Working Group on the Use of Mercenaries
Call for Input: Report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact

February 2021

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (U.N.) Working Group on the Use of Mercenaries (the Working Group) to inform the Working Group's report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact to be presented to the U.N. General Assembly at its 76th session in October 2021.[1] As an ECOSOC accredited organisation, Access Now routinely engages with U.N. Special Procedures in support of our mission to extend and defend digital rights of users at risk around the world.[2] Access Now, through its Digital Security Helpline, is a member of the Forum for Incident Response (FiRST), the leading global incident response network.[3] We are founding members of CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the cybersecurity incident response capabilities of its members and share information on threats that affect NGOs, journalists, and other human rights defenders around the world. This submission addresses the following (I) regulatory frameworks and their application and (II) human rights and international humanitarian law impacts of cyber-capabilities and operations conducted by actors operating alone or through Private Military and Security Companies (PMSCs).

Cyber products and services by 'cyber mercenaries'

The evolving threat of the privatization of cybersecurity attacks through a new generation of private companies referred to as 'cyber mercenaries' is rampant. In addition to the use of cyber offensive operations in the space of armed conflict, cybersecurity tools are also used to facilitate surveillance and other forms of repression targeting vulnerable communities and human rights defenders. Though governments have long employed different methods to surveil and track their citizens, dissidents, and political opponents, the technological tools now available to them lower costs, broaden geographic reach, and increase the scope and scale of surveillance, enabling more complete digital repression than ever.[4]

---

[1] OHCHR, Call for inputs: report on the provision of military and security cyber products and services by 'cyber mercenaries and its human rights impact, 2021, available at https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx

[2] Access Now, About Us, 2021, available at https://www.accessnow.org/. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the continued openness of the internet and the protection of fundamental rights. Access Now works to defend and extend the digital rights of users at risk around the world through policy, advocacy, technology support, grants, legal interventions, and global convenings like RightsCon.

[3] https://www.accessnow.org/first-digital-security-helpline/

[4] Access Now, Export bans alone won't stop surveillance — we need a new global approach, 18 November 2019, available at https://www.accessnow.org/export-bans-wont-stop-surveillance-we-need-a-new-global-approach/.

Private and opaque spyware producers such as NSO Group and Hacking Team make it possible for repressive regimes to target those who oppose them in order to stifle dissent. The covert nature of targeted spyware makes it the tool of choice for authoritarians. Take for instance the case of Ahmed Mansoor, an Emirati human rights defender, serving a 10-year sentence for speaking out on social media about human rights violations in the United Arab Emirates. In 2017, Mr. Mansoor was detained by authorities in the UAE after being targeted and surveilled using tools provided by the now infamous spyware company, NSO Group. The NSO was implicated in the case of Jamal Khashoggi, a *Washington Post* columnist and a prominent critic of the Saudi government, who was brutally murdered inside the Kingdom's consulate in Istanbul by a team of Saudi agents.[5] Two years since Khashoggi's assassination, NSO Group has yet to be held accountable for Khasghoggi's slaying, and instead continues to be implicated in egregious human rights violations worldwide. According to The Citizen Lab, a research laboratory based at the University of Toronto, there have been more than 100 abuse cases against NSO Group alone.[6] NSO Group represents the latest high profile firm in this industry, which despite a sordid record of human rights infringement,[7] looks to grow as "other companies are increasingly rumored to be joining in what has become a new $12 billion global technology market."[8] However, our understanding of this sector remains limited, as its closely-held companies operate darkly, changing tactics[9] and constantly shifting domiciles, trade names, affiliates, and corporate shells.[10]

We do see, clearly, that the impact that surveillance technology has had on vulnerable individuals and members of at-risk communities. The adverse effects of this business sector demonstrate why comprehensive, systemic regulation of this industry is both necessary and urgent. Export controls have long been held up as one of the few instruments that democratic countries can leverage to control, and, when necessary, stifle the trade of certain categories of spyware, but must be supplemented by further measures.[11]

---

[5] Access Now, Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government, 1 October 2020, available at https://www.accessnow.org/khashoggi-two-years-later/.

[6] The Citizen Lab, NSO Group/ Q Cyber Technologies: Over One Hundred New Abuse Cases, 29 October 2019, available at https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

[7] *See, e.g.*, Vice, "Topic: Hacking Team," available at https://www.vice.com/en/topic/Hacking-Team

[8] Microsoft, A moment of reckoning: the need for a strong and global cybersecurity response, 17 December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/. *See also* Microsoft, Cyber mercenaries don't deserve immunity, 21 December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/ which outlines the problems with cyber mercenaries like NSO Group. First, even if the tools are sold to governments who use them for narrowly targeted attacks, there are a variety of ways they can still fall into the wrong hands. Second, private-sector companies creating these weapons are not subject to the same constraints as governments. Finally, companies like the NSO Group threaten human rights whether they seek to or not.

[9] *See* Access Now, "Alert: Finfisher Changes Tactics To Hook Critics," May 2018, available at *https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf*

[10] *See, e.g.,* Sinovatio which spun-off of Chinese firm ZTE, at, "Sinovatio: Breaking away from "ZTE" system, Sinovatio has become the leader of network data visualization," available at 21 November 2017, and FinFisher, once part of the Gamma Group, at http://www.sinovatio.com/en/ctt.php?cid=1094; Business & Human Rights Resource Centre, "Ethiopia: Human Rights Watch reports technology companies aid govt. surveillance of political opponents," 24 March 2014, available at https://www.business-humanrights.org/en/latest-news/ethiopia-human-rights-watch-reports-technology-companies-aid-govt-surveillance-of-political-opponents .

[11] Access Now, Export bans alone won't stop surveillance -- we need a new global approach, 18 November 2019, available at https://www.accessnow.org/export-bans-wont-stop-surveillance-we-need-a-new-global-approach/.

I. Regulatory Frameworks and Their Application

I.I Information on existing national, regional or international legislative, policy and regulatory frameworks, or other initiatives, regarding conduct in cyber space and their application (e.g. transparency, responsible behavior, prevention of prohibited conduct)

The relatively successful multi-stakeholder push for norms governing private military and security contractors provides a foundation to advance cyber and digital focused norms and a mechanism to monitor their implementation. As the Working Group noted in their preliminary observations following the 2019 official visit to Switzerland, the international multi-stakeholder initiatives on private military and security companies —*i.e.* the Voluntary Principles on Security and Human Rights (the Voluntary Principles),[12] the Montreux Document,[13] and the more recent International Code of Conduct Association (ICoCA)[14] overseeing the International Code of Conduct for Private Security Service Providers (the Code)[15]—primarily led by Switzerland, "play a seminal role in the creation of an international regulatory framework for private military and security companies."[16] In terms of ICoCA's effectiveness and limitations, it has been noted that the ICoCA is a soft-law, not legally binding mechanism that relies on the voluntariness of private security companies to participate. Nonetheless, despite being voluntary, this soft-law mechanism becomes more effective as more States, international organizations and other clients "favour or require membership of the ICoCA in their procurement practices and include them in their contracts. Importantly, contractual obligations are easier than national law to enforce across borders."[17]

Rather than developing entirely new frameworks to address emerging issues, the U.N. and multilateral entities often conserve resources and maintain hard-won consensus by reviewing and reforming existing agreements. Examples include the repetition of resolutions in the General Assembly and Human Rights Council, the 10-year-review of the World Summit on the Information Society (WSIS+10), and the drafting of a Second Additional Protocol to the Budapest Convention.[18] In this context, the Code explicitly builds on previous normative texts, including the Voluntary Principles and the U.N. Guiding Principles on Business & Human Rights. In the years since the Code's formulation, advancements in information and communications technologies (ICTs) and their increasing impact on human rights and security led to normative guidance being updated for the digital age across multilateral bodies, including the Human Rights Committee, Human Rights Council, OECD, and

[12] Voluntary Principles on Security and Human Rights, 2021, available at https://www.voluntaryprinciples.org/.
[13] Montreux Document Forum, The Montreux Document, 2021, available at https://www.mdforum.ch/.
[14] International Code of Conduct Association (ICoCA), 2021, available at https://icoca.ch/.
[15] International Code of Conduct Association (ICoCA), The Code: The International Code of Conduct for Private Security Service Providers, 2021, available at https://icoca.ch/the-code/
[16] OHCHR, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24622&LangID=E
[17] Anne-Marie Buzatu, "The emergence of the International Code of Conduct for Private Security Service Providers" in *Business and Human Rights From Principles to Practice*, Dorothee Baumann-Pauly and Justine Nolan (Ed), 2016 Routledge, NY at page 170.
[18] *See* EDRi, "New Protocol on cybercrime: cutting red tape ≠ cutting human rights safeguards," 25 Nov. 2019, available at https://edri.org/our-work/new-protocol-on-cybercrime-cutting-red-tape-cutting-human-rights-safeguards.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, among countless others.[19] The Code does not refer to the digital age, and neither mentions cybersecurity nor the internet. Yet its fundamental definitions of PSCs and "Security Services" could reasonably be read to include cyber-enabled operations, or at minimum, to cover operations with digital and cyber aspects. The Working Group should therefore find ways to adapt this existing framework and update it for the digital age.

Parallels exist between private military security contractors and spyware developers. Both often involve privately-held, small and medium-sized corporations that direct their operations at complex environments beyond the borders of their domicile countries. Both often contract exclusively with state and multilateral clients to engage in these security operations, with human rights and humanitarian impacts arising, directly and indirectly. Of course, kinetic warfighting and protection operations have long sought to incorporate new ICTs, and continue into the realms of artificial intelligence and the internet of things.[20] As traditional weapons expand their cyber functionality, and cyberweapons advance in capability while dropping in cost, we see no limit to the expansion of cyber in the work of PSCs.

While the Code, like the Wassenaar Arrangement, launched in a pre-digital age, to put it bluntly, it's all we have; in the absence of state action to protect human rights or adequate judicial oversight of private contractors supplying cyber weaponry and invasive spyware services to governments that abuse them, we rather desperately look to this framework and its implementation mechanism to provide at least a modicum of the accountability – and preventive and mitigation steps – lacking in this evolving context.

Civil society, journalists, and academic partners stand ready to assist the Working Group in addressing digital harm and cyber operations. Existing cyber, digital focused norms found within the international legal framework can also provide guidance. We therefore draw the Working Group's attention to multi-stakeholder cybersecurity initiatives at the international level involving global technology companies, commissions and government coalitions, specifically (a) the Cybersecurity Tech Accord (b) The Global Commission on the Stability of Cyberspace (GCSC) (Norm 8) and (c) the Freedom Online Coalition (FOC) statement on cyber and human rights.

I.I.(a). The Cybersecurity Tech Accord

The Cybersecurity Tech Accord (Tech Accord) is a voluntary public commitment to promote a safer online world by fostering collaboration among more than 145 global technology companies. Together these global technology companies make a commitment to protect their customers and users and help them defend against malicious threats.[21] Signatories specifically commit to advancing the mission

[19] *See, e.g.*, UN Human Rights Committee, General Comment 34 Article 19: Freedoms of opinion and expression, 12 September 2011, U.N. Doc. CCPR/C/GC/34 available at https://www.refworld.org/docid/4ed34b562.html.
[20] *See* IEEE, Internet of Things Meets the Military and Battlefield, 2017, available at https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt .
[21] Tech Accord, About the Cybersecurity Tech Accord, 2021, available at https://cybertechaccord.org/about/

of the Tech Accord by "partnering on initiatives that improve the security, stability and resilience of cyberspace." Such commitments therefore include opposing cyberattacks against innocent civilians—including lawyers, civil society, human rights defenders—and enterprises.

The companies that have signed the Tech Accord have agreed to resist nation-state and criminal attacks to protect their customers, and have taken a step toward promoting corporate respect for the human rights of their users. The Tech Accord asks global tech companies not to assist governments in offensive operations, to protect technology against tampering, and to offer products that "prioritize" privacy and security. It does not identify the harms users face from these attacks, nor does it address the proactive steps companies should take to protect users, such as implementing data security and data privacy measures that would improve accountability across sectors. The Tech Accord could serve to apply more pressure on companies to respect human rights when developing and deploying their products. The Tech Accord does not commit the companies to participating in any particular process to promote protections for their users, such as the FOC, or to assess their own efforts, like the Global Network Initiative undertakes. The companies behind the Tech Accord also have the opportunity to demonstrate the work they are already doing in this area by promoting the United Nations Guiding Principles on Business and Human Rights, a framework that the technology sector can reinforce through innovative implementation.[22]

I.I.(b). The Global Commission on the Stability of Cyberspace (GCSC)

The Global Commission on the Stability of Cyberspace (GCSC or the Commission) was established to help "promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity."[23] GCSC specifically aims to support "policy and norms coherence related to the security and stability in and of cyberspace."[24] In this context, the GCSC convened to make recommendations for advancing cyberstability identifying a seven element Cyberstability Framework, including the development and implementation of voluntary norms.

In November 2019, the GCSC released a report to define and explore its Cyberstability Framework while developing principles, norms and recommendations for further action. In the report, the GCSC concluded that "non-state actors were not only critical for ensuring the stability of cyberspace, but that they too should be guided by principles and bound by norms."[25] The four principles stemming from this conclusion therefore call on *all parties* to "be responsible, exercise restraint, take actions, and respect human rights." In addition to the four principles, the GCSC also established a set of eight norms designed to "better ensure the stability of cyberspace and address technical concerns or gaps in previously declared norms." Norm 8 explains that "non-state actors should not engage in offensive cyber operations and state actors should prevent such activities and respond if they occur." In the

[22] Access Now, A Digital Rights Approach to the Tech Accord and the Digital Geneva Convention, September 2018, available at https://www.accessnow.org/cms/assets/uploads/2018/08/DGC-tech-accord-human-rights.pdf.
[23] Tech Accord, About the Cybersecurity Tech Accord, 2021, available at https://cybertechaccord.org/about/
[24] *Ibid.*
[25] Global Commission on the Stability of Cyberspace, Advancing Cyberstability Final Report, November 2019, available at https://cyberstability.org/report/

commentary accompanying Norm 8, the GCSC emphasizes that "states explicitly granting or knowingly allowing non-state actors the authorization to conduct offensive operations, for their own purposes or those of third parties, would set a dangerous precedent and risk violating international law." As a result "if states permit such action, they may therefore be held responsible under international law."[26]

The Government of Singapore provided an additional comment to supplement Norm 8 as proposed by the GCSC. Drawing upon the 2015 U.N. Group of Governmental Experts on Advancing responsible State behaviour in cyberspace (GGE)[27] Report, Singapore maintains that "if a state permits non-state actors to undertake offensive cyber operations, the states where the consequences of operations materialize may claim that the territorial state has breached its due diligence obligation."[28] As a result, "if that state does not comply with its obligation of due diligence, and thus does not take the necessary but feasible measures to terminate the cyber operations, the territorial state of the victim may resort to proportionate and necessary countermeasures and measures of retorsion to incentivize the state to comply with its obligation of due diligence."[29]

These norms build on the initial Call of the GCSC to protect the public core of the internet.[30] This essential norm, agreed in 2017, explicitly applies to "state and non-state actors." Among other manifestations, this norm speaks to the growing phenomenon of "internet shutdowns," or intentional disruptions of connectivity or blocking of social media platforms. In a stark, recent example, we observe the internet shutdowns levied in Myanmar by its military upon overthrowing the civilian government. These disruptions, carried out with the assistance of private companies, violate this norm and damage human rights, democracy, and security in the country.

In sum, international law does apply to states who allow non-state actors to engage in offensive cyber activities, and those states who fail to carry out adequate due diligence into actions by non-state actors under their jurisdiction or control may be held responsible by those states where harm occurs[31].

The emerging norms arise in part to pierce the impunity that states and non-state actors enjoy and promote to continue their pursuit of profits and power, without regard for adverse human rights and

---

[26] Global Commission on the Stability of Cyberspace, Advancing Cyberstability Final Report, November 2019, available at https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf at page 45.

[27] Developments in the Field of Information and Telecommunications in the context of international security, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Advancing responsible State behaviour in cyberspace in the context of international security, 22 July 2015, U.N. Doc. A/70/174, available at https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[28] Global Commission on the Stability of Cyberspace, Norm Package Singapore, Additional Note to the Norm Against Offensive Cyber Operations by Non-State Actors, available at https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf

[29] *Ibid.*

[30] Global Commission on the Stability of Cyberspace, Call to Protect the Public Core of the Internet, 21 November 2017, available at https://cyberstability.org/research/call-to-protect/

[31] This view is also supported by the findings of the second edition of the Tallinn Manual on the international law applicable to cyber operations, which we discuss later in this submission

humanitarian impacts. For example, see the "derivative sovereign immunity" arguments that cyber mercenaries like NSO Group are pushing, including in federal courts in California, in order to shield themselves from liability for their human rights violating and often criminal conduct.[32] We reject this interpretation of sovereign immunity statutes generally and in this case in particular,[33] because of their close relationship with states.[34] National security arguments that states use to shield cyber mercenaries from regulation, such as in the case of the State of Israel refusing to revoke NSO's license after extensive evidence of human rights violations, also need to be carefully scrutinized and challenged as violating the responsibilities placed on states by international law.[35]

I.I.(c) The Freedom Online Coalition

The Freedom Online Coalition (FOC) is a partnership of 32 governments working to advance Internet freedom. FOC Member States work closely together to coordinate their diplomatic efforts and engage with civil society and the private sector to support Internet freedom—free expression, association, assembly, and privacy online—worldwide.[36] The FOC specifically seeks to identify best practices regarding the application of human rights in the rapidly changing online landscape, and call attention to conditions that undermine those rights.

In February 2020, the FOC issued a joint statement on the human rights impact of cybersecurity laws, policies and practices. The statement, timely issued in advance of the February 2020 OEWG session held in New York, "reaffirms and builds on commitment the FOC made in 2016, while elaborating further on the human rights based approach to cybersecurity as a basis for strengthening cybersecurity, promoting stability in cyberspace, and promoting emerging technologies that are trust-worthy whilst ensuring the protection of all online users."[37] The FOC statement notes the challenges posed to business and government alike by the scarcity of domestic laws, international best practice, and private sector awareness of human rights abuses linked to the export of items with surveillance capabilities and tools to support efforts to conduct human rights due diligence to mitigate the risk of potential adverse human rights impact. The FOC statement concludes with a series of recommendations including the recommendation to States to encourage private sector actors "to adhere to the UN Guiding Principles on Business and Human Rights, to improve their accountability

[32] *See* Lawfare, "Why Is NSO Group Asserting Sovereign Immunity in WhatsApp Litigation?" 22 May 2020, available at https://www.lawfareblog.com/why-nso-group-asserting-sovereign-immunity-whatsapp-litigation

[33] Access Now, human rights organizations respond to NSO: victims' voices will not be silenced, 7 January 2021, available at https://www.accessnow.org/nso-victims-voices-will-not-be-silenced/

[34] Microsoft, Cyber mercenaries don't deserve immunity, 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/. Access Now, Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts, 2020, available at https://www.accessnow.org/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/.

[35] Amnesty International, Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence, 2020, available at https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/.

[36] Freedom Online Coalition, About, 2021, available at https://freedomonlinecoalition.com/.

[37] Freedom Online Coalition, Joint Statement on Human Rights Impact of Cybersecurity Laws, Practices and Policies, February 2020, available at https://freedomonlinecoalition.com/news/foc-issues-joint-statement-on-human-rights-impact-of-cybersecurity-laws-practices-and-policies/

and to share best practices in this respect and help to share lessons learned" and to "encourage private sector actors to promote and practice good cyber hygiene."[38]

II. Human Rights and International Humanitarian Law Impacts of Cyber-Capabilities and Operations Conducted by Actors Operating Alone or through PMSCs

II.I. Cyber Mercenaries under International Humanitarian Law, Public International Law, and International Criminal Law

The term 'mercenary' under the International Humanitarian Law is defined by Article 47 of Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (Additional Protocol I).[39] Under Protocol I, which only applies to international conflicts, a mercenary is a person who directly takes part in hostilities; is specifically recruited to take part in such hostilities; is motivated by private gain; is neither a national of or a resident of a Party to the conflict; is not a member of the armed forces of a Party to the conflict; and has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces. Under Article 47, mercenaries do not have the right to a combatant or a prisoner of war status. This rule is also a part of the Customary International Humanitarian Law, as confirmed by the Rule 108 of the 2005 ICRC customary IHL study.[40]

Rule 28 of the first edition of the Tallinn Manual,[41] which reflects the customary international law[42] applies Protocol I definition to cyber mercenaries. The Rule similarly excludes "mercenaries involved in cyber operations" from enjoying combatant immunity or prisoner of war status, thus qualifying them as "unprivileged belligerents." The second edition of the Tallinn Manual further cements this in its Rule 90,[43] and provides useful illustrations of activity covered by its definition of mercenaries involved in cyber operations - hinging on such activity meeting the six conditions set out by Article 47(2) of Additional Protocol I. Firstly, private companies located in a State A, engaged by State B to conduct cyber operations on its behalf in State C. Secondly, it illustrates that a "hacker for hire" who meets the criteria of the Additional Protocol would also be regarded as a mercenary involved in cyber operations even if they were acting alone and far removed from the battlefield. Rule 91 of the second edition of the Tallinn Manual also lays down that civilians forfeit their protection from attacks under

---

[38] *Ibid.*

[39] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (Additional Protocol I) U.N.T.S. 3, available at https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[40] ICRC, Customary International Humanitarian Law Volume I: Rules, 2009, Jean-Marie Henckaerts and Louise Doswald-Beck, Cambridge University Press, available online at https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf.

[41] The Tallinn Manual, originally called the Tallinn Manual on the International Law Applicable to Cyber Warfare, is a non-binding study on how international law applies to cyber conflicts and cyber warfare, available at https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

[42] UK Manual, paras 4.10-4.10.4 (as amended); Canadian Manual, para 319, German Manual para 303, ICRC Customary IHL Study, Rule 108 cited in the Tallinn Manual, Michael N. Schmitt, 2013, Cambridge University Press, available at https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf at footnote 26.

[43] Schmitt, M. (2013). Short form citations. In Tallinn Manual on the International Law Applicable to Cyber Warfare (pp. Xiv-Xx). Cambridge: Cambridge University Press.

international humanitarian law if they directly participate in cyber operations amounting to hostilities. Additionally, Rule 32 lays out that while peacetime cyber espionage by States does not per se violate international law, the manner by which it is carried out might do so. The explanatory text also explicitly notes that the group of experts believed that if cyber operations undertaken for espionage purposes violate the international human right to privacy - itself recognised as relevant to cyber operations under Rule 35 - then, the cyber espionage operation is unlawful. We also believe it useful to note the principles laid out by Rule 36, i.e. with respect to cyber activities, States must not only respect the international human rights of individuals, but also protect these rights from abuse by third parties.

While the subsequently adopted International Convention against the Recruitment, Use, Financing and Training of Mercenaries[44] and the Organization of African Unity Convention for the elimination of mercenarism in Africa,[45] have expanded the Protocol I mercenary definition to apply to situations of non-international armed conflict, the definition could be further refined and updated to reflect further developments in the space of cyber warfare. Since 2003, the reports of the Special Special Rapporteur on the Question of the Use of Mercenaries and the Working Group, which succeeded the mandate, have been highlighting the gaps in the existing legal mechanisms and criteria applied to mercenaries provided by private companies and the new technologies used in modern conflict. [46] While the Montreux Document[47] and the International Code of Conduct for Private Security Service Providers[48] attempt to bridge some of those gaps, binding international principles are needed to explicitly regulate cyber mercenaries and outline legal responsibilities of private technology companies as well as states that use their services to violate international human rights and international humanitarian law.

Cyber mercenaries and states deploying them to violate grave crimes should also be held responsible under International Criminal Law. Non-state actors can commit war crimes, crimes against humanity, and genocide and international tribunals and national courts have found such actors criminally (and

---

[44] UNGA, International Convention against the Recruitment, Use, Financing and Training of Mercenaries, 4 December 1989, entry into force 20 October 2001, OHCHR, available at https://www.ohchr.org/EN/ProfessionalInterest/Pages/Mercenaries.aspx.

[45] Organization of African Unity Convention for the Elimination of Mercenarism in Africa, 3 July 1977, registered by the Organization of African Unity on 15 January 1988, available at https://treaties.un.org/doc/Publication/UNTS/Volume%201490/volume-1490-I-25573-English.pdf.

[46] Commission on Human Rights, The Right of Peoples to Self-Determination and Its Application to Peoples Under Colonial or Alien Domination or Foreign Occupation, 24 December 2003, U.N. Doc. E/CN.4/2004/15 available at https://undocs.org/E/CN.4/2004/15; UNGA, Right of peoples to self-determination, 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 evolving forms, trends and manifestations of mercenaries and mercenary-related activities, 28 July 2020, U.N. Doc. A/75/259 available at https://undocs.org/en/A/75/259; OHCHR, 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, Mercenarism and Private Military and Security Companies, 2018, U.N. Doc. HRC/None/2018/40, available at https://www.ohchr.org/Documents/Issues/Mercenaries/WG/MercenarismandPrivateMilitarySecurityCompanies.pdf.

[47] ICRC, The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict, 11 June 2020, available at https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies#:~:text=The%20Montreux%20Document%20on%20Private%20Military%20and%20Security%20Companies,-Publication%2011%20June&text=The%20Montreux%20Document%20is%20an,are%20present%20in%20armed%20conflicts.

[48] Private Security Governance Observatory, The International Code of Conduct for Private Security Service Providers, available at http://observatoire-securite-privee.org/en/content/international-code-conduct-private-security-service-providers-icoc#:~:text=Service%20Providers%20(ICoC)-,The%20International%20Code%20of%20Conduct%20for%20Private%20Security%20Service%20Providers,the%20interests%20of%20their%20clients.

civilly) liable in the past.[49] State officials that hire such actors can also be held accountable for their crimes, even though some forms of criminal liability (like superior liability)[50] which require a showing of command and control over the subordinate actors, may be harder to establish when it comes to cyber mercenaries. Nevertheless, officials who order the commission of devastating cyber attacks or fail to prevent such attacks by mercenaries under their control should not evade accountability.

II.II. Government hacking impinges internationally protected human rights

In our 2016 report on 'A human rights approach to Government Hacking',[51] we came to the conclusion that all government hacking substantially interferes with human rights, including the right to privacy and freedom of expression. We consider government hacking in three categories based on the broad goal to be achieved: (1) to control a message, (2) to cause damage, or (3) to conduct surveillance. While in many ways this interference may be similar to more traditional government activity, the nature of hacking creates new threats to human rights that are greater in both scale and scope. Hacking can provide access to protected information, both stored or in transit, or even while it is being created or drafted. Exploits used in operations can act unpredictably, damaging hardware or software or infecting non-targets and compromising their information. Even when a particular hack is narrowly designed, it can have unexpected and unforeseen impact. Based on analysis of human rights law, we concluded that there must be a presumptive prohibition on all government hacking.

II.III International human rights expert calls for moratorium on surveillance technologies

We believe the present expert group should join and strengthen the calls for a moratorium on surveillance technologies made by the UN's special mandate holders in the human rights system. The May 2019 report of the UN Special Rapporteur on Freedom of Expression called for an immediate moratorium on the sale, transfer and use of surveillance tools, noting that:[52]

> "Surveillance tools can interfere with human rights, from the right to privacy and freedom of expression to rights of association and assembly, religious belief, non-discrimination, and public participation. And yet they are not subject to any effective global or national control,"

The report of the UN Special Rapporteur on Freedom of Expression gave examples of computer intrusions, mobile device hacking, network intrusion, facial recognition surveillance and other highly sophisticated surveillance tools that have been used by States and other actors to monitor journalists,

---

[49] American Society of International Law, Accountability of Private Security Contractors under International and Domestic Law, 26 December 2007, Volume 1 Issue 31, available at https://www.asil.org/insights/volume/11/issue/31/accountability-private-security-contractors-under-international-and#_edn1.

[50] ICLS- OSCE-ODIHR, International Criminal Law and Practice Training Materials, Modes of Liability: Superior Responsibility https://iici.global/0.5.1/wp-content/uploads/2018/03/icls-training-materials-sec-10-superior-responsibility.pdf.

[51] Access Now, A human rights approach to Government Hacking, September 2016, available at https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

[52] Report on the adverse effect of the surveillance industry on freedom of expression, 28 May 2019 A/HRC/41/35, available at https://www.undocs.org/A/HRC/41/35.

politicians, UN investigators and human rights advocates. States were urged to adopt domestic safeguards in accordance with international human rights law to protect individuals from unlawful surveillance, particularly the development of public mechanisms for approval and oversight of surveillance technologies, along with the strengthening of export controls and assurance of legal tools of redress.

Both the High Commissioner for Human Rights Michelle Bachelet,[53] and the Special Rapporteur on racism, E. Tendayi Achiume, have joined calls for a moratorium on the sale, transfer or use of surveillance technologies.[54]

Concluding Recommendations

1. The Working Group should promote the review and reform of existing frameworks and mechanisms addressing private security contractors for the digital age, with attention to human rights and humanitarian frameworks and full involvement of civil society;
2. States, international organizations, and the private sector should continue to require ICoCA membership in their procurement practices and contractual obligations to increase enforcement beyond borders;
3. Companies that have signed the Cybersecurity Tech Accord should further develop their commitments, and support the development of global standards for attribution of cyber attacks;
4. Further develop the Cybersecurity Tech Accord to clearly articulate the extent and boundaries of the problems at issue; the methods participating companies will use to address them; and how the accord interacts with existing efforts on business and human rights;
5. Call for binding international principles to explicitly regulate cyber mercenaries and outline legal responsibilities of private technology companies and states that use their services to violate international human rights and international humanitarian law;

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

[53] New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States, June 2020, available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25996&LangID=E

[54] Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Report of the United Nations High Commissioner for Human Rights, 2020, A/HRC/44/24, available at https://undocs.org/A/HRC/44/24.

For more information, please contact: ***un@accessnow.org***