, competition among different organisations with overlapping competences stimulates monitoring and transparency, ultimately providing more opportunities for accountability and preventing the emergence of competing standards. In the context of the UN, the establishment of the GGE and OEWG with identical mandates and tasked to produce consensus reports has resulted in informal and interactive peer-review mechanisms. Chairmen of each group have used informal channels to exchange information that helped to avoid diverging standards around the framework of responsible state behaviour in cyberspace. In the field of CCB, the competition between China's Digital Silk Road initiatives, the EU's Global Gateway and the US-led OECD-coordinated Blue Dot Initiative have also triggered mutual informal oversight mechanisms. For instance, the United States clearly points out the risks to freedoms and long-term security implications associated with the use of the Chinese-manufactured digital technologies promoted through the Digital Silk Road. Such publicly expressed positions increase awareness among the less powerful and technology-dependent countries who might use this information and exit a risky relationship. It also creates a push for more transparency that strengthens monitoring and accountability. In response to the criticism from the US and other countries, Huawei has opened six Cyber Security and Privacy Protection Transparency Centers around the world. Competition might also serve as a form of accountability in cases where organisations attempt to expand their mandates without explicit permission from the accountability holder. For instance, the ITU's attempt to expand the scope of GCA into the field of cybercrime was criticised by the Council of Europe and opposed by the United States and the EU.

4 | CONCLUSIONS

The exclusive attention to standards, attribution and sanctions in negative accountability debates has resulted in very little progress in the discussion about accountability in cyberspace. Rather than helping to find a comprehensive answer to who is accountable to whom and for what, it has created de facto immunity for a large group of actors operating in the dense cyber ecosystem. Unilateral cyber sanctions regimes adopted by the EU, US, UK, Australia and South Korea, and the collective attribution statements calling out violations of agreed norms and international law, have provided only partial satisfaction for the more hawkish observers. However, given the profound legal, institutional, political and societal implications that CCB interventions by international and regional organisations might have, the debate about accountability in cyberspace needs to embrace different dimensions of positive accountability.

The multiplication of donors and initiatives that pursue similar goals in an uncoordinated way leads to dispersed accountability that makes it difficult to answer who is responsible, for what and to whom. Pluralist accountability through deliberation, learning and competition may be a useful alternative to traditional, more static and backward-looking methods. However, one also needs to acknowledge that in certain policy areas where states still play a dominant role—especially in the context of international security—such novel approaches may not work. The case of accountability for cyber-attacks against the critical infrastructure in Ukraine and the hack of the German Parliament demonstrates the continued prevalence of traditional approaches. Although states have been debating different ways to hold the perpetrators of cyber-attacks accountable—including through collective attribution statements, targeted sanctions against individuals or entities involved, or the exclusion of certain technology providers from the market—anything short of a counter-cyber operation that would switch off the lights in Saint Petersburg or Pyongyang seems insufficient.

The discussion in this article also suggests that capacity building itself may be considered a mechanism for anticipatory and pluralist accountability. This proposal complements the mechanisms proposed by Eilstrup-Sangiovanni and Hofmann. Capacity building as a pluralist accountability mechanism might be particularly relevant to ensure that international organisations do not serve only as 'talk shops' but are used to deliver concrete outcomes. In that sense, international organisations can be held accountable for the progress (or lack thereof) towards the goals they set for their members. For instance, states at the UN have agreed to abide by a set of non-binding and voluntary norms which create concrete obligations. They are expected, among others, not to allow their territory to be used for cyber-attacks against any other state. This commitment assumes a certain level of institutional, regulatory and human capability that not all countries possess. Capacity building plays a particularly important role where the gaps between commitments and actual capacities exist. Whereas the ultimate responsibility lies with individual states under the due diligence principle, one could also argue that the UN and regional organisations are partly responsible, and ought to be accountable, for the progress made by its members towards this shared goal. Such an approach might be particularly suitable in the field of international security (e.g., counterterrorism, maritime security and crime) where states constantly use international organisations to make commitments. Further analysis into this accountability mechanism would also need to investigate how the concepts such as the 'common but differentiated responsibility' would ultimately impact their implementation.

Finally, to push the accountability agenda forward, future research might explore the friction between the

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

promise of more accountability through centralisation and democratisation of the deliberative processes in universal membership organisations like the UN, on the one hand, and more decentralised approach to accountability in a dense institutional environment, on the other hand. While many countries view the UN as a guarantor of equal access to the decision-making structures where they can voice their concerns (a strong argument for deliberative accountability mechanism), they should also be concerned about the limited ways to holding the UN accountable for its failure to deliver on those expectations. In that sense, the proposals made by some countries to give the UN a central coordinating role for CCB might further weaken accountability in this domain. As the developments to date have demonstrated, pluralist accountability through deliberation, learning and competition in a dense institutional environment might work just fine.

ACKNOWLEDGEMENTS

The author would like to express gratitude to Stephanie Hofmann, Mette Eilstrup-Sangiovanni, and the anonymous reviewers for their insightful comments. This article has also benefited from the discussions during workshops on accountability in cyberspace hosted by the Hague Program on International Cyber Security and the Stimson Center.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

REFERENCES

Buchan, R. & Tsagourias, N. (2016) Non-state actors and responsibility in cyberspace: state responsibility, individual criminal responsibility and issues of evidence. *Journal of Conflict and Security Law*, 21(3), 377–381.

Buchanan, A. & Keohane, R.O. (2006) The legitimacy of global governance institutions. *Ethics and International Affairs*, 20(4), 405–437.

Collett, R. & Barmpaliou, N. (2021a) *Annex 3. Notes on cyber capacity building funders*. European Commission.

Collett, R. & Barmpaliou, N. (2021b) *International cyber capacity building. Global trends and scenarios*. European Commission.

Council of Europe. (2016) *Comparative analysis of the Malabo convention of the African union and the Budapest convention on cybercrime*. 20 November 2016. Council of Europe.

Council of Europe. (2022) *Global action on cybercrime extended. Project summary*. 10 February 2022. Council of Europe.

Crootof, R. (2018) International Cybertorts: expanding state accountability in cyberspace. *Cornell Law Review*, 103(3), 565–644.

Decker, D., Rauhut, K. & Pytlak, A. (2023) Fostering accountability in cyberspace. The Stimson Center. 3 July 2023. Available from: https://www.stimson.org/2023/fostering-accountability-in-cyberspace/. [Accessed 30 September 2023].

European External Action Service. (2021) Cyberspace: strengthening cooperation in promoting security and stability. 17 May 2021.

Global Forum on Cyber Expertise. (2023) *Cyber capacity knowledge portal*. Available from: https://cybilportal.org/. [Accessed 30 September 2023].

Grant, R.W. & Keohane, R.O. (2005) Accountability and abuses of power in world politics. *American Political Science Review*, 99(1), 29–44.

ITU. (2012) Cybercrime/e-crimes: model policy guidelines & legislative texts. In: *HIPCAR – harmonization of ICT policies, legislation and regulatory procedures in the Caribbean*. Geneva: International Telecommunication Union.

ITU. (2013) Computer crime and cybercrime: southern African development community (SADC) model law. In: *HIPSSA – harmonization of ICT policies in Sub-Saharan Africa*. Geneva: International Telecommunication Union.

Lewis, J. (2022) *Creating accountability for global cyber norms*. 23 February 2022. Washington, DC: Center for Strategic and International Studies.

Ma, X. (2020) US-China competition in international development assistance. In: *Contemporary international relations 4*. Beijing: China Institutes of Contemporary and International Relations, pp. 109–117.

Milanovic, B. (2021) Competition can Be good for the developing world. *Foreign Affairs*, 21 May.

Pawlak, P. (2016) Capacity building in cyberspace as an instrument of foreign policy. *Global Policy*, 7(1), 83–92.

Pawlak, P. & Barmpaliou, N. (2017) Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy*, 2(1), 123–144.

United Nations. (2021) *Final substantive report of the open-ended working group on developments in the field of information and telecommunications in the context of international security*. New York: NY: United Nations.

United Nations. (2023a) *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*. 25 July 2023.

United Nations. (2023b) *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 2023.

Wolfe, R. (2015) An anatomy of accountability at the WTO. *Global Policy*, 6(1), 13–23.

Woods, N. & Narlikar, A. (2001) Governance and the limits of accountability: the WTO, the IMF, and the World Bank. *International Social Science Journal*, 53(170), 569–583.

World Bank. (2016) *World development report 2016: digital dividends*. Washington, DC: World Bank Publications.

AUTHOR BIOGRAPHY

Patryk Pawlak is a Visiting Fellow at the Robert Schuman Centre for Advanced Studies at the European University Institute and a Visiting Scholar at Carnegie Europe. Before that, he headed the Brussels office of the EU Institute for Security Studies where he was responsible for the Institute's cyber and digital projects. His research focuses on global governance of cyberspace and the European Union's cyber and digital diplomacy.

How to cite this article: Pawlak, P. (2023) The pursuit of positive accountability in the cyber domain. *Global Policy*, 00, 1–7. Available from: https://doi.org/10.1111/1758-5899.13302

17585899, 0, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.13302 by EVIDENCE AID - BELGIUM, Wiley Online Library on [05/12/2023]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License