United Nations A/76/151

General Assembly

Distr.: General
15 July 2021

Original: English

Seventy-sixth session
Item 74 of the provisional agenda*
Right of peoples to self-determination

Use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, in accordance with Assembly resolution 75/171 and Human Rights Council resolution 42/9.

* A/76/150.

21-09837 (E) 130821

Report of the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination

The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyberactivities

Summary

In the present report, the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination examines the provision of military and security products and services in cyberspace by mercenaries, mercenary-related actors and private military and security companies and its human rights impacts.

There is a wide range of military and security services provided in cyberspace, including data collection, intelligence and espionage. Private actors can be engaged by States and non-State actors in various proxy relationships to conduct offensive or defensive operations and to protect their own networks and infrastructure, as well as to carry out cyberoperations to weaken the military capacities and capabilities of enemy armed forces or to undermine the integrity of other States' territory. Individuals carrying out cyberattacks can cause damage remotely, across various jurisdictions. As such, they can be regarded as undertaking a mercenary-related activity, or even a mercenary activity, if all of the qualifying criteria are met.

The present thematic study aims towards exploring the manifestations and activities of these actors who benefit from developing, maintaining and operating cybercapabilities, which might be used in the conduct of hostilities, in conflict and in non-conflict settings. It assesses the impacts that this may have on human rights, including the right of peoples to self-determination, as well as examines the issue of regulating the provision of military and security products and services in cyberspace.

During the preparation of the present report, the Working Group was composed of Jelena Aparac (Chair), Lilian Bobea, Ravindran Daniel, Chris Kwaja and Sorcha MacLeod.

Contents

I. Introduction and context

1. The present report is submitted to the General Assembly by the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination, in accordance Assembly resolution 75/171 and Human Rights Council resolution 42/9.

2. In pursuance of this mandate, the Working Group monitors mercenaries and mercenary-related activities in all their forms and manifestations, as well as private military and security companies in different parts of the world. In addition, the Working Group studies their activities and the impact they may have on human rights, in particular the right to self-determination.

3. This report relies on extensive desk research and contributions received from relevant stakeholders on the basis of a call for submissions issued by the Working Group in January 2021.[1] On 7 December 2020, the Working Group convened an online expert consultation on mercenaries and related actors in the context of cybersecurity and new technologies, with a view to feeding its outcomes into the report. The Working Group thanks all those who contributed to the preparation of the report by submitting information and participating in the expert consultation.

4. Discussions on the activities of mercenaries over the years have focused on traditional modes of warfare where mercenaries are involved either on behalf of States or other clients. More recently, mercenaries, mercenary-related actors and private military and security companies have become active in cyberspace. In its report on the evolving forms, trends and manifestations of mercenaries and mercenary-related activities (see A/75/259), the Working Group referred to so-called "cybermercenaries" as constituting one category of actors that can generate mercenary-related activities. In addition, the issue of the use of technologies and knowledge transfers is regularly raised in the annual reports of the Working Group in relation to various topics.[2] The present report examines the provision of military and security products and services in cyberspace by mercenaries, mercenary-related actors and private military and security companies, and their human rights impacts.

5. In its previous analyses, the Working Group has pointed to the range of mercenaries and mercenary-related actors that continue to influence the course of contemporary armed conflicts, to commit human rights abuses and to undermine the right to self-determination, including through cyberactivities. Today, cyberspace represents a major geostrategic arena for both State and non-State actors with a variety of private entities mobilizing and harnessing both defensive and offensive cybercapabilities in the pursuit of proxy agendas or interests, with devastating consequences for the enjoyment of human rights and for the right of peoples to self-determination.

6. In particular, the Working Group has previously noted the increasingly asymmetric nature of modern armed conflicts as well as the rise in the involvement of private actors (A/75/259). While traditional kinetic warfare continues to play a major role in contemporary conflict, the use of cyberattacks and other cyberactivity is becoming increasingly prevalent as new technologies are developed and continue to evolve, even outside of traditional armed conflicts. As a corollary to these developments, contemporary mercenaries and other actors have adapted to and become active in cyberspace and, in some instances, they have become a necessary component of cyberoperations.

[1] See www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx.

[2] See A/75/259, para. 50; A/HRC/45/9, para. 39 et seq.; A/HRC/42/42.

II. Definitional considerations

7. The term “mercenary” is defined in article 47 of Protocol I Additional to the Geneva Conventions of 1949, the International Convention against the Recruitment, Use, Financing and Training of Mercenaries and the Organization of African Unity Convention for the elimination of mercenarism in Africa. Nevertheless, the definition of “mercenary” in international law has been the subject of much analysis and reflection centred on its overly restrictive nature. The Working Group recognizes that the scope of the definition is problematic and that the criteria are difficult to meet, especially with regard to contemporary forms of mercenary-related activities, including when those activities are carried out in cyberspace by non-State actors.

8. In addition, in the absence of an internationally agreed legal definition, the Working Group has previously defined the term “private military and security companies” as corporate entities providing, on a compensatory basis, military and/or security services by physical persons and/or legal entities.[3] They may operate in both conflict and peacetime situations and are significant providers of military and security products and services in the cybersphere.

9. While none of the above definitions incorporate an express reference to cyberactivities or cyberactors, it is nevertheless clear that some actions in the cybersphere may rise to the level of mercenarism or may be considered mercenary-related activities and also impact human rights both in armed conflict and in peacetime. Such actions could include malicious cyberoperations conducted by cyberintermediaries regardless of their nationality or their place of operations or whether they are operating offline or online or causing harm directly or indirectly.[4] Malicious cyberoperations are understood as entailing the use of deliberate actions and operations to alter, disrupt, deceive, degrade or destroy computer systems or networks, or otherwise undermine the confidentiality, integrity, and availability of computer systems or networks for individuals and communities.[5] This does not include emerging technologies – for example, drone technology – that have kinetic impacts outside computer networks.

10. The Working Group wishes nevertheless to stress that military and security services provided in cyberspace should not be taken to designate the operations of mercenary-related actors in general but rather that each possible case arising from among these categories needs to be assessed in the light of its specific context and circumstances (see A/75/259, para. 54).

11. In 2020, the Working Group recognized cyberwarfare as a method of warfare that can not only infiltrate, disrupt, damage or even destroy military or civilian objects, but also cause serious human harm. The International Committee of the Red Cross has concluded that similar to conventional warfare, it must comply with international humanitarian law.[6] This is all the more relevant as strategic capabilities increasingly depend on infrastructure and technology (see A/75/259, para. 42).

12. The Working Group was prompted by, inter alia, the transformation of contemporary conflicts and the rapid evolution of new forms of warfare paired with the lack of regulation, monitoring and oversight, as well as the difficulties of investigating crimes that are perpetrated across jurisdictions, to shine a light on this

[3] For the full definition see A/HRC/15/25, annex, article 2.

[4] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 31.

[5] Herbert S. Lin, “Offensive cyber operations and the use of force”, *Journal of National Security Law and Policy*, vol. 4, No. 1 (13 August 2010), pp. 4–63; and ISO/IEC 27000:2009.

[6] International Committee of the Red Cross, “International humanitarian law and cyber operations during armed conflicts”, ICRC position paper, November 2019.

phenomenon. The unequal access of certain developed countries and wealthy actors to technologies and related know-how has also concerned the Working Group.

13. The Working Group is mindful that the contexts in which mercenaries operate have a differentiated and disproportionate impacts on women, children and other groups (see A/75/259, para. 5) The Working Group notes the difficulties arising from the lack of an internationally agreed definition of what constitutes a cyberattack or cyberhostilities within international humanitarian law and that currently it is therefore conceptually difficult to map cyberhostilities into the international humanitarian law framework and identify non-compliance and violations.

14. A critical element of the ongoing debate on when, where and how such cyberactivities are and could be regulated is the role of non-State actors in cyberactivities and cyberwarfare, in particular mercenaries, mercenary-related actors and private military and security companies, as well as other private and commercial entities. The Working Group therefore seeks in the present report to examine a range of military and security services provided in cyberspace which can generate mercenary-related activities in order to stimulate a discussion on how to better frame and address them (see A/75/259, para. 52). Beyond regulation, effective cooperation at the national and international levels between relevant actors must be developed to tackle this phenomenon.

III. Military and security services in cyberspace: activities, categories of actors and relationships between State and non-State actors

15. Military and security services encompass a range of services which include data collection and espionage. Private actors can be engaged by States and non-State actors in various proxy relationships to conduct offensive or defensive operations to protect their own networks and infrastructure, as well as to carry out cyberoperations to weaken the military capacities and capabilities of enemy armed forces or to undermine the integrity of another State's territory. In utilizing their offensive or defensive cyberfirepower, these actors are linked to attempts or actions that seek to identify, invade, distort critical military or civilian installations, with the goal of destroying them.

16. As mentioned above, it is important to note that cyberservices are provided to States outside of the context of armed conflict including for the purposes of not only intelligence gathering and surveillance but also domestic law enforcement and the maintenance of security.[7] In addition, cyberservices include both the provision of support services to States in relation to existing cybercapabilities and the provision of cyberproducts that can be utilized by States. It is important to note that a vast range of products and services are being provided and are available for purchase on the open market, which must be taken into account when considering the regulation of cyberservices.

17. The multiple types of cyberactivities and methods of cyberoperations that are currently being undertaken include, inter alia, sabotage via malware and ransomware, espionage and subversion which involves the supply of misinformation and disinformation. In practical terms, these activities can take the form of shutting down or damaging key pieces of infrastructure including electricity and water supplies, hospitals, surveillance services and communication facilities, or they can also facilitate the targeting or incapacitation of military defence and other systems.

[7] See submission by ICT for Peace.

18. In their work for private companies and States, cybersecurity firms provide defences against cyberattacks and cyberwarfare. These purely defensive operations include firewalls, patches and antivirus software, while more active but still defensive steps include creating honeypots and tar pits and beaconing to warn off and entrap attackers.[8] Whether passive or active, such defensive operations fall within existing legal guidelines for cybersecurity operations.

19. However, both private and government cybersecurity firms, as well as rogue operators, also have offensive capabilities, which is an area of particular concern to the Working Group. The offensive capabilities of cybersecurity firms can be deployed against developed States, for example, in attacks on election infrastructure, which are assumed to be carried out by either State-sponsored actors or proxies working for States. Malicious cyberactivities also include the targeting of virtual assets and virtual asset service providers, as well as attacks on defence companies, including to illegally access military technology (see S/2021/211, annex, paras. 125–126). There is no obvious and apparent unifying pattern characterizing the State and non-State actors that purchase these technologies. Both democratic and non-democratic States acquire offensive technologies from external providers, as do States with in-house cybercapabilities as well as those without such resources.

20. The market for offensive cybercapabilities is growing rapidly, is subject to little regulation and offers an opportunity to make a significant profit. As a result, many conventional private military and security companies are developing cybersecurity divisions.[9] Whatever their provenance, cybersecurity providers, like more traditional private military and security companies, work hand in hand with national Governments and become extensions of State power and could thus be considered mercenary-like proxies.

21. The distinctions between offensive and defensive services and between transparency and ambiguity over legal status apply to military and security services provided in cyberspace. Private actors can be engaged by States and non-State actors not only to protect their own networks and infrastructure but also to carry out cyberoperations designed to weaken the military capacities and capabilities of enemy armed forces or to undermine the integrity of another State's territory. The presence of mercenaries in cyberspace, where they are now involved in the production and sale of offensive cyberweapons, underscores their adaptive capacity.[10] Individuals carrying out cyberattacks can be viewed as undertaking a mercenary-related activity, or even a mercenary activity if all of the qualifying criteria are met (see A/75/259, para. 71).

A. Categories of relevant cyberactors

Cyberunits or cybercommands integrated into the official armed forces

22. In recent years, the competition for cyberexpertise was stimulated by the strategies of cyberinfluence which demonstrated their devastating effects on modern geopolitical relationships.[11] Some States are engaging in what has been described as an "informational fight in cyberspace"[12] and are integrating the operations of military

[8] Submission received under seal.

[9] W. J. Hennigan, "Defense contractors see opportunity in cybersecurity sector", *Los Angeles Times*, 21 January. Available at www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html.

[10] Tom Burt, "Cyber mercenaries don't deserve immunity", Microsoft website, 21 December 2020. Available at https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] See https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, pp. 9–10.

[12] See https://spire.sciencespo.fr/hdl:/2441/1uu1c1r2ua9f0o7n0co15a8trv/resources/2021-03-derochegonde-tenenbaum-cyberinfluence-focus-strategique.pdf, pp. 7–8.

strategies of influence into their military capacities. The rapid evolution of digital technologies has profoundly transformed warfare and prompted investments in the development of cyberunits or cybercommands integrated into the formal armed forces. Furthermore, the classical forms of warfare between two armed forces are now accompanied by cyberwarfare, where cyberunits operate along the thin lines separating defensive and offensive operations.[13] Cyberoperations can be conducted alone or in combination with traditional military operations. However, the most concerning scenario remains that associated with the case of "hybrid operations", where the State responds with its cybermilitary operations in a context that would not be deemed as having reached the threshold of armed conflict under the rules of international humanitarian law. The informational fight in cyberspace is even more complex when formal armed forces outsource some of their cyberactivities to a third party.

Actors outside of official armed forces

23. Non-State entities that are not integrated with the armed forces play a highly significant and increasingly large role in the provision of cyberservices to and on behalf of States. The evolving threat of the privatization of cybersecurity attacks through a new generation of private companies referred to as so-called "cybermercenaries" is proliferating,[14] and there is an increasingly blurred line separating the private and national spheres.[15]

Business entities

24. Unlike conventional private military and security companies, which have typically privatized functions and capabilities which were once monopolized by the State, cybersecurity providers first emerged and flourished in the private sector. While the most advanced global militaries have developed in-house cybersecurity expertise and capabilities, even these sophisticated military operations draw heavily on private sector cybersecurity expertise.[16] Private cybersecurity firms include long-established for-profit players and nimble start-ups which have won market shares in a rapidly expanding market.

25. Private software and technology companies that fall within the scope of the analysis can be divided into two groups. One subcategory is made up of large technology platforms which work in collusion with government entities in order to enable the Government to access information and run surveillance programmes.[17] The other subcategory is made up of companies that are much smaller in size and level of revenue but have specific capabilities for manufacturing products that may be used for conducting malicious activities. The sector of private cybersecurity firms is rapidly growing and evolving. In addition, several private military and security companies have moved into cybersecurity, often by acquiring boutique technology firms and bringing them in-house.

26. Companies in the defence sector that traditionally produced weapons and military equipment have extended their activities to the digital sector. These contractors have largely developed in-house cybersecurity solutions and services, although some have also hired commercial cybersecurity firms as subsidiaries to

[13] Neri Zilber, "The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?", *Foreign Policy* (FP), 31 August 2018. Available at https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

[14] See submission by Access Now, p. 1.

[15] See submission by Ori Swed and Daniel Burland, p. 15.

[16] See www.cmi.no/publications/file/6637-russian-use-of-private-military-and-security.pdf.

[17] See https://harvardlawreview.org/2018/04/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/.

bolster their capabilities. The public messaging of the defence contractors intentionally blurs the lines between actions and services designed purely to defend the resilience of cyberspace and disruptive technologies which would allow clients to undertake offensive operations and potentially malicious activities.

Advanced persistent threat (APT) groups

27. Members of advanced persistent threat groups are rogue/criminal actors engaged in sustained penetration of cybersecurity systems of States and public and private actors. They are technologically sophisticated and possess important financial and technical resources, have long-term strategic goals and are often supported in some manner by national Governments.[18] They have in-house offensive capability development capacity and can conduct large-scale cyberoperations. Cyberdivisions of national militaries also launch advanced persistent threats. “Hackers for hire” may also persistently test the cyberdefences of private companies and Governments. By their very nature, advanced persistent threat groups are associated with a longer-term goal than that of realizing quick profits through use of ransomware.

Cybermilitias

28. Another category comprises so-called cybermilitias, which encompass a variety of organizations sustained by volunteers. As such, those militias might lie beyond the pale of mercenaries or mercenary-related actors. They differ from advanced persistent threat groups in that they are not as well organized or as well funded and do not have long-term strategic objectives. A theoretical model for volunteer-based offensive cybermilitias distinguishes among the forum, the cell and the hierarchy. The forum is an ad hoc cybermilitia structure which is organized around a central communications platform, where the members share the information and tools necessary to carry out cyberattacks against their chosen target. The cell model is given form in hacker cells, which engage in politically motivated hacking over extended periods of time. The hierarchy reflects the traditional hierarchic model, which may be embodied by government-sponsored volunteer organizations, as well as cohesive self-organized non-State actors. The category of cybermilitias also includes organized groups of cyberprofessionals who volunteer to repel cyberattacks.[19]

Individuals

29. Cyberexperts who possess technical expertise in information technology often work outside any organizational structure and conduct independent research aimed at detecting software vulnerabilities or bugs.[20] These individuals are known as security researchers and may sell information connected with those vulnerabilities to adversaries.[21] Depending on the context, they are often compensated for this work through payouts known as “bug bounties”. They are connected with potential clients through online portals.

Cybercriminals

30. Criminal extortion rings are rogue criminal actors whose goal is not necessarily to disrupt the economy or carry out political sabotage, but rather to utilize the holding

[18] See https://targetedthreats.net/media/1-ExecutiveSummary.pdf.

[19] See Rain Ottis, “Proactive defence tactics against on-line cyber militia”, in *Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01–02 July* (Reading, United Kingdom, Academic Publishing, 2010), pp. 233–237.

[20] Steve Ranger, “Meet the hackers who earn millions for saving the web, one bug at a time”, ZD Net, 16 November 2020. Available at www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecu.

[21] See submission by Women’s International League for Peace and Freedom.

of corporate data as an extortion mechanism. They are individuals or groups operating for their own benefit that target services, products and infrastructure provided by the public and private sectors, and upon which entire communities and populations are reliant. They extort ransoms and the response to the ransom demand by the targeted victims has economic and political implications extending beyond the individual act itself, with respect to the potential expansion and perpetuation of these types of attacks. For example, disruptions continue until a ransom is paid.

B. Relationships between State and non-State actors

31. State engagement with these cyberactors can take different forms. In the case of delegation, the State exercises clear oversight over the actions of proxies through screening and selection of actors, punitive sanction and a clear evaluation of potential impacts.[22] In this case, clear responsibilities are assigned to proxies through the channels of municipal law and policy, for example to undertake pre-emptive strikes against perceived cyberthreats[23] on critical infrastructure.[24] In the event of orchestration, the State extends passive support to the proxies but does not establish clear oversight mechanisms over their operations.[25] This is generally achieved through loosely defined or absent policy frameworks and ad hoc collaboration through "network relationships".[26] Under the sanctioning model, the State does not acknowledge the actions taken by the private actors operating from their territory.[27]

32. Through the process of privatization of some of informational operations and military strategies of influence, a State outsources to private actors those tasks that it is no longer able or willing to provide. Multiple providers conduct tasks that may have been performed previously by public security forces, as well as additional tasks that were never within the domain of State security forces (see A/74/244).

33. States outsource cyberservices to non-State actors for a number of reasons. In the same way that States often lack the necessary capacities for traditional modes of warfare, certain States may not possess sufficient cybercapabilities, especially when the relevant technology is ever evolving and entails a significant cost. Similarly, States may not be able to maintain such cybercapabilities and thus may prefer to outsource on an ad hoc basis. The demand for cybercapabilities is booming.[28] It has coincided with and has been caused by extensive capacity and capability shortages within States.[29] The move to recruiting private actors or to outsourcing may correlate in some States with a reduction in defence budgets and the more general trend towards involving the private sector in the provision of public services which will include

[22] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018), p. 29.

[23] Amanda N. Craig, Scott J. Shackelford and Janine S. Hiller, "Proactive cybersecurity: a comparative industry and regulatory analysis", *American Business Law Journal*, vol. 52, no. 4 (winter 2015).

[24] Ellyne Phneah, "S'pore beefs up cybersecurity law to allow preemptive measures", ZDNet, 14 January 2013), Available at www.zdnet.com/sg/spore-beefs-up-cybersecurity-law-to-allow-preemptive-measures-7000009757/.

[25] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

[26] Arindrajit Basu and Elonnai Hickok, "Conceptualizing an international framework for active private cyber defense". Available at https://4bac176f-2e16-421b-823f-0ab6d7712f85.filesusr.com/ugd/066049_e1a28ac2850d49fbb6f52eeb9fc79ae7.pdf.

[27] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).

[28] See submission by Krieg, p. 1.

[29] Ibid.

military operations and security services.[30] Further, this outsourcing can allow States to disassociate themselves from cyberactivities and avoid scrutiny and consequences.[31]

34. The Working Group notes the difficulty of identifying with any certainty specific examples where States use mercenaries and mercenary-related actors and outsource provision of cyberservices to non-State actors. It is also difficult to ascertain the exact extent and nature of the provision of those services, given the highly sensitive nature of such operations and the secrecy and opaqueness that characterize the cyberindustry. More research is needed to identify which actors are delivering what kinds of services.[32] Current research on how State and non-State actors contract for cybercapabilities and what kind of services they are purchasing is both imperfect and incomplete. The incompleteness of the picture is the result of a number of factors, including the fact that most companies operating in this space are private (non-listed) companies.[33]

35. Nevertheless, information received strongly suggests that such contracting and outsourcing are ongoing and will continue into the future. It is also safe to assume that they are taking place given the vast growth of the cyberservices industry and the fact that prior to the expansion of the role of cyberactivities, States were outsourcing traditional security functions and military functions to non-State actors. Government typically cannot keep up with the pace at which the private sector is developing new technologies.[34] In the context of rapid technological developments, and investments in digital technologies and artificial intelligence, the Working Group strongly believes that cyberservices and cyberproducts will continue to be outsourced to non-State actors.

36. Cyberattacks are multi-stage and multi-step and attributing responsibility to the perpetrators and their clients is therefore extremely challenging. In a botnet attack, for instance, a botmaster infiltrates a large network of vulnerable computers and directs the net of compromised computers to attack a victim network. Tracing the attack back to the bot-master would span several countries and several jurisdictions.[35] This raises significant concerns owing to the potential of cyberoperations to significantly undermine human rights. The possibility that cyberproxies may move across borders and thus escape regulatory control and accountability mechanisms is a serious cause for concern.[36]

37. States as well as non-State actors have started using private actors to project cyberpower, given the relatively low costs of such operations compared with those of conventional warfare and the possibility of hiding behind an actor whose identity it is very difficult to uncover. The use of a proxy creates one level of separation between the perpetrator and its target, which benefits further from the high degree of anonymity available online and the challenges of how to attribute responsibility for a cyberoperation in a timely manner.[37] The benefit of using such actors hinges on the fact that unlike States that are subject to international human rights and humanitarian law protocols, they operate outside the purview of such protocols, making attribution,

[30] Submission submitted under seal.
[31] See submission by Krieg, p. 1.
[32] See submission by ICT for Peace, p. 2.
[33] See submission by The Citizen Lab, p. 1.
[34] See submission by ICT for Peace, p. 2.
[35] David D. Clark and Susan Landau, “Untangling attribution”, *Harvard National Security Journal*, vol. 2, No. 2 (2011).
[36] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, United Kingdom, Cambridge University Press, 2018).
[37] See submission by Women’s International League for Peace and Freedom, p. 4.

arrests and prosecution difficult.[38] This allows a State in turn to disassociate itself from cyberoperations and as a result avoid scrutiny and the attribution of responsibility and liability.[39]

IV. Regulating the role and involvement of mercenaries, mercenary-related actors and private military and security companies in the provision of cyberservices

38. Regulating the role and involvement of mercenaries, mercenary-related actors and private military and security companies in the provision of cyberservices, including cyberattacks and cyberwarfare, at the international level poses a significant number of challenges and difficulties. In particular, these are related to (a) conceptualization of what constitutes cyberactivities including cyberwarfare and cyberattacks; (b) identification of the source of cyberattacks and other cyberactivities; (c) attribution of such attacks or activities to particular persons or entities; and (d) identification of the relationship between the non-State actor and the State on behalf of which such activities are undertaken, if at all, and the issue of whether particular cyberactivities constitute involvement or direct or indirect participation in ongoing hostilities. There is much discussion and debate focused on the extent of the current regulation of cyberactivities and the extent to which they should be regulated at the international level.

39. These challenges stem from the opaque nature of cyberactivities, their source and the entities that conduct them, and the relationship between States and the other non-State actors. This disassociation, which is not as easily achievable in the context of traditional kinetic armed conflict, benefits State and non-State actors, as it potentially shields them both from liability for their actions; however, it makes regulating those activities much more difficult. The issue of the attribution of cyberoperations and the matter of the intentional disassociation of such operations from State armed forces, such that there can be "plausible deniability", is patently a serious problem in advancing regulation.

40. The existing relevant international regulatory framework includes the Charter of the United Nations, international humanitarian law, the Tallinn Manual on the International Law Applicable to Cyber Warfare, international criminal law, international human rights law, soft law and domestic law.

A. Charter of the United Nations

41. The Charter of the United Nations, and particularly Article 2 (4), which prohibits the threat or use of force against the territorial integrity or political independence of any State, is to play a role in the regulation and sanctioning of cyberactivities including mercenary activities. This is based on the fact that cyberactivities may be of such scale and effect as to constitute "use of force" and may thus be prohibited under the Charter of the United Nations. Similarly, such activities may meet the threshold of an "armed attack" which triggers a State's right to take action in self-defence, pursuant to Article 51 of the Charter of the United Nations. Whether such cyberactivities meet the relevant thresholds, in particular regarding the principles of

[38] Ataa Dabour, "The rise of cyber-mercenaries", 2021. Available at www.hscentre.org/technology/the-rise-of-cyber-mercenaries/.

[39] See submission by ICT for Peace, p. 2.

necessity and proportionality,[40] is a question of fact and degree but there can be little doubt that, given the nature and effects of modern cyberactivities, they could satisfy those thresholds in particular circumstances.

42. A more difficult question that needs to be considered, however, is whether cyberattacks or other activities that are conducted by non-State actors would engage the relevant provisions of the Charter of the United Nations. The answer would depend on whether the actions of those individuals or entities are attributable to a particular State under the Draft articles on Responsibility of States for Internationally Wrongful Acts, given that the Charter of the United Nations applies only to situations occurring between sovereign States.

43. The issue of attribution may pose considerable challenges evidentially given that entities that provide cyberactivity services will often operate at a significant arm's-length distance from the State and the source of cyberattacks may be difficult or impossible to trace given that they are initiated remotely and may comprise various inputs from different locations and actors. And there is, of course, a deliberate use of mechanisms for avoiding detection and attribution of attacks.

B. International human rights and humanitarian law

44. States are bound to respect international human rights rules, both in peacetime and during armed conflict, subject to relevant and specific exceptions and derogations. States are also required to guarantee compliance by private actors within their territory through domestic law and enforcement. The comprehensive and well-developed framework of human rights protection at the international level, with its various treaties, monitoring bodies and enforcement mechanisms, is a ready means of cyberspace regulation.

45. In its statement at the open-ended working group on developments in the field of information and telecommunications in the context of international security, the International Committee of the Red Cross affirmed that the rules of international humanitarian law apply to new forms of armed conflict including cyberwarfare.[41] In the reaching of that conclusion, reliance is placed on the Advisory Opinion of the International Court of Justice in the case concerning the legality or use of nuclear weapons, in which the Court concluded that international humanitarian law applies to current and future weapons and types of warfare.[42] While there is an ongoing debate on a specific interpretation with respect to application of the relevant principles of international humanitarian law to cyberoperations in the context of armed conflict, it appears that the rules do apply in principle. This approach is confirmed in the Tallinn Manual with respect to the law applicable to cyberwarfare. The Manual states unequivocally that "[t]he law of armed conflict applies to cyberoperations as it would to other operations undertaken in the context of an armed conflict".

46. However, once again, such an approach is not without its difficulties, particularly in light of the role of non-State actors which provide such cyberservices. There is no internationally agreed definition of what constitutes a cyberattack or

[40] See https://international-review.icrc.org/articles/can-jus-ad-bellum-override-jus-bello-reaffirming-separation-two-bodies-law.

[41] Statement delivered by Véronique Christory, senior arms control adviser for the International Committee of the Red Cross, to the Open-ended working group on developments in the field of information and telecommunications in the context of international security, New York, 10 September 2019.

[42] *Legality of the Threat or Use of Nuclear Weapons*, *Advisory Opinion*, *I.C.J. Reports 1996*, issued on 8 July 1996; ICRC, position Paper on international humanitarian law and cyber operations during armed conflict, November 2019, p. 4.

cyberhostilities within international humanitarian law. The notion of "attack" itself, however, is of importance, primarily in relation to the principle of distinction and to what constitute military and civilian objectives. The military or civilian character of objectives may be subject to interpretation, but this interpretation does not depend on the method of warfare used during the attack. Whether the attack is conducted through kinetic means of warfare or through use of cybertechnologies, the civilian character of the object should be respected.

47. Another issue of concern is the status of a cyberoperation during an armed conflict and, more particularly, determining whether the operation constitutes direct participation in the hostilities, which is relevant for meeting the criteria for classification as a mercenary under article 47 of Protocol I Additional to the Geneva Conventions of 1949, or has a sufficient nexus to the specific armed conflict. In some instances, cyberattacks directed at destroying State capabilities and State infrastructure would be equivalent to direct participation in hostilities by a non-State actor in the context of an armed conflict.[43] It is a matter of fact and degree whether any particular cyberactivity is likely to affect the military capacity of a party to a conflict, and whether it is likely to cause harm to a party to a conflict, with a sufficient nexus between the act and the armed conflict. Besides legal aspects, this question has also a more practical dimension, as it may not always be possible to identify the occurrence of cyberattacks or subtler cyberactivities. The interpretation of all the concepts will likely depend on State practice.

48. In relation to mercenaries more specifically, persons who satisfy the definition of a mercenary are not entitled to the status of combatant and its inherent protections. More important, currently, they can be prosecuted for the very fact that they participated in the hostilities, regardless of whether a State or a non-State actor contracted them to participate in (cyber)hostilities. They can also be prosecuted for the fact that they participated in the mercenary activities provided that the relevant domestic regime sets forth such legal provisions. Furthermore, pursuant to common article 1 of the 1949 Geneva Conventions, States are obligated to ensure respect for the Convention and this includes ensuring that entities that are operating on their behalf, which can include non-State actors operating on behalf of States, act in compliance with international humanitarian law.

49. As a consequence, it has been suggested that the traditional definition of a mercenary may not be suited to the evolution of the means of warfare and contemporary conflicts which are characterized by, or at least involve, the use of cyberwarfare or other cyberactivities, suggesting the need to reconceptualize the understanding of what constitutes a mercenary within the cyberdomain.[44]

50. Another issue that arises, and which will need to be considered in relation to the application of international humanitarian law to cyberspace, concerns the different legal regimes which apply to non-international and international armed conflicts, and whether that same approach will need to be taken in relation to cyberservices. The question also arises of whether, with the evolution of cyberwarfare and cyberoperations, the traditional distinction can be maintained.

51. In addition, there is a fundamental issue that stems from the fact that while international humanitarian law provides a well-developed and comprehensive regulatory framework which can be applied to cyberactivities, it of course applies only during times of armed conflict. It is the case that many cyberactivities, and

[43] Nils Melzer, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Geneva, ICRC, May 2009). Available at www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf.

[44] See submission by Van der Waag-Cowling, Van Niekerk and Dr Ramluckan, p. 4.

perhaps the majority, occur outside of the context of an armed conflict and therefore the international humanitarian law regulatory regime would not apply.

C. International criminal law

52. International criminal law applies to any natural person who commits an international crime, and the International Criminal Court, has jurisdiction over war crimes, crimes against humanity, genocide and war of aggression. Therefore, if cyberservices provided by natural persons satisfy one or more elements of one or more crimes, and other relevant criteria are satisfied, the International Criminal Court could potentially have jurisdiction over criminal acts committed by mercenaries and mercenary-related actors in the cybersphere. International criminal law can be useful insofar as the command responsibility doctrine could help overcome some of the obstacles related to identifying and locating the actual perpetrator. The superiors of such individuals who are implicated in the commission of the crime, such as through ordering the commission of devastating cyberattacks, or fail to prevent such malicious cyberattacks should not evade accountability.[45] In addition to challenges already identified above, international criminal law requires crimes to be proved in international proceedings beyond a reasonable doubt, the highest evidentiary standard. Furthermore, given that cyberoperations may involve several States, issues with regard to jurisdiction and complementarity may arise which could create additional challenges for investigations and prosecutions.

53. Both the International Convention against the Recruitment, Use, Financing and Training of Mercenaries and the Organization of African Unity Convention for the elimination of mercenarism in Africa criminalize mercenarism which creates an alternative legal basis for the prosecution and punishment of mercenary-related activity. States that ratify these conventions should transpose the relevant provision to their domestic legal regimes, thereby enabling domestic courts to prosecute mercenary activities.

D. Soft law and ongoing initiatives

54. In addition to the binding international law frameworks, a number of multi-stakeholder and multilateral initiatives targeting various actors and seeking to foster responsible behaviour during the use of information and communications technology have emerged over the past decade. These include normative non-binding frameworks targeted at private actors such as the Cybersecurity Tech Accord and the Charter of Trust instituted by Siemens. Independent expert groups such as the Global Commission on the Stability of Cyberspace and the Independent Group of Experts that drafted the Tallinn Manual elaborated recommendations on norms and applicable international law. Other multi-stakeholder initiatives such as the Paris Call for Trust and Security in Cyberspace have been targeted at the private sector, civil society and Governments.

55. At the level of the Human Rights Council, an open-ended intergovernmental working group plays a significant role in elaborating the content of an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies plays. Owing to the rapidly changing operating contexts and services provided, any regulatory mechanism developed through this process should refer to “services” or “activities” rather than to “private

[45] See submission by Access Now, p. 10.

military and security companies" as more effective terminological options for capturing human rights or international humanitarian law abuses.[46]

56. Two groups have been established by the General Assembly to discuss broader issues of security in the field of information and communications technology and could potentially provide guidance in this respect: the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (see Assembly resolution 73/27), and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (see Assembly resolution 73/266). Both processes consider six main areas, including existing and potential threats; rule, norms and principles for responsible State behaviour; international law; confidence-building measures; capacity-building; and regular institutional dialogue.

57. In March 2021, the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security adopted a consensus report which outlined some non-binding recommendations for all member States. While none of the recommendations address the issue of mercenaries or mercenary-related actors, the report contains several references to human rights and the fact that some non-State actors have demonstrated information and communications technology capabilities previously available only to States is acknowledged in the report. It was noted in the report that the continuing increase in incidents involving the malicious use of information and communications technologies (ICT) by State and non-State actors was a disturbing trend (see A/AC.290/2021/CRP.2, para. 16). In its resolution 75/240 of 31 December 2020, the General Assembly decided to convene a new Open-ended Working Group until 2025 and the Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination believes that this offers an important opportunity to discuss the issue of mercenaries and mercenary-related actors operating in the cybersphere.

58. In its 2021 consensus report, the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security reaffirmed that "States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts".[47] While this does not establish a legal standard for States, it does condemn State orchestration and sanctioning of proxies. The Group of Governmental Experts noted that efforts by States to promote respect for and observance of human rights and ensure the responsible and secure use of information and communications technologies (ICT) should be complementary, mutually reinforcing and interdependent endeavours, while acknowledging that mass surveillance may have negative impacts on human rights, including the right to privacy.[48]

59. The emerging standard-setting initiatives have been described as constituting a "regime complex" for cybersecurity involving an arrangement of efforts rather than one hierarchic binding instrument.

[46] See statement by Jelena Aparac, Chair of the Working Group on the use of mercenaries. Available at www.ohchr.org/EN/HRBodies/HRC/IGWG_PMSCs/Pages/Session2.aspx.

[47] See https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf., para. 71 (g).

[48] Ibid., paras. 39 and 37.

V. Human rights impacts

60. It is undeniable that cyberactivities engage human rights norms and rules and have the ability to cause violations both in armed conflicts and in peacetime, and thus that a whole variety of rights are engaged. The Working Group recalls its findings that the gendered risks and impacts generated by the activities undertaken by private military and security companies share many commonalities irrespective of size and services provided (see A/74/244, para. 6). In addition, the Working Group has identified groups that are particularly affected by mercenaries and mercenary-related actors hired by States, such as human rights defenders, migrants, opposition leaders and journalists, and lesbian, gay, bisexual, transgender, intersex and gender non-conforming persons within the context of gender-based violence.

61. New and emerging forms of warfare can have a significant impact on both military objectives and civilian populations and can result in violations of international humanitarian law as well as the rights and freedoms of individuals in the context of armed conflicts and otherwise. The Working Group indicated previously that cyberwarfare has been recognized as a method of warfare that can not only infiltrate, disrupt, damage and even destroy military and civilian objects but also cause serious human harm.[49] Cybersabotage can have immense secondary effects on the functioning of critical infrastructure, potentially undermining public health, safety and security. In this context, the right to life and the right not to be subjected to torture and other inhuman or degrading treatment are the primary rights at risk of being violated by cyberoperations.

The right to privacy and freedom of expression

62. In all contexts, the right to privacy and the right to freedom of expression are at risk of being violated. When mercenaries and mercenary-related actors are deployed to attack States, they invariably become the key tools for undermining the sovereignty and territorial integrity of such States, which also impedes the exercise of the right to privacy.

63. The right to privacy may also be compromised by monitoring and intelligence gathering. There are substantial concerns regarding cyberoperations targeting civil society and, particularly, human rights defenders and journalists in order to disrupt their activities with a view to stifling dissent and increasing a State's control over its population. Though Governments have long employed different methods to surveil and track their citizens, dissidents, political opponents and human rights defenders, the technological tools now available such as malware and spyware allow them to do so at lower cost and to broaden the geographical reach of surveillance and increase its scope and scale, thereby enabling Governments to carry out digital repression more completely than ever before.[50] Certain forms of spyware are paradigmatic examples of instruments that allow targets to be monitored remotely.[51]

64. Moreover, it has been suggested that the right to freedom of expression may be breached through the control exercised by some States over Internet content or through the dissemination of disinformation and misinformation. Subversive cyberoperations conducted or contracted by governmental clients can undermine the integrity of the cybersphere, freedom of speech and other civil liberties not just of

[49] ICRC, "International humanitarian law and cyber operations during armed conflicts", position paper, November 2019.

[50] See Submission by The Citizen Lab, p. 8.

[51] A/HRC/41/35, para. 9; Bill Marczak and others, *Hide and seek: tracking NSO Group's Pegasus spyware to operations in 45 countries*, Citizen Lab, 18 September 2018.

individuals but of groups and societies at large.[52] Targeted surveillance also creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information.[53]

65. Surveillance technologies developed, maintained and sometimes operated by private companies also play an instrumental role in the shifting of migration routes away from detectable areas and into areas that are beyond the range of surveillance equipment. Migrants are thus compelled to take less direct and more dangerous routes on journeys of migration by water or land, increasing the physical difficulty of movement and the associated physiological and mental toll, pain and suffering which frequently result in death due to heatstroke, severe dehydration and other afflictions.[54]

66. The impacts of cybercapabilities translate into substantial harmful effects on both institutions and individuals, negatively affecting Governments' capacity to provide protection and ensure the well-being of large parts of the population and impeding the enjoyment of human rights. Attacks on electoral systems, for instance, directly impact fundamental democratic rights of representation of citizens who are disenfranchised of their right to vote. It was also reported that some countries routinely launch cyberattacks on civilian areas, hacking private companies or undermining foreign militaries, using online tools to manipulate information or digital propaganda to shape others' opinions and employing digital mercenaries to do the work.[55]

67. There are reports of cyberattacks causing widespread physical damage, including to power grids, financial institutions and government ministries.[56] Destruction of databases which contain information concerning civilians could quickly bring government services and private businesses to a complete standstill and thus cause more harm to civilians than the destruction of physical objects.[57]

Self-determination

68. With regard to the right to self-determination, through the use of military and security products and services in cyberspace, cybersecurity firms could significantly impede the exercise of the right of peoples to self-determination. These actors have the potential to influence domestic insurgencies in ways that may ultimately undermine the right to self-determination (see A/71/318, para. 20).

VI. Conclusions and recommendations

69. **The development and digitalization of technologies have a direct impact on all spheres of civilian life. The military domain is also increasingly reliant on digital technologies. The growing trend towards digitization is reflected in an increased convergence of information space and cyberspace and can have negative impacts on populations in peacetime and during armed conflicts.**

[52] S/2021/569, para. 103.
[53] See A/HRC/38/35/Add.2, para. 53; A/HRC/41/35 para. 26.
[54] A/HRC/45/9, paras. 44–45.
[55] Paul D. Shinkman, "America Is losing the cyber war", U.S. News and World Report website, 29 September 2016. Available at www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries.
[56] Neri Zilber, "The rise of the cyber-mercenaries: what happens when private firms have cyberweapons as powerful as those owned by governments?", *Foreign Policy* (FP), 31 August 2018. Available at https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.
[57] ICRC, "International humanitarian law and cyber operations during armed conflicts", position paper, November 2019.

70. **The Working Group has taken into account the evolution of the provision of military and security products and services in cyberspace by mercenaries, mercenary-related actors and private military security companies and the corresponding consequences for the enjoyment of human rights. It noted the challenges of focusing solely on activities that meet the definition of "mercenary" under the applicable international legal framework and took a broader approach by examining a variety of actors and manifestations that fit under a more adaptable concept of mercenary-related activities.**

71. **The Working Group noted with concern that some States, either by commission or omission, obscure their involvement in malicious cyberoperations, seeking to gain strategic military influence by evading their responsibilities under international law, including for violations and abuses committed by non-State actors recruited for this purpose. However, recruiting private actors to provide military and security services in cyberspace does not relieve States of their obligations under international law.**

72. **The new and evolving manifestations of mercenary-related actors therefore call for urgent attention from States and other relevant stakeholders. The present report elaborates considerations to be taken into account to support States and other actors when developing regulation of actors in cyberspace more effectively, with a view to ensuring respect, protection and fulfilment of the right of peoples to self-determination, protecting civilians in situations of armed conflict and safeguarding the principles of non-intervention and territorial integrity. Discussions centred on any regulation should be grounded in the international legal framework pertaining to mercenaries, notwithstanding its shortcomings, and in the broader framework of international humanitarian and human rights laws.**

Recommendations

73. **To prevent and mitigate the negative human rights impacts caused by mercenary and mercenary-related actors and private military and security companies in cyberspace, States should refrain from recruiting, using, financing and training mercenaries and should prohibit such conduct in domestic law and effectively regulate private military and security companies.**

74. **States should commit to and operationalize transparency with regard to the contracting of military support services, including for cyberoperations, and make public information on the nature of services, procurement procedures, the terms of contracts and the names of services providers in a sufficiently detailed and timely manner. They should not invoke national security concerns as a general reason to restrict access to such information; rather, limitations on access to information must meet the test of legality, necessity and proportionality, in line with the right to freedom of expression.**

75. **States must investigate, prosecute and sanction alleged violations of international humanitarian law and human rights abuses by mercenaries, mercenary-related actors and private military and security companies and provide effective remedies to victims. Investigations, prosecutions and trials must respect and guarantee the right to a fair trial and due process of law.**

76. **At the international level, States should initiate dialogue on new and evolving forms of mercenaries and, in particular, those operating in the cybersphere in all their forms, the risks they pose to international humanitarian and human rights laws and ways to address and counter them more effectively. Any such dialogue should include international and regional organizations, civil society and experts and consider existing tools and initiatives.**

77. **States should reinvigorate discussions with the open-ended intergovernmental working group to elaborate the content of an international regulatory framework on the regulation, monitoring and oversight of the activities of private military and security companies,[58] including with respect to when they provide cyberservices and operate in the context of cyberwarfare. There is a need for a legally binding instrument that governs cyberspace. An international legal framework would lead to certainty and predictability through clear legal obligations which can be enforced through specialized dispute resolution forums. Fragmentation of governance regimes furthers regulatory confusion and often disadvantages developing countries and civil society actors.**

78. **The Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security should further address human rights concerns arising from the involvement of mercenaries and related actors in cyberoperations.**

79. **With regard to activities of mercenary, mercenary-related and private military and security companies associated with armed non-State actors, States should agree on and support international processes to identify, assess and further develop mechanisms to more clearly and formally recognize the international human rights obligations of armed non-State actors, including criteria to determine the latter's capacity to hold human rights obligations.**

[58] See Human Rights Council resolution 36/11.