



Task Force 7
Towards Reformed Multilateralism: Transforming Global
Institutions and Frameworks



A FRAMEWORK FOR THE GLOBAL GOVERNANCE OF PRIVATE CYBERSECURITY COMPANIES

July 2023

Shaun Riordan, Director of the Chair for Diplomacy and Cyberspace, the
European Institute of International Studies, Sweden

Mario Torres Jarrín, Director of the Institute of European and Human Rights
Studies at the Pontifical University of Salamanca, Spain


Alejandro Garofali Acosta, Deputy Director of the European Institute of
International Studies, Sweden

वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE



Abstract




P rivate cybersecurity companies (PCSCs) have developed cyber capabilities significantly greater than those of many governments, including members of the G20. These capabilities focus on protecting the computer systems of their clients and undertaking forensic investigation to attribute responsibility for cyberattacks. However, without proper oversight, such attributions may also exert unhelpful influence on governments, weakening their response to cyberattacks. While PCSCs currently limit their activities to passive cyber defence, the pressure to move into more active forms of cyber


defence could lead them to offering cyber offense capabilities to their public and private sector clients. This would pose serious threats to internet stability and international peace, and impact human rights, security, and the rule of law. The G20 should task a commission with exploring PCSCs' current and future activities, the need for regulation and how to strengthen government cybersecurity capabilities at the global level, particularly in developing countries. The commission's report should help the G20 develop a Cybersecurity Action Plan to promote responsible and accountable private cybersecurity practices.



The Challenge




1



P rivate Cybersecurity Companies (PCSCs) provide a wide variety of cybersecurity services to their private and public sector clients. This Policy Brief focuses on PCSCs offering system defence, vulnerability identification, and attribution services. These companies are analogous to private military security companies (PMSCs), although their cybersecurity capabilities exceed those of most national governments, including some members of the G20. This would not be true of the great majority of PMSCs. Despite the extent of their cyber capabilities, there are no international agreements that regulate the activities or monitor the performance of PCSCs. The biggest PCSCs are geographically concentrated in a small number of countries. Countries with limited cyber capabilities often feel compelled to contract PCSCs to ensure their own cybersecurity as well as that of their citizens. It also means handing over responsibility for their cybersecurity to companies based in, and regulated in foreign jurisdictions. Moreover, given the limited cyber capabilities of these countries, it could mean that they do not fully understand the implications of contracting foreign PCSCs or the vulnerabilities these can create.

PCSCs currently focus on two areas: building and monitoring cybersecurity architecture for their clients, and carrying out forensic investigations into cyberattacks. Although forensic investigations may help clients identify those responsible for attacks on their systems, major PCSCs generally investigate cyberattacks. PCSCs publicise forensic investigations, including the attribution of cyberattacks, mainly for marketing. These are ways by which they can advertise their forensic capabilities, but may cause problems for the governments on the receiving end of such cyberattacks.¹ There are no international agreements on the criteria for such forensic investigations or the degree of confidence a PCSC should have in its investigation before publishing its attribution. There are multiple reasons why governments may wish to avoid premature attribution for a cyberattack, including uncertainty about attribution or about possible retaliatory measures.² Publication of an attribution by a PCSC can force a government's hand, risking misattribution or unnecessary cyber escalation.³

At present, PCSCs largely restrict their activities to passive cyber defence, constructing cybersecurity systems for their clients and monitoring them for




possible incursions. More proactive measures are limited to trapping hackers within the systems under attack. Some PCSCs do carry out penetration attacks on clients' systems to identify vulnerabilities, but with the client's permission. However, as the economic and political costs of cyberattacks increase, PCSCs are increasingly under pressure to develop more proactive cyber defence. Active cyber defence seeks to identify potential hackers and launch pre-emptive cyberattacks against them. This is but a small step from active cyber defence to cyber offence.

For this reason, and to maintain the state's monopoly on cyber offence, many national governments prohibit the private sector from taking such pre-emptive measures. There are no international agreements to this effect, however. Some companies already provide 'consultancy services' to governments in cyber offence and cyber disinformation operations.⁴ Without any international regulation, there is a growing risk that PCSCs may begin offering cyber offence services, especially to those governments without their own cyber capabilities. This would not only risk increasing instability and

conflict within the cyberspace, but also cause similar problems of criminal responsibility and chains of command to those caused by PMSCs.⁵

Indeed, the superior cyber capabilities of PCSCs are a challenge to global governance. Given the geographical concentration of PCSCs, governments contracting their services are constrained in regulating their activities as they do not fall within their country's jurisdiction. The unregulated activities of PCSCs, driven by commercial rather than geopolitical concerns, carry risks of destabilising cyberspace, including through premature attributions of cyberattacks. The evolution of PCSCs to cyber mercenaries offering cyber-offence capabilities carry even greater destabilisation risks with potential spill-overs into the physical world. Without international regulation, PCSCs are a serious challenge to global governance and stability, analogous to PMSCs in the physical space, but with the difference in that their capabilities are far superior than many governments—a fact often poorly understood by their clients.⁶

In the last decade⁷ there has been some international multi-stakeholder initiatives that raise awareness on the



many vulnerabilities that unchecked PCSCs may pose for security in general. These include the Voluntary Principles Initiative and the International Code of Conduct Association – ICoCA, with its International Code of Conduct for Private Security Providers,⁸ and cybersecurity at large. Both the UN Guiding Principles on Business and Human Rights⁹ and the Voluntary Principles on Security and Human Rights¹⁰ provide frameworks for acceptable behaviour that are followed by some PMSCs. However, developments in cybersecurity, and future developments driven by AI and, possibly, quantum computing, escape the provisions of these principles. Issues such as attribution, for example, are not covered.

Moreover, the effectiveness of self-regulation has been questioned, including in the context of ICoCA. Not all PMSCs accept these codes

or principles, nor do all PCSCs. The challenges do not only relate to the behaviour of the companies. A crucial area of concern is governments hiring PCSCs for capabilities that they themselves do not possess, especially if such capabilities include cyber offence. An agreement among governments to limit the ways in which they interact with PCSCs, and the services they contract from them, may be more effective than another self-regulation agreement among the PCSCs themselves.


Despite these initiatives and those that some countries have developed as national regulations for international security companies (licensing and certification requirements, supervisory bodies and regulatory frameworks—all with limited effectiveness), no single global governance framework exists. This reveals the urgent requirement for high standards and effective oversight.



The G20's Role

2





The G20 brings together the leading economies of both the global North and the global South. Minimising instability in cyberspace, while maximising equitable access to the benefits of digital technologies, is in the interests of both North and South. Unregulated PCSCs risk escalating instability and conflict in cyberspace, particularly in complex


and conflict-affected environments. The concentration of PCSCs in the North could lead to a greater digital divide while increasing the dependency and vulnerabilities of South countries which lack their own cybersecurity capabilities. The economic focus of the G20 and its combination of global North and global South countries give it the heft to regulate PCSCs both economically and commercially, rather than geopolitically.



Recommendations to the G20

3





Both the current activities of PCSCs (especially attribution) and their possible future development could pose serious challenges to internet stability and international security. The increasing size and scope of ecommerce means that such developments would also have serious consequences for international trade and global economic development. Smaller governments with limited cybersecurity capabilities or understanding, especially in the global South, are particularly vulnerable. The key objectives for the G20 on cybersecurity should be enhancing the stability of cyberspace and reducing the digital divide between the South and the North as well as strengthening the position of South governments vis-à-vis PCSCs.

Given this scenario, it becomes imperative that the G20 establish a commission to examine the activities, future evolution, and potential regulation of PCSCs. The commission should form part of a broader G20 approach to cybersecurity, which should also include the behaviour of governments and the protection of citizens. Previous T20 Policy Briefs have made recommendations to this effect, including one by two of the

current authors, on Cyberdiplomacy in 2020¹¹ and Techplomacy in 2021.¹² Previous research work on international collaboration in cyberspace has largely underestimated the role of PCSCs.¹³ The commission should bring together academics, government representatives, the business community, and PCSCs for a multidisciplinary approach. The commission should be given the following tasks:

- Explore the activities of PCSCs and their international implications, especially the implications of their geographical concentration in the global North.
- Explore the asymmetries in cyber capabilities between PCSCs and governments, especially governments in the global South, and the extent to which this increases the cyber vulnerabilities of those governments.
- Assess the dangers of PCSCs issuing attributions for major cyberattacks, both for misattributions and cyber escalation.
- Assess the cyber defence capabilities of governments, especially those in the global South, in relation to the




capabilities of PCSCs and how the G20 could contribute in improving the understanding of cybersecurity matters and cyber capabilities among smaller governments. Establish benchmarks for good practices for smaller governments in hiring PCSCs.

- Evaluate the pressures in the industry to develop more proactive cybersecurity measures and assess the resulting changes in the practices of PCSCs. Assess the extent to which private companies are already collaborating with governments in cyber offence operations. Evaluate the dangers of PCSCs evolving into ‘cyber mercenaries’ selling cyber offence capabilities to governments and other clients and the implications this would have for cyber stability and broader international security.

The commission should be tasked with producing a report covering these issues for the G20. The first draft of the report should be submitted to the G20 at its meeting in 2024. Apart from the issues mentioned above, the report should also include:

- Recommendations on the international regulation of the existing activities of PCSCs.
- Recommendations on how the G20 should contribute to greater cybersecurity awareness and understanding among smaller countries, especially in the global South, including improving cybersecurity capabilities.
- Recommendations on the international regulation of future PCSC activities, especially to avoid or limit the emergence of ‘cyber mercenaries’ offering cyber offence capabilities to private or public sector clients.
- A draft guide of best practices for countries, especially in the global South, who are compelled to seek the expertise of PCSCs, especially foreign PCSCs, to enhance their national cybersecurity.

Based on the commission’s report, the G20 should develop a ‘Cybersecurity Action Plan.’ Its primary objectives should be to strengthen stability in cyberspace and ensure equitable



access to cybersecurity for all countries, especially those in the global South. The provisions on PCSCs should include:

- Proposals for enhancing collaboration among PCSCs, governments, and the G20.
- Proposals for the international regulation of PCSCs activities (this should include criteria for attribution of cyberattacks and the relation between PCSCs).
- Measures to improve cybersecurity understanding and strengthen cybersecurity capabilities among governments in the global South.

- Guidance on good practices for governments contracting PCSCs.
- Propose an intergovernmental protocol on legal obligations of states regarding the activities of PCSCs that duly deal with transparency, accountability, and effective oversight.

The G20 should create a Cybersecurity Task Force to monitor the implementation of the action plan and to develop relations between the G20 and the PCSCs industry.

Attribution: Shaun Riordan, Mario Torres Jarrín, and Alejandro Garofali Acosta, “A Framework for the Global Governance of Private Cybersecurity Companies,” *T20 Policy Brief*, July 2023.

Endnotes

- 1 Florian Egloff, "Semi-State Actors in Cyberspace," Oxford: Oxford University Press, 2022.
- 2 Tim Maurer, "Cyber Mercenaries: The State, Hackers and Power," Cambridge: Cambridge University Press, 2018.
- 3 Martin Libicki, "Cyberspace in Peace and War," Annapolis: Naval Institute Press, 2016.
- 4 Jean-Loup Richet, "Cybersecurity Policies and Strategies for Cyberwarfare Prevention," Hershey: PA, 2015.
- 5 Peter Warren Singer, "Corporate Warriors: The Rise of the Privatised Military Industry," New York: Cornell University Press, 2003.
- 6 George Perkovich, and Levitte, Ariel, "Understanding Cyber Conflict: 14 Analogies," Washington: Georgetown University Press, 2017.
- 7 Shaun Riordan, "Cyberdiplomacy: Managing Security and Governance in Cyberspace," Cambridge: Polity, 2019.
- 8 https://icoca.ch/wp-content/uploads/2022/01/INTERNATIONAL-CODE-OF-CONDUCT_Amended_2021.pdf
- 9 https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf
- 10 https://www.voluntaryprinciples.org/wp-content/uploads/2021/11/The-Voluntary-Principles_English.pdf
- 11 https://t20saudi Arabia.org.sa/en/briefs/Documents/T20_TF5_PB4.pdf
- 12 <https://www.t20italy.org/wp-content/uploads/2021/09/TF8-torres.pdf>
- 13 Alaa Assaf, Daniil Moshnikov and International Law in the Digital Age Research and Study Group, "Contesting sovereignty in cyberspace", Springer, International Cybersecurity Law Review, volume 1, 2020; Felix Biermann and Moritz Weiss, "Cyberspace and the protection of critical national infrastructure", Geschwister-Scholl-Institute of Political Science, LMU Munich, Germany, September 2020; Aapo Cederberg, "Future Challenges in Cyberspace", GCSP Policy Paper 2015/4, April 2015; Dhaval Chudasama and Kathan Patel, "National Security Threats in Cyberspace", *National Journal of Cyber Security Law, Review NJCSL*, Volume 4, Issue 1, 2021.



वसुधैव कुटुम्बकम्

ONE EARTH • ONE FAMILY • ONE FUTURE