WOMEN'S INTERNATIONAL LEAGUE FOR
PEACE & FREEDOM

Submission to the Working Group on the use of mercenaries

report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact

Submitted on 12 February 2021

For more information, please contact:
Women's International League for Peace and Freedom (WILPF)
Rue de Varembé 1, Case Postale 28, 1211 Geneva 20, Switzerland
Email: secretariat@wilpf.org| Tel: +41 (0) 22919 70 80 | Web: wilpf.org

I. Introduction

The Women's International League for Peace and Freedom (WILPF) welcomes the Working Group's focus on cyber mercenaries. WILPF opposes the militarisation of cyberspace and is supportive of solutions that advance cyber peace. WILPF views military privatisation in the context of neoliberal restructuring of the state, as well as part of a broader transformation in governance and the commercialisation of security. Within this context, the militarisation and misuse of technology only serves to expand, exacerbate, and create violence in new mediums or with new tools, while entrenching existing systemic and root causes of violence, discrimination, and oppression. Our work in this area is guided by the understanding that hostile cyber activity, along with all remote and technology-facilitated violence, must be understood as an expansion of existing patriarchal structures of power.

This submission is guided by the questions the Working Group has provided. We respond to key themes raised by the questions but given their complex and interrelated nature, it is not always possible to respond to each question separately.

Noting that there is no formal definition of a "cyber mercenary," we work within the description provided by the Working Group in its call for submissions.[1] We offer some reflection on terminology in Annex I, alongside examples of these actors in Annex II.

II. Current trends and developments

The use of cyber mercenaries is an old problem dressed up in new clothing. There are specific characteristics of the so-called cyber domain that allow non-state actors such as mercenaries to flourish in novel ways, and which raise unique legal and policy challenges. These are outlined in Annex I. Yet core elements of cyber mercenary behaviour, particularly when they are employed by governments or other authorities, are in keeping with how such groups have operated and been used

[1] See: https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx. As much as possible, our submission has focused more on actors that are motivated for financial or personal gain over purely ideological reasons; and those that have been employed or sponsored by governmental or other authorities, rather than by private individuals or criminal networks. We note it's not always possible to make these distinctions.

historically, reinforcing existing concerns about the privatisation of security services and growth in remote warfare and violence.

Characteristics of cyber mercenaries

The existing literature on cyber mercenaries tends to focus on the activities and composition of a wide range of non-state actors in which some researchers identify mercenaries as an entire category of actor;[2] others view cyber mercenaries as subset of other types of non-state actor;[3] while yet others do not use the term at all.[4] Whether named as mercenaries or not, these non-state actors perform varied functions that sometimes overlap.

In Annex II, we offer examples from a cross-section of mercenary or mercenary-like actors in order to outline the range of roles in which they engage, as well as certain products and services that they provide. This includes advanced persistent threat (APT) groups; cyber militias; private software and technology companies; private contractors and individuals; private military and security companies (PMSCs); and weapons producers. These examples show that mercenaries are active in espionage; data collection and theft; coordinating cyber operations; surveillance; providing access to threat intelligence; and developing and selling a range of cyber products and services. The range of products include malware, including stalkerware, surveillance software (or spyware) and ransomware, as well as surveillance equipment and other technology.

Motivations

Despite some of the unique facets of cyberspace that can empower mercenary-like actors in new ways, the strategic and political motivations that drive states or authorities to work with them are consistent

[2] Nicolo Bussolati lists cyber mercenaries as one of five classifications of non-state actors in "The Rise of Non-State Actors in Cyberwarfare" in *Cyberwar: Law and Ethics for Virtual Conflicts*, edited by Jens David Ohlin, Kevin Govern, and Claire Finkelstein, 2015, p. 102. Tim Maurer focuses exclusively on the role of cyber mercenaries in his research; see for example, *Cyber Mercenaries: The State, Hackers, and Power*, 2017.

[3] Johan Sigholm names cyber mercenaries as an element of cyber militias, and views cyber militias as one of 13 classifications of non-state actors in cyberspace. See, "Non-state actors in cyberspace operations," *Swedish National Defence College*, 2013, https://doi.org/10.1515/jms-2016-0184.

[4] Jamie Collier's work on non-state actors does not list mercenaries as a category. See Jamie Collier, "Proxy Actors in the Cyber Domain", *St Antony's International Review*, Vol. 13, No. 1, 2017, https://www.jstor.org/stable/10.2307/26229121, p.33.

with how such actors have been used historically by states to expand power, such as through their use of navies, pirates, and privateers.[5]

Among the most commonly cited factors that motivate states to use a proxy, including mercenaries, are plausible deniability, cost effectiveness, avoidance of direct intervention, and to prevent conflict escalation.[6] 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 cyber operation in a timely way. Examples include Russia-linked cyber militia activities against Georgia in 2007;[7] the operation targeting Saudi petroleum company Aramco and Qatar's RasGas in 2012, linked to an "independent" Iranian hacking group;[8] the 2014 Sony Hack associated with North Korea;[9] and multiple China-linked operations targeting Japan in 2009 and earlier, that occurred in the context of geopolitical disputes between the two countries.[10]

Many of the categories of non-state actors described in Annex II are composed of individuals who may move from public to private sector and back again, in a revolving door pattern reminiscent of that which already exists between some governments and their national weapons producers.[11] The weaponisation of technology and the fabrication of a new space for war-fighting has profit incentives and motivations for private industry in a way not dissimilar from the established military-industrial

[5] Florian Egloff, "Cybersecurity and the Age of Privateering: a historical analogy," Cyber Studies Programme, Working Paper Series 1, no. 1, 4 March 2015, pp. 1–14.

[6] There is not a lot of literature looking at motivations to employ cyber mercenaries specifically. This draws from what has been written about state use of proxy actors in cyberspace, in ways consistent with our examples in Annex II. See Collier; Maurer; and Sigholm, as well as Manuel R. Torres Soriano, "Proxy Wars in Cyberspace", June 2017 and Justin Key Canfil, "Outsourcing Cyber Power: Why Proxy Conflict in Cyberspace May No Longer Pay", May 2020, https://ssrn.com/abstract=3611582/.

[7] Richard B Andres, "Cyber-Gang Warfare," *Foreign Policy,* 12 February 2013, http://foreignpolicy.com/2013/02/12/cyber-gang-warfare/.

[8] Kim Zetter, "The NSA acknowledges what we all feared: Iran learns from US cyberattacks", *Wired,* 10 February 2015, https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/.

[9] Andrea Peter, "The Sony Pictures Hack, explained", *The Washington Post,* 18 December 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

[10] "Japan Trying to Fend Off Chinese Cyber-Attacks", 27 October 2009, https://www.voanews.com/archive/japan-trying-fend-chinese-cyber-attacks.

[11] Ron Deibert, *Reset: Reclaiming the Internet for Civil Society*, 2020, p.149.

complex.[12] As WILPF has noted, "Privatisation creates a continuous push to expand the market. Driven by profits, PMSCs seek to extend narratives and claims of protection to the global scale so as to expand their market access. "In promising to 'deliver the impossible' 'anytime, anywhere'… PMSCs seek to (re)define who is a legitimate and effective protector and who and what needs protecting."[13] In cyberspace, this means manufacturing a narrative of constant vulnerability and danger that may not always accurately reflect the realities of a given situation, and which enables certain actors to undertake offensive and aggressive actions under the guise of "defence".[14]

Remote harm and technology-facilitated violence

Building on the above information, and in response to the question about the role of new technologies in causing remote harm (Question #5), WILPF views cyber operations as fitting within a shift toward ever-more remote violence and warfare. Foreign military bases, uncrewed aerial vehicles (UAVs), surveillance equipment, and autonomous weapons all fit within this frame, in which physical distance between perpetrator and target facilitates an easier devaluing of human life and dignity.[15] As WILPF and others have argued in the context of UAVs, this is a discourse "that is grounded in elite, militarised

[12] Ron Deibert, "The New Cyber Military Industrial Complex," *The Globe and Mail,* 2 May 2011, https://deibert.citizenlab.ca/2011/05/the-new-cyber-military-industrial-complex-globe-and-mail/.

[13] Submission by the Women's International League for Peace and Freedom (WILPF) on *Private Military and Security Companies (PMSCs) and Gender to the Working Group on Mercenaries*, March 2019, https://www.ohchr.org/Documents/Issues/Mercenaries/WG/Gender/WILPF_PMSCs_Gender.pdf.

[14] It is increasingly recognised that defensive cyber operations and activities include offensive action, such as "hacking back" into an adversary's network in retaliation, while an increasing number of private corporations offering a range of aggressive defensive services to other corporations transnationally.

[15] Relevant publications from WILPF and its partners include: Ray Acheson, *Remote warfare and sexual violence in Djibouti*, July 2017; Ray Acheson, *Feminist perspectives on autonomous weapon systems: briefing paper series,* December 2020, https://reachingcriticalwill.org/resources/publications-and-research/publications/14975-feminist-perspectives-on-autonomous-weapon-systems?limitstart=0; Ray Acheson, Matthew Bolton, Elizabeth Minor, and Allison Pytlak (eds.), *The Humanitarian Impact of Drones,* 2017, https://reachingcriticalwill.org/resources/publications-and-research/publications/11960-the-humanitarian-impact-of-drones?limitstart=0; and Ray Acheson, "COVID-19: The Risks of Relying on Technology to "Save Us" from the Coronavirus," 2020, https://www.wilpf.org/covid-19-the-risks-of-relying-on-technology-to-save-us-from-the-coronavirus/.

power structures, where capacities for violence are bolstered by access to high technology and the ability (and willingness) to project violence far beyond one's own borders."[16]

Most of the harm caused by cyber operations is remote, whether it be surveillance activities of law enforcement, data breaches, or offensive operations on critical infrastructure.[17] The 2017 WannaCry ransomware operation, now linked to North Korea, affected an estimated 230,000 computers in 150 countries, leading to the cancellation of surgeries and impacting other medical care especially in the United Kingdom.[18] Throughout the COVID-19 pandemic, ransomware operations of cyber mercenaries and criminals targeting medical facilities have ballooned in ways that have had a real impact on physical well-being of individuals, including the death of one person in Germany.[19]

Cyber operations, especially those conducted by mercenary or proxy, therefore create challenges for how the concept of direct participation is defined and applied. A perpetrator can be on the "frontline" of an operation, including in contexts of armed physical conflict, without needing to leave their home state, or possibly even their home.[20] One suggestion has been to conceptualise participation in cyber operations in terms of non-physical proximity to critical data or functions of a system.[21] There are also implications for the responsibility assigned to those employing these actors. One typology establishes three types of state-proxy cyber relationships—delegation, orchestration, and sanctioning—with the caveat that even these run along a spectrum.[22]

---

[16] Ray Acheson, Matthew Bolton, and Elizabeth Minor, "Introduction", in *The Humanitarian Impact of Drones*, p.7.

[17] Tim Maurer and Wyatt Hoffman, *The Privatization of Security and the Market for Cyber Tools and Services*, Geneva Centre for Security Sector Governance, 2019, p.5.

[18] See https://www.kaspersky.com/resource-center/threats/ransomware-wannacry and James Lewis, "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine," in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, 2015.

[19] Joe Tidy, "Police launch homicide inquiry after German hospital hack", *BBC News*, 18 September 2020, https://www.bbc.com/news/technology-54204356.

[20] Mauer and Hoffman, p.7.

[21] Ibid.

[22] Tim Maurer, *Cyber mercenaries: The state, hackers, and power*, 2018.

III. Regulatory frameworks and their application

The behaviour of cyber mercenaries or similar actors is not specifically addressed by any one legal, normative, or regulatory agreement. There are multiple instruments, frameworks, and laws that can be applied and/or are relevant, but each tends to focus on only one aspect of the problem, thus creating loopholes, while others are poorly implemented or understood. The characteristics of cyberspace additionally present unique legal and regulatory challenges that may require either the development of new laws or frameworks, or that existing regulation be updated and reinterpreted for a digital age.[23]

For example, while most states agree that international law applies to cyberspace, there is not yet much specificity as to how it is being interpreted and applied.[24] Most cyber operations lead to effects

[23] Some relevant frameworks or elements of international law include: the UN Charter; the 2013 and 2015 Final Reports of the UN Group of Governmental Experts on advancing responsible state behaviour in cyberspace; the Tallinn Manual; the Convention on Cybercrime; the Geneva Conventions (Articles 47(1) and 47(2) of Additional Protocol I; Article 4A (2) of the Third Geneva Convention); the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts; the United Nations Mercenary Convention; the UN Secretary-General's Roadmap for Digital Cooperation; UN General Assembly resolution 73/218 of 20 December 2018 on the information and communications technologies for sustainable development; 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.

Some relevant frameworks or elements of the international human rights framework include: The International Covenant on Civil and Political Rights (article 19 and article 17(1)); the Universal Declaration of Human Rights protect everyone's rights to privacy, opinion and expression; the UN Guiding Principles on Business and Human Rights; the UN Declaration of Human Rights; the International Covenant on Civil and Political Rights; General Comment No. 16 (1998) of the Human Rights Committee on the right to privacy; the Vienna Declaration and Programme of Action (paragraph 11), the Principles on Personal Data Protection and Privacy; and all relevant Human Rights Council resolutions, listed below. For a comprehensive overview of applicable human rights framework, see the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, 28 May 2019.

Applicable international export control: Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies; as well as domestic domestic export controls.

[24] This was first affirmed in the 2013 Final Report of the UN Group of Governmental Experts on state behaviour in cyberspace. See *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/68/98, 24 June 2013,

that fall short of the threshold of traditional understandings of the "use of force" or an "armed attack" but are nevertheless harmful or even destabilising. Issues like these come into focus when considering cyber activities that seem low impact, such as espionage or disinformation, but culminate in election interference, such as in Ukraine in 2014-15, and 2019[25] and the United States in 2016.[26]

Adding complexity to the question of whether the effects of these activities amount to an act of war is the problem of determining responsibility for those activities. For instance, it is believed that the Russian government is linked to the electoral operations targeting Ukraine[27] and the US[28] but confirming who carried out those operations; their precise relationship to the government or its military structures; and from where their orders emanated, is infinitely more complicated given the web of proxy cyber relationships that a state may hold.

Even if an indisputable connection is established between a non-state proxy and a state, such a connection does not legally grant the individuals responsible for cyberattacks combatant status under IHL, should the operation take place in a physical armed conflict. In fact, certain core IHL principles and concepts that would apply to mercenary or non-state actors in a physical battlefield require

---

https://undocs.org/A/68/98. It was affirmed by the subsequent GGE in its 2015 report. See *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/70/174, 22 July 2015, https://undocs.org/A/70/174.

[25] Laurens Ceruleus, "How Ukraine became a test bed for cyberweaponry", *Politico*, 14 February 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

[26] Ryan Goodman, "International Law and the US Response to Russian Election Interference", Just Security, 5 January 2017,https://www.justsecurity.org/35999/international-law-response-russian-election-interference/.

[27] *Post-Election Assessment Of The Cybersecurity Infrastructure And Interagency Cooperation In Ukraine With Related Recommendations*, Estonia Center of Eastern Partnership, Cybexer Technologies, and the European Union, https://eceap.eu/wp-content/uploads/2019/11/Post-Election-Assessment-RecommendationsFINAL.pdf and International Election Observation Mission: Ukraine—Presidential Election, *Statement of Preliminary Findings and Conclusions,* 31 March 2019, https://www.oscepa.org/documents/election-observation/election-observation-statements/ukraine/statements-25/3833-2019-1-presidential-eng/file.

[28] *Report of the Select Committee on Intelligence of the United States Senate, on Russian active measures campaigns and interference in the 2016 U.S. Election, Volume 1: Russian efforts against election infrastructure*, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf and *Volume 2: Russia's use of social media*, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

additional scrutiny with respect to cyber actors. For example, articles that pertain to determining who is a combatant include criteria that do not always make sense in cyber operations, such as carrying arms openly, or having a command and organisational structure (i.e. some of the actors listed in Annex II are deliberately informal and horizontal in their structure, or small in number).[29]

When responsibility is attributed, the most frequent outcome is that individuals are charged under national criminal laws of the country that was targeted or are sanctioned.[30]

Some of the private sector entities highlighted in Annex II take advantage of patchy criminal laws and jurisdictional ambiguity, particularly in relation to the products they manufacture, a pattern similar to that followed by weapons companies.[31] "The chips are made in X, assembled in Y, and the software is written all over the world by 125 different nationals."[32]

Companies can sell surveillance software directly to countries that may be under a UN arms embargo and where there is a demonstrated record of human rights abuse and repression. There have been some efforts to update existing arms control agreements like the Wassenaar Arrangement to include intrusion software and network surveillance equipment in 2012. Pushback from the cyber security industry, however, led to the creation of exemptions to this in 2019, largely at the behest of the United States.[33] In 2019 the UN Special Rapporteur on freedom of opinion and expression called for an

[29] Sigholm, pp.27-28 and Bussolati.

[30] See for example: "Mueller charges 13 Russians with interfering in US election to help Trump", *The Guardian*, 17 February 2018, https://www.theguardian.com/us-news/2018/feb/16/robert-mueller-russians-charged-election; "U.S. charges, sanctions Iranians for global cyber attacks on behalf of Tehran", *Reuters*, 23 March 2018, https://www.reuters.com/article/us-usa-cyber-iran/u-s-charges-iranians-for-global-cyber-attacks-on-behalf-of-tehran-idUSKBN1GZ22K.

[31] This is not necessarily a new problem—weapons companies often are headquartered in one country, produce parts and components elsewhere, and assemble the final product in a third location, evading national requirements around arms transfers and human rights. See, for example, WILPF's 2020 submission to the Committee on the Rights of the Child's review of Canada: https://www.reachingcriticalwill.org/images/documents/Disarmament-fora/att/WILPF_CRC_June2020.pdf.

[32] Neri Zilber, "The Rise of the Cyber Mercenaries", *Foreign Policy,* 31 August 2018, https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/.

[33] Garrett Hinck, "Wassenaar Export Controls on Surveillance Tools: New Exemptions for Vulnerability Research", *Lawfare*, 5 January 2018, https://www.lawfareblog.com/wassenaar-export-controls-surveillance-tools-new-exemptions-vulnerability-research.

immediate moratorium on the sale, transfer and use of surveillance technology,[34] an initiative that has not been successful.[35] In November 2020, the European Union (EU) updated its export control system for dual-use items[36] following civil society advocacy highlighting the outflux of digital surveillance tools from EU member states.[37]

There may not be a "one size fits all" solution for the specific challenges of cyber mercenary actors, but certainly there is a need for cohesion and communication across relevant communities of security, human rights, and cyber crime, in order to close gaps. More than that, international law and regulatory frameworks need both updating and enforcement.

IV. Human rights impacts of cyber-capabilities and operations conducted by actors operating alone or through PMSCs[38]

In 2012, the UN Human Rights Council (HRC) adopted by consensus a key resolution that affirmed that "the same rights that people have offline must also be protected online."[39] The human rights impact of cyber capabilities and operations is extensive and growing.[40] It's beyond the scope of this submission to provide an exhaustive review of all intersections between technology and human rights—

[34] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736&LangID=E

[35]https://www.business-humanrights.org/en/latest-news/un-draft-text-on-digital-rights-ducks-call-for-spyware-moratorium/

[36] European Commission, "Commission welcomes agreement on the modernisation of EU export controls", 9 November 2020, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2209.

[37] Joint Letter Re: Strengthening the European Commission Position on Dual-Use Recast, 9 June 2020, https://www.hrw.org/news/2020/06/09/joint-letter-re-strengthening-european-commission-position-dual-use-recast.

[38] We do not respond to the question about IHL in this section, but have touched on IHL considerations somewhat in Section II and certain of the examples in Annex II.

[39] *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13, 29 June 2012, https://undocs.org/A/HRC/20/L.13.

[40] These range from issues of meaningful access to the internet and internet shutdowns, and what that can mean for rights to education and health; to gender-based violence against women, men, non-binary and LGBT+ people; sexual exploitation of children; and issues of hate speech, cyber racism, cyber bullying, and disinformation.

in this section we focus on rights that are more frequently at risk in relation to the cyber mercenary actors included in Annex II.

Surveillance and the right to privacy

Many of the actors highlighted in Annex II are engaged in some form of surveillance, the impacts of which are very harmful and increasingly well-documented.

This has led to several pronouncements by human rights mechanisms and bodies. The 2020 Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression looks closely at and identifies several forms of surveillance: mobile phone hacking, social engineering, network surveillance, facial recognition, International Mobile Subscriber Identity catchers (Stingrays), and deep packet inspection.[41] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has also raised the issue of surveillance and the right to privacy.[42]

Through a 2020 resolution on "The right to privacy in the digital age," the UN General Assembly emphasised that:

[41] *Surveillance and human rights*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/42/35, paragraphs 6-14.

[42] See for instance: *Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family*, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/46/36, 22 January 2021, particularly paragraphs 11 and 16 . See also: *Human rights impact of policies and practices aimed at preventing and countering violent extremism,* Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/43/46, 21 February 2020; *Recent developments and thematic updates*, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/34/61, 21 February 2017; *Impact of counter-terrorism measures on civil society,* Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/70/371, 18 September 2015; *Counter terrorism and mass digital surveillance,* Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014.

> "unlawful or arbitrary surveillance and/or interception of communications, as well as the unlawful or arbitrary collection of personal data, hacking and the unlawful use of biometric technologies, as highly intrusive acts, violate the right to privacy, can interfere with the right to freedom of expression and to hold opinions without interference, the right to freedom of peaceful assembly and association and the right to freedom of religion or belief and may contradict the tenets of a democratic society, including when undertaken extraterritorially or on a mass scale".

This follows the 2019 Human Rights Council resolution on "The right to privacy in the digital age". [43] Importantly, the HRC expressed concern "at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights."[44]

[43] *The right to privacy in the digital age*, A/HRC/RES/42/15, 7 October 2019, A/HRC/RES/42/15, 7 October 2019, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/297/52/PDF/G1929752.pdf?OpenElement. See resolutions from past years: The right to privacy in the digital age, A/HRC/37/2, 22 March 2018; The right to privacy in the digital age, A/HRC/RES/28/16, 2015

Other relevant HRC resolutions on digital services and surveillance and concerns about privacy and freedom of expression and assembly:

New and emerging digital technologies and human rights, A/HRC/RES/41/11, 17 July 2019.

The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/26/13, 26 June 2014

[44] *The right to privacy in the digital age*, A/HRC/RES/28/16, 2015.

The Human Rights Committee addressed the issue of surveillance in numerous concluding observations, notable of which are those to Lebanon,[45] Italy,[46] and France.[47] Relevant

[45] Concluding observations to Lebanon, CCPR/C/LBN/CO/3 (CCPR 2018): "33.The Committee is concerned about reports of arbitrary interference with the privacy of individuals, including allegations of mass surveillance of digital communications; allegations of direct authorizations by the Prime Minister of the interception of private communications and access to data without the prior judicial authorization required by law; and the granting of full telecommunications data access to security agencies, following the relinquishment of the authority of the Council of Ministers to approve or deny such requests. The Committee is also concerned about the insufficient protection of biometric data under the current legal framework and notes that a bill on this issue was submitted to the Standing Committee of the Parliament (arts. 2 and 17)."

"34. The State party should ensure that all laws governing surveillance activities, access to personal data and communications data (metadata) and any other interference with privacy are in full conformity with the Covenant, in particular article 17, including as regards the principles of legality, proportionality and necessity, and that State practice conforms thereto. It should, inter alia, ensure that (a) surveillance, collection of, access to and use of data and communications data are tailored to specific legitimate aims, are limited to a specific number of persons and are subject to judicial authorization; (b) effective and independent oversight mechanisms are in place to prevent arbitrary interference with privacy; and (c) affected persons have proper access to effective remedies in cases of abuse. The State party should also ensure biometric data protection guarantees, in accordance with article 17 of the Covenant."

[46] See Concluding observations to Italy, CCPR/C/ITA/CO/6 (CCPR 2017): 36. The Committee is concerned about reports that intelligence agencies are intercepting personal communications and employing hacking techniques without explicit statutory authorization or clearly defined safeguards from abuse. It is also concerned that the anti-terrorism decree and Law No. 21/2016 compel telecommunications service providers to retain data beyond the period allowed by article 132 of the personal data protection code, and that the authorities can access such data without authorization from a judicial authority. It is further concerned about allegations that companies based in the State party have been providing online surveillance equipment to Governments with a record of serious human rights violations and about the absence of legal safeguards or oversight mechanisms regarding the export of such equipment (art. 17)."

"37.The State party should review the regime regulating the interception of personal communications, the hacking of digital devices and the retention of communications data with a view to ensuring: (a) that such activities conform with its obligations under article 17, including the principles of legality, proportionality and necessity; (b) that robust, independent oversight systems are in place regarding surveillance, interception and hacking, including by ensuring that the judiciary is involved in the authorization of such measures, in all cases, and by affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were placed under surveillance or that their data was hacked; and (c) that measures

recommendations have also been made under the Universal Periodic Review (UPR) to Chile;[48] Kenya;[49] and the United States, the latter of which emphasised respect for privacy of individuals outside of its territorial borders.[50]

---

are taken to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad."

[47] See Concluding observations to France, CCPR/C/FRA/CO/5 (CCPR 2015):

"12. The Committee is concerned about the powers granted to the intelligence services for digital surveillance both within and outside France. The Committee is particularly concerned about the fact that the law on intelligence adopted on 24 June 2015 (submitted to the Constitutional Court) gives the intelligence agencies excessively broad, highly intrusive surveillance powers on the basis of broad and insufficiently defined objectives, without the prior authorization of a judge and without an adequate and independent oversight mechanism (art. 17)." "The State party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular article 17. Specifically, measures should be taken to guarantee that any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity. The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail. It should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the judiciary to take part in the authorization and monitoring of surveillance measures."

[48] UPR of Chile (2019). Recommendation 125.109: "Adopt specific legislation to protect and promote human rights in the digital environment, including the right to privacy" (Brazil)

[49] UPR of Kenya (2015): "Review its national laws and policies in order to ensure that surveillance of digital communications is consistent with its international human rights obligations and is conducted on the basis of a legal framework which is publicly accessible, clear, precise and non-discriminatory" (Liechtenstein)

[50] UPR of US (2015): "Strengthen the independent federal-level judicial and legislative oversight of surveillance activities of all digital communications with the aim of ensuring that the right of privacy is fully upheld, especially with regard to individuals outside the territorial borders of the United States" (Hungary). See also similar recommendations to the United States by other states: "Respect international human rights obligations regarding the right to privacy when intercepting digital communications of individuals, collecting personal data or requiring disclosure of personal data from third parties" (Germany); "Review their national laws and policies in order to ensure that all surveillance of digital communications is consistent with its international human rights obligations and is conducted on the basis of a legal framework which is publicly accessible, clear, precise, comprehensive and non-discriminatory" (Liechtenstein); "Respect the privacy of individuals outside the United States in the context of digital communications and data" (Pakistan)

Right to freedom of expression, association, and peaceful assembly

Various human rights mechanisms have expressed concern about the impacts on freedom of expression, association and peaceful assembly, particularly with respect to human rights defenders and journalists, provided or facilitated by "cyber mercenaries".

The HRC has adopted various resolutions expressing concerns about freedom of expression in cyberspace.[51] Notably, the HRC called upon states "to refrain from the use of digital technology to silence, unlawfully or arbitrarily surveil, or harass individuals or groups" for being involved in peaceful protests, "or from ordering blanket Internet shutdowns and from blocking websites and platforms around protests or key political moments; and to refrain from applying any undue restrictions to technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity online."[52]

Different human rights bodies have also made recommendations amidst concerns of violations of freedom of expression that are put in place through restrictions under the guise of "combatting" cyber

[51] *Freedom of opinion and expression*, A/HRC/RES/44/12, 24 July 2020

The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/20/8, 5 July 2012

Situation of human rights in the Libyan Arab Jamahiriya, A/HRC/RES/S-15/1, 25 February 2011 (Libyan authorities shutting down Internet access)

The current human rights situation in the Syrian Arab Republic in the context of recent events, A/HRC/RES/S-16/1, 29 April 2011 (access to Internet)

The human rights situation in the Syrian Arab Republic, A/HRC/RES/S-18/1, 2 December 2011 (shut down of Internet)

Situation of human rights in Myanmar, A/HRC/RES/16/24, 25 March 2011 (censorship on the Internet)

Situation of human rights in Myanmar, A/HRC/RES/13/25, 26 March 2010 (censorship on the Internet)

[52] *The promotion and protection of human rights in the context of peaceful protests*, A/HRC/RES/44/20, 23 July 2020, paragraphs 24 and 25.

The resolution also expresses its concern "at the unlawful or arbitrary surveillance, both in physical spaces and online, of individuals engaged in peaceful protests, including through the use of new and emerging digital tracking tools, such as facial recognition, international mobile subscriber identity-catchers ("stingrays") and closed-circuit television" (OP 23).

crime.[53] Relevant UPR recommendations have been made to Bangladesh;[54] Tanzania;[55] Viet Nam;[56] Cambodia;[57] Lao PDR;[58] Iran;[59] and the United Arab Emirates.[60]

[53] Some countries have made certain online activities illegal in order to increase their control over how civil society actors use digital technologies. See for example: Concluding observations to Bangladesh, E/C.12/BGD/CO/1 (CESCR 2018), paragraph 12: "The Committee recommends that the State party ensure a safe and favourable environment for human rights defenders, review the above-mentioned legislation in close consultation with such defenders with a view to removing restrictive provisions, including section 57 of the Act on information and communications technology and similar provisions in the draft act on digital security of 2018, and repeal the Special Powers Act, 1974. The Committee draws the attention of the State party to its statement on human rights defenders and economic, social and cultural rights."

[54] UPR of Bangladesh (2018). Recommendation 149.48: "Ensure that human rights activists and journalists can exercise their rights without fear, intimidation and harassment by redrafting the planned Digital Security Act, and repealing or amending all laws that violate the rights to freedom of expression, association and peaceful assembly, including the provisions of the Penal Code related to defamation and sedition, the Information and Communication Technology Act (in particular section 57), and the Foreign Donations (Voluntary Activities) Regulation Act, in line with international human rights law" (Germany)
See also: Recommendation 148.15: "Redraft the Digital Security Act in line with international norms and standards for freedom of expression" (Sweden)
Recommendation 148.14: "Review and redraft the proposed Digital Security Act to ensure online freedom of expression" (Norway)
Recommendation 148.3: "Enforce constitutional provisions safeguarding freedom of expression, including by amending section 57 of the Information and Communication Technology Act and relevant provisions of the draft Digital Security Act" (Australia)
Recommendation 148.70: "Guarantee freedom of expression in the Digital Security Act" (France)

[55] UPR of Tanzania (2016): "Undertakes a thorough review with key stakeholders and civil society of its existing Cyber Crime and Statistic Acts and proposed Media Services and Access to Information bills, to meet human rights obligations" (United Kingdom). See also: "Amend all laws infringing on press freedom, in particular the Statistics Act and the Cyber Crimes Act" (Belgium)

[56] UPR of Viet Nam (2019). Recommendation 38.189: "Strengthen efforts to ensure freedom of expression, including in the digital environment" (Peru)

[57] UPR of Cambodia (2019). Recommendation 110.98: "Immediately remove all undue restrictions on civil society and independent media, including by withdrawing the interministerial decision known as prakas No. 170 on digital expression" (United States).

[58] UPR of Laos (2015): "Take measures to ensure that all the legislation, especially on press and media, including digital media, is fully aligned with its international human rights obligations" (Costa Rica). See also:

Over the years, human rights mechanisms, such as the Special Rapporteur on the promotion and protection of the right to freedom of expression,[61] have produced a wealth of evidence attesting to the diverse and grave human rights violations resulting from the use of digital technologies.

In its recent report, the Office of the High Commissioner for Human Rights (OHCHR) touched on the human rights impacts of surveillance and biometric technologies, including facial recognition with a particular focus on the "chilling effect on the right of peaceful assembly."[62]

"Ensure that the right to freedom of expression and its other international human rights commitments are upheld in any move to adopt a cyber law" (United Kingdom)

[59] UPR of Iran (2010): "Provide guarantees of a fair trial, allowing access to independent observers during the judicial proceedings amend the provisions of the procedural criminal code that allows the Government to deny the basic right to a lawyer during the accusation period guarantee transparency and accountability and allow lawyers access to relevant information concerning each case investigate and prosecute all public officials and Basij paramilitary members suspected of torture, ill treatment or extrajudicial execution eliminate every restriction on the freedom of expression, particularly with regard to digital media, which runs counter to ICCPR" (Spain)

[60] UPR of United Arab Emirates (2013): "Ensure legislation in the area of freedom of expression is in line with international standards, including by amending the Cyber Crime law and repealing the November 2012 Federal Legal Decree No. 5 on Cyber Crime" (Ireland). See also: "Continue to take steps to uphold freedom of expression by reviewing restrictive articles of its recent Cyber Crime law and consider updating the 1980 Media Law, ensuring that new legislation be aligned with article 19 of the ICCPR" (Canada)

[61] *The right to freedom of opinion and expression exercised through the Internet,* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/66/29, 2011*; The implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2014; *Freedom of expression, states and the private sector in the digital age,* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 May 2016; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**,** A/73/348, 29 August 2018; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**,** A/HRC/42/35, 28 May 2019.

[62] *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, A/HRC/44/24, June 2020, paragraph 19.

A range of economic and social rights are also impacted when cyber operations target critical infrastructure such as electrical grids or medical facilities. This includes the right to health and potentially the rights to education, food, water, a healthy environment, and access to information, depending on the nature and severity of the operation. While the behavioural norm against attacking such critical infrastructure is well-acknowledged within the cyber security field,[63] the extent of potential human rights impacts stemming from such operations could be stressed and better highlighted and evidently, operations targeting such infrastructure continue to occur.[64]

Gender

In the context of human rights, WILPF emphasises that the actions of cyber mercenaries can differently impact people based on their gender identity or expression, while gender dynamics have been shown to reinforce or even amplify the unequal social, economic, cultural, and political structures of the physical world.

Some of the spyware products created by the cyber mercenary actors described in Annex II have been used to target women human rights defenders;[65] while cell phone applications that have geolocation and messaging abilities have been misused by authorities to entrap and arrest or physically assault LGBTQ individuals in multiple countries.[66] Other apps and software are developed by private

[63] For more on this norm, see "Cyber Norm Development and the Protection of Critical Infrastructure," *Council on Foreign Relations*, 23 July 2015, https://www.cfr.org/blog/cyber-norm-development-and-protection-critical-infrastructure.

[64] Apart from the examples cited in this submission relating to operations targeting medical facilities, other relevant examples include the 2015 attack on the Ukrainian electrical grid; a 2019 infiltration of India's nuclear power system; and the 2020 breach of diverse US governmental agencies.

[65] Concluding observations to Mexico, CEDAW/C/MEX/CO/9 (CEDAW 2018), paragraph 27: "The Committee notes with concern that women human rights defenders and journalists are subjected to various and increasing manifestations of violence, seemingly committed by State agents in some cases. The Committee is further concerned about reports indicating that attacks on social media and digital platforms are being used as tools by anonymous groups to incite violence against women human rights defenders and journalists."

[66] Article 19, *Apps, arrests and abuse in Egypt, Lebanon and Iran,* February 2018, https://www.article19.org/apps-arrests-abuse-egypt-lebanon-iran/.

companies with the express purpose of facilitating intimate partner surveillance, harassment, abuse, stalking, and/or violence, or can be modified to use in this way.[67]

Some of the mercenary actors described in Annex II are active in data theft. Data breaches have been shown to expose sensitive information that have put women or individuals with other gender identities at unique risk, particularly when health records are exposed and made public.[68] Facial recognition technologies are developed with the same gender and other biases that their creators have, which can perpetuate negative gender norms and have real-life implications for the people targeted by these technologies.[69]

Research shows that there is a strong gender dimension in politically motivated disinformation activities, which are sometimes implemented by trolls or other for-hire mercenary actors described in Annex II. Such activities are often highly sexualised and gendered in the nature of who they target as well as the tone and content of the abuse. A recent survey of female legislators found that 81.8 per cent of the respondents had experienced psychological online gender-based violence, including high

---

[67] The Coalition Against Stalkerware defines as software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence. See: https://stopstalkerware.org/.

[68] In July 2016, the municipality of São Paulo experienced a data breach exposing the personal data of an estimated 650,000 patients from the Brazilian public health system. This massive data breach included names, addresses, and medical information such as information about pregnancy and abortion care. The illegality of abortions in Brazil means that the data breach not only violated the right to privacy of the women affected around a socially sensitive issue, but also exposed them and their doctors to potential criminal charges. See R. Hernandes, "Gestão Haddad expõe na internet dados de pacientes da rede pública", Folha de Sao Paulo, 6 July 2016, https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-redepublica.shtml. Another massive data breach occurred in Chile in 2016. In this case, a public hospital suffered a cyber security failure and made available to their workers and even to the general public (via their intranet) more than three million health records including the names, ID numbers, and addresses of women and girls who asked for the morning-after pill in a public hospital and people living with HIV. See M. Jara and V. Carvajal, "Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes," *CIPER*, 3 March 2016, https://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-depacientes.

[69] Ray Acheson, *Gender and bias,* Campaign to Stop Killer Robots, 2020, https://www.stopkillerrobots.org/wp-content/themes/cskr/resources/images/resources_images/pdf/Gender%20and%20Bias.pdf.

incidences in which humiliating or sexual images that were often fake or doctored had been circulated.[70] A 2020 report from the UNSG's panel on digital cooperation observes that "This is leading many women to "log off" of social media, perpetuating and entrenching inequalities in the space."[71]

The gendered impacts of different operations in cyberspace have been recognised by different human rights mechanisms. The HRC called on states to prevent and eliminate all forms of discrimination and gender-based violence and harassment in digital contexts in its resolution *Elimination of all forms of discrimination against women and girls,*[72] and urged states "to modify social and cultural patterns of conduct …to preventing and eliminating in the public and private spheres, including in digital contexts, patriarchal and gender stereotypes, negative social norms, attitudes and behaviours and unequal power relations that view women and girls as subordinate to men and boys, that underlie and perpetuate discrimination and violence against women and girls".[73]

Importantly, the HRC also recognised "the importance of partnership and dialogue between States and business enterprises, including social media companies and digital technology companies, in collaborating on joint initiatives that prevent and respond to impunity for violence against women and girls in digital contexts." [74]

[70] Inter-Parliamentary Union, *Sexism, harassment and violence against women parliamentarians*, October 2016, http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf.

[71] UN Secretary-General, *Roadmap for Digital Cooperation*, June 2020, p.18, https://www.un.org/en/content/digital-cooperation roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

[72] *Elimination of all forms of discrimination against women and girls*, A/HRC/RES/44/17, 21 July 2020, OP 3 (c).

[73] *Elimination of all forms of discrimination against women and girls,* A/HRC/RES/41/6, 19 July 2019, paragraph 5 (d).

[74] *Accelerating efforts to eliminate all forms of violence against women and girls: preventing and responding to violence against women and girls in the world of work*, A/HRC/RES/41/17, 19 July 2019, pp 15. See also *Accelerating efforts to eliminate all forms of violence against women and girls: preventing and responding to violence against women and girls in the world of work*, A/HRC/RES/38/5.

Relevant recommendations have been made in the Universal Periodic Review, including to Albania,[75] Pakistan,[76] and Chile,[77] while the Committee on the Elimination of All Forms of Discrimination Against Women (CEDAW Committee) has expressed relevant concerns to Mexico in concluding observations.[78]

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism found in her most recent report that that "new technologies and data collection methods in particular have disparate impacts on minorities and are profoundly gendered."[79] She further notes:

> "Significant research has uncovered wide misuse and abuse of surveillance laws on a discriminatory basis, targeting particular communities and groups based on ethnic background, race and religion. This has rendered some forms of masculine expression as hyper-visible to law enforcement (exacerbated by ethnic and religious identity) and others, particularly the masculine protector expression, as above suspicion."[80]

The Special Rapporteur on the right to privacy dedicated an entire report on this topic from a gender perspective, finding that many states are acting in ways that "increasingly put it at risk, by employing new technologies that are incompatible with the right to privacy, such as big data and health data,

[75] UPR of Albania (2019). Recommendation 95.50: **"**Ensure the protection of the rights of vulnerable groups, such as women and children, in particular in the context of digital space" (Pakistan)

[76] UPR of Viet Nam (2019). Recommendation 38.121: "Strengthen protection of the rights of vulnerable groups, such as women and children, in particular in the context of expanding digital space" (Pakistan)

[77] UPR of Chile (2019). Recommendation 125.175: "Review and revise laws, policies and regulations to address violence against women, including in digital contexts, in compliance with international human rights obligations" (Iceland) See other recommendations to Chile: Recommendation 125.166: **"**Ensure that women can live a life free of violence, including in digital contexts, through appropriate legislation, preventative measures, education and adequate resources, including services for survivors" (Canada).

[78] Concluding observations to Mexico, CEDAW/C/MEX/CO/9 (CEDAW 2018),

[79] *Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family*, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/46/36, 22 January 2021, paragraph 11.

[80] Ibid.

infringing the dignity of its citizens on the basis of gender or gender identity and expression, and arbitrarily surveying their own citizens."[81]

Despite these pronouncements, and significant documentation of the gendered human rights threats and abuses stemming from the misuse of technology including through the services and products of cyber mercenaries, the problem is deepening and having compounding effects. More needs to be done by policymakers and private actors to apply the human rights framework to these contexts as well as advance understanding about gendered impact and dimensions of cyber operations within international cyber security fora.[82]

V. Recommendations

Drawing on the information provided in this submission and its annexes, WILPF puts forward the following recommendations:

- Given the persistent and grave challenges to civilian protection, human rights, and accountability posed by PMSCs and other types of mercenaries, states and law enforcement agencies should not hire or engage proxies for domestic or international surveillance, military operations, or any other actions that risk undermining IHL and human rights. Existing normative and legal commitments with respect to state use of proxy actors in cyberspace must be adhered to.

[81] *Report of the Special Rapporteur on the right to privacy, Privacy, technology and other human rights from a gender perspective*, A/HRC/40/63, 16 October 2019, paragraph 6.

[82] While great strides have been made in recognising the applicability of the human rights framework to threats and abuses against women's digital contexts the gender dimensions of international cyber security and operations remain nearly unexplored. WILPF and the Association for Progressive Communications put forward several recommendations in this regard to the UN's Open-ended working group on developments in the field of information and telecommunications in the context of international security in 2020, and governments such as Canada, New Zealand, Australia, the United Kingdom, and the Netherlands have focused efforts on elevating gender within this forum. See Deborah Brown and Allison Pytlak, *Why gender matters in international cyber security*, WILPF and the Association for Progressive Communications, April 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

- As the Special Rapporteur on the rights to freedom of peaceful assembly and of association has said, "Existing international human rights norms and principles should not only dictate state conduct, but also be the framework that guides digital technology companies' design, control and governance of digital technologies."[83] In this context, states should ensure that all human rights are respected by technology companies, protected and implemented in national legal frameworks, policies, and practices, in accordance with international law.

- States, in partnership with technical communities, including public and private technical entities and individual technologists, and civil society, must take steps to reach common understandings around cyber-related terms and concepts in order to eliminate ambiguity and exploitable legal loopholes. To this end, states should outline and exchange in greater detail how they understand that international law applies to cyberspace. This could be done through annual national reports that states make to the UN Secretary-General on international cyber security, as one suggestion.

- Digital technology companies must commit to respect human rights and carry out due diligence to ensure that they do not cause, contribute to or become complicit in violation of these rights. Technology companies need to ensure that their activities—including product design, promotion, deployment, selling and licensing—do not contribute to human rights harms by making this a central aspect of their due diligence, in line with the Guiding Principles on Business and Human Rights, and the recommendations to states, companies, and civil society contained in the Special Rapporteur on peaceful assembly's report of May 2019 should be fully implemented.[84]

- States should hold manufacturers of commercial spyware accountable and engage legal measures to ensure that their products are not abused to facilitate surveillance or technology-facilitated violence, including gender-based violence.

- The gender dimensions of cyber operations conducted by mercenaries or implemented through their products merits stronger action and attention. States must act to uphold

[83] *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, A/HRC/41/41, 17 May 2019, paragraph 17.

[84] Ibid., paragraphs. 17-20.

women's rights online, in the context of their obligations under international human rights law and recognise that international cyber operations can have gender-differentiated impacts.

- The international transfer of surveillance technologies needs to be restricted. In line with the recommendations of the Special Rapporteur on the right to freedom of expression and opinion's report of 2019, "states should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place."[85] Existing prohibitions and controls that apply to physical weapons could be expanded and applied to dual-use technologies.

- Efforts should be made to bring together the diverse communities working on digital human rights, international cyber security, and cyber crime. This submission has demonstrated that cyber mercenaries pose multi-faceted and cross-cutting challenges that cannot be meaningfully addressed through siloed efforts.

ANNEX I: Terms and concepts

On mercenaries

There is not a universal or agreed definition of a "cyber mercenary" and the term is not used as frequently as similar terms such as "proxy," "hackers," or "cyber militias". When used, "cyber mercenary" is applied loosely or vaguely; interchangeably with terms for other, similar actors; or not employed at all, as explained in Section I of this submission.

We have also observed, in the course of our research, that distinctions between different types of non-state actors in cyberspace are evolving. Labels that were applied to participants in cyber operations ten years ago may have since proved to be inaccurate or inadequate, just as new types of actors have cropped up or more has been learned about the structure and objectives of earlier non-state cyber actors.

In this submission, WILPF is guided somewhat by the definition of a mercenary provided by the 2001 UN Mercenaries Convention: in particular, a person recruited for the purpose of fighting in armed

[85] *Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/41/35, 28 May 2019, p. 8.

conflict or conducting a concerted act of violence; that is primarily motivated by private gain; and who would not otherwise be party to the conflict by virtue of nationality or residency.[86] We note concerns that this definition may be too narrow if the term person is to be understood as a natural person, particularly with respect to private military and security companies (PMSCs) or other privately owned business entities—a dimension that is significant in the context of cyber security.

The Working Group's call for submissions describes cyber mercenaries as "one category of actors that can generate mercenary-related activities."[87] The call goes on to note that those activities "entail a wide range of military and security services provided in cyberspace, including 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 cyber operations to weaken the military capacities and capabilities of enemy armed forces, or to undermine the integrity of another State's territory. Individuals carrying out cyberattacks can cause damage remotely, across various jurisdictions. As such, they can be considered as undertaking a mercenary-related activity, or even a mercenary activity if all the qualifying criteria are met."

On cyberspace

Cyberspace and cyber security also do not enjoy universal definitions or understandings. In some ways, this is a reflection of the "space" itself. It is virtual but created, maintained, and utilised by and through physical infrastructure, devices, and people.

Many of the characteristics of cyberspace lend themselves to outsourcing and proxy actors in ways that reconfigure the traditional state monopoly on the use of force. In fact cyberspace might best be described as an "alter-space" that challenges geographical distance, space, and time.[88] A lack of physical boundaries gives it a transnational character that erodes the traditional influence and role of national governments in ways that make it easier for other actors to operate practically, manoeuvre

[86] UN General Assembly, *International Convention Against the Recruitment, Use, Financing and Training of Mercenaries,* https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-6&chapter=18&clang=_en.

[87] Call for inputs: report on the provision of military and security cyber products and services by 'cyber mercenaries' and its human rights impact, December 2020, https://www.ohchr.org/EN/Issues/Mercenaries/WGMercenaries/Pages/Report-Cyber-Mercenaries-2021.aspx.

[88] Collier, p. 33.

with impunity, and shift the balance of power.[89] Recognising their reduced role but also the allure of a new "battlefield" means that states turn to such actors to maintain their primacy and expand power.

It's also been shown that the skills required to succeed in cyberspace tend to be more firmly entrenched in the civilian sector.[90] This is owing not only to how digital networks and technologies have evolved over time, but also by the inability of government agencies to keep pace with the economic and other incentives offered in private sector technological roles. The result is less in-house government technological capacity, which creates situations where outsourcing is their only option, and often more cost-effective.[91]

Yet, governments are increasingly establishing official cyber divisions and units within their militaries or intelligence agencies. This is to aid in the digital dimensions of regular military or intelligence gathering activities; for defence; or to conduct offensive cyber operations that are not integrated within non-cyber operations. These units sometimes outsource to boost their own capacity, although may do so in different ways, as examples below from Estonia and the US Cyber Command demonstrate.

Much has been written about the lower barriers of entry within cyberspace, which enables non-state actors or even smaller countries to become active and more effectively pursue goals through cyber technologies and tactics. "Unlike the significant capital required to build fighter jets and naval vessels, sophisticated tools in the cyber domain can be developed by small businesses and start-ups."[92] Yet, most experts maintain that the most sophisticated cyber operations are still fully in the hands of national governments, and some research shows that the states most active in cyber conflict are those with large physical militaries, particularly nuclear-armed countries.[93]

Cyberspace also affords unique levels of anonymity. Some experts maintain that this is a drawback for states wishing to exercise "cyber deterrence,"[94] but the fact that anonymity fuels remote violence and

[89] Bussolati, p. 102.

[90] Jamie Collier, p.33.

[91] Collier, p. 35.

[92] Ibid., p.33.

[93] Allison Pytlak and George E. Mitchell, "Power, rivalry and cyber conflict: an empirical analysis," in *Conflict in Cyber Space*, 2016.

[94] The concept of cyber deterrence became popular especially among US academics and cyber policy experts in the early 2000s. It came into greater focus as more states began to undertake cyber operations alongside or

harm is well-accepted. This is true for individuals in the context of online gender-based violence and bullying, and for the behaviour of states, whether in how they interact with one another or toward civilians.

ANNEX II: Types of cyber mercenaries

Below are examples of six different types of actors WILPF identifies as being involved in mercenary-like cyber activities, as well as certain of the products and services they provide. This corresponds with Questions 2 and 4 of the first section of the Working Group's questionnaire.

There is no universal classification system for such actors and as a result our examples draw from different sources including academic research, investigative journalism, civil society reporting and lived experience, as well as UN documents. It is not an exact science—there is some degree of cross-over between the categories, and that it's not always clear if these actors are profit-motivated as mercenaries traditionally are, or if their motivation is political, ideological, or a combination of factors. We focus mainly on mercenaries that are connected to governments or other authorities, rather than purely criminal networks.

---

as a component of their military actions against other states, such as the operations against Estonia (2007) and Georgia (2008), and the Stuxnet operation (2013). Like nuclear deterrence, it argues that a build-up (real or perceived) of offensive capabilities will deter other states from attacking because of the likelihood of retaliation. Underlying this is the assumption that states are "rational" actors that do not want to be counter-attacked. In reality, deterrence only contributes to arms racing and greater instability—it's likely not a coincidence that the concept of "cyber arms racing" also became popular in this same time period. In WILPF's view, efforts to import already problematic security concepts like deterrence into cyber security discussions needlessly militarises cyberspace by affecting the tone and nature of policy-making in this area, and risks inflating threats or escalating crises. Over time, cyber deterrence has lost popularity, due largely to the realisation that key aspects of deterrence "theory" do not work well in cyberspace—for example, states value secrecy in planning and executing cyber operations in order to gain the competitive advantage by surprising their targets, over overt demonstrations of capability and strength such as with physical weapons. The diversity of actors active within cyberspace, including mercenary actors, also has implications for assumptions rationality. For an overview of cyber deterrence literature, and about the rise and fall of the theory, see Dr. Max Smeets and Stefano Soesanto, "Cyber Deterrence Is Dead. Long Live Cyber Deterrence!", Council on Foreign Relations, 18 February 2020, https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence.

It's also helpful to bear in mind that what is often popularly referred to as a "cyber attack" might be better described as an "operation" comprising a multitude of activities and/or tools that could range from intrusion and espionage to so-called "payload delivery," and which usually occur over a period of time and not necessarily in a single moment.[95] This means that one actor may play multiple roles within an operation or attack, or have to engage with a third actor; or that a single operation consists of different types of non-state actors with varying motivations and skills.

1. Advanced Persistent Threat (APT) groups

When cyber security firm Mandiant released a 2013 report exposing the relationship between the government of China and an "advanced persistent threat" (APT) group known as APT1, it drew unprecedented attention to the phenomenon of state-sponsored cyber operations conducted by proxy.[96] FireEye describes the activities of APT groups as "trying to steal data, disrupt operations or destroy infrastructure. Unlike most cyber criminals, APT attackers pursue their objectives over months or years. They adapt to cyber defenses and frequently retarget the same victim."[97] They are characterised as technologically sophisticated; well-financed by national governments; and with long-term strategic goals.[98]

Today there are dozens of APT groups; identified ones have been linked to China, Iran, North Korea, Russia, the United States, and Viet Nam, although most governments work hard to obscure their relationship to an APT so it's possible there are others on this list.[99] Commercial data theft and espionage are among the activities most commonly attributed to APTs, and they use a range of intrusion techniques to enter the information systems of targets that include foreign government agencies, ethnic minority groups, media outlets, scientific research institutes, and financial institutions. In late 2020, Blackberry research uncovered a new type of APT group that does not appear

[95] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," Journal of National Security Law and Policy, Vol. 4, No. 63, 2010, p. 64, https://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

[96] "APT1: Exposing One of China's Cyber Espionage Units", February 2013, http://www.worldinwar.eu/wp-content/uploads/2017/07/mandiant-apt1-report.pdf.

[97] See FireEye monitoring: "Advanced persistent threat groups: who's who of cyber threat actors" at https://www.fireeye.com/current-threats/apt-groups.html.

[98] Ensar Seker, "Top Famous, Dangerous, and Active APT Groups who can Turn Life to A Nightmare," *Medium*, 27 October 2020, https://medium.com/datadriveninvestor/top-famous-and-active-apt-groups-who-can-turn-life-to-a-nightmare-5d130168f43,

[99] FireEye.

to be linked to any one government but conducts the same range of activities as traditional APTs do. Blackberry says, "Mercenary groups offering APT-style attacks are becoming more and more popular" and that "by using a mercenary as their proxy, the real attacker can better protect their identity and thwart attempts at attribution."[100]

2. Cyber militias

Another category of actors could be described as "cyber militias," in that they are technically civilian networks or groups but offering voluntary support to governmental cyber operations or cyber security objectives. The role, structure, and capacity of cyber militias varies quite a lot from state to state, as does the extent to which they receive formal support, encouragement, and compensation.

The Syrian Electronic Army (SEA) was established in 2011, with vague links to the government but purporting independence. Either way, its actions have been described as a "useful tool"[101] for the Assad regime in its early years because of its aggressive pro-Assad cyber operations, which included hacking the websites of prominent Western human rights organisations and the US military, as well as the Twitter account of the Associated Press, through which it spread false information.[102]

Since 2011, cyber militias within India and Pakistan have been "fighting" one another through hacking operations, website defacements, and intelligence gathering, among other activities.[103] The contours of their engagement have changed over time from more minor nuisance-like activities to increasingly sophisticated operations that are believed to benefit (unofficially) from the governments on both sides, and possibly other states such as China and Israel.[104]

---

[100] "The CostaRicto Campaign: Cyber-Espionage Outsourced", *Blackberry ThreatVector Blog*, 12 November 2020, https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced.

[101] Collier, p.29.

[102] Abdulrahman Al-Masri, "The New Face of the Syrian Electronic Army", *Open Canada,* 17 May 2018, https://opencanada.org/new-face-syrian-electronic-army/.

[103] See Sandeep Unnithan, "Inside the Indo-Pak Cyber Wars," *India Today*, 18 March 2011, https://www.indiatoday.in/nation/story/india-pakistan-cyber-war-run-by-hired-hackers-130151-2011-03-18.

[104] Kate Fazzini, "In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides," *CNBC*, 27 February 2019, https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html.

A different, somewhat hybrid, example comes from Estonia, whose Defence League Cyber Unit contains volunteers with expertise in topics such as computer science, cyber law, and crisis management strategy. The unit's broad remit includes providing assistance in developing cyber security practices and protecting critical national infrastructure, and its members are organised on a voluntary reserve basis and only paid when they become active.[105] Similar structures exist in other Baltic states like Lithuania and Latvia, who have often found themselves the focus of Russian-led operations, as well as Kyrgyzstan and Kazakhstan.[106]

3. Private software and technology companies

While some software and technology companies play theoretically neutral provider roles, others have been shown to collude with authorities in providing data and information, or overtly manufacture products like surveillance software ("spyware") and malware. One of the most well-known and well-researched examples is Hacking Team, an Italian company that sold surveillance software directly to governments who utilised the software to spy on people, in particular focus on activists, human rights defenders, and journalists.[107] Other companies offering similar products include NSO Group/Q Cyber Technologies (producer of Pegasus software),[108] Gamma International (producer of FinFisher),[109] and CyberBit (producer of PC Surveillance System).[110] Destinations and/or purchasers of these technologies are governments, law enforcement, or criminal groups in Bahrain, Ethiopia, Kazakhstan, Mexico, Morocco, Saudi Arabia, Sudan, and United Arab Emirates (UAE), amongst others. Some private companies form agreements with local law enforcement to allow use of their face or voice recognition

[105] The official webpage for the unit is at: http://www.kaitseliit.ee/en/cyber-unit.

[106] Franklin Holcomb, "Assessment of Militia Forces as a Model for Recruitment and Retention in Cyber Security Forces," *RealClear Defense*, November 2019, https://www.realcleardefense.com/articles/2019/11/18/assessment_of_militia_forces_as_a_model_for_recruitment_and_retention_in_cyber_security_forces_114856.html.

[107] Citizen Lab at the University of Toronto has done extensive research on Hacking Team operations. Visit https://citizenlab.ca/tag/hacking-team/ for an overview of reports, media coverage, and other relevant information.

[108] See Citizen Lab research about NSO Group, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

[109] Samantha Early, "German prosecutors investigate spyware maker FinFisher," *Deutsche Welle*, 5 September 2019, https://www.dw.com/en/german-prosecutors-investigate-spyware-maker-finfisher/a-50293812.

[110] Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware,* December 2017;

technologies for domestic surveillance activities (i.e. Amazon's Ring and Alexa);[111] sell information to law enforcement (i.e. Dataminr);[112]or are developing "predictive policing" tools based on artificial intelligence and facial recognition software (i.e. Clearview AI).[113]

DarkMatter Group in the UAE has gone a step further in seeking to manipulate hardware by exploiting probes that are installed across major cities for surveillance purposes, in addition to hunting down vulnerabilities and "building stealth malware implants to track, locate, and hack basically any person at any time in the UAE."[114]

Research by Privacy International identifies that the majority of companies in the surveillance industry are overwhelmingly based in "economically advanced, large arms exporting states, with the United States, United Kingdom, France, Germany, and Israel comprising the top five countries where these companies are headquartered."[115]

Social media companies such as YouTube, Facebook, and Twitter and others might offer useful platforms for civil society to connect but can also become spaces for repression and information

[111] Kari Paul, "Amazon's doorbell camera Ring is working with police – and controlling what they say," The Guardian, 30 August 2019, https://www.theguardian.com/technology/2019/aug/29/ring-amazon-police-partnership-social-media-neighbor.

[112] Sam Biddle, "Twitter surveillance start-up targets communities of color for police", The Intercept, 21 October 2020, https://theintercept.com/2020/10/21/dataminr-twitter-surveillance-racial-profiling/.

[113] Miles Kenyon, "Algorithmic Policing in Canada Explained", Citizen Lab, 1 September 2020, https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/.

[114] Jenna McLaughlin, How the UAE is recruiting hackers to create the perfect surveillance state", *The Intercept*, 24 October 2016, https://theintercept.com/2016/10/24/darkmatter-united-arab-emirates-spies-for-hire/.

[115] Deibert, *Reset*, p.149.

control. Political conflicts and crises such as in Syria,[116] Thailand,[117] Venezuela,[118] and Yemen[119] have demonstrated the ways in which information and communications often become a focal point for contestation and control during a crisis.

Beyond crisis situations, a recent report from Amnesty International documents how Facebook and YouTube have complied with requests from the Vietnamese government to censor content that it deems as "anti-state" while state-affiliated groups "deploy sophisticated campaigns on these platforms to harass everyday users into silence and fear."[120]

The example of Viet Nam demonstrates that different mercenary/non-state actors can be involved in a single cyber operation as the report also sheds light on another kind of cyber mercenary actor, the "Force 47," which Amnesty describes as "a cyberspace military battalion made up of some 10,000 state security forces whose function is to "fight against wrong views and distorted information on the internet."

Groups like these are sometimes described less formally as "troll armies" or "troll farms" and can be described as for-hire actors whose main function is flooding any given digital platform or forum with (mis-)information, often to harass people who present opposing views.[121] Troll groups operate in a

[116] John Scott-Railton and Morgan Marquis-Boire, "A call to harm", *Citizen Lab*, 21 June 2013, https://citizenlab.ca/2013/06/a-call-to-harm/.

[117] Allison Pytlak and Brandon Valeriano, "The Frontlines of Cyber Repression: Thailand and the Crop Top King", 4 August 2017, https://www.niskanencenter.org/frontlines-cyber-repression-thailand-crop-top-king/.

[118] Allison Pytlak and Brandon Valeriano, "The Frontlines of Cyber Repression: The Venezuelan Digital Caudillo", 14 September 2017, https://www.niskanencenter.org/frontlines-cyber-repression-venezuelan-digital-caudillo/.

[119] Jakub Dalek, Ron Deibert, Sarah McKune, Phillipa Gill, Adam Senft, and Naser Noor, "Information Controls during Military Operations: The case of Yemen during the 2015 political and armed conflict", *Citizen Lab*, 21 October 2015, https://citizenlab.ca/2015/10/information-controls-military-operations-yemen/.

[120] "Viet Nam: Tech giants complicit in industrial-scale repression," Amnesty International, December 2020, https://www.amnesty.ca/news/viet-nam-tech-giants-complicit-industrial-scale-repression.

[121] As just one of many examples, see "Philippines Troll Patrol: The woman taking on trolls on their own turf," BBC News, 25 September 2020, https://www.bbc.com/news/world-asia-54275891.

blurry public-private space, in that they are frequently employed or sponsored by political actors and entities but are not necessarily or always a formal part of the state governmental structures.[122]

4. Private contractors/individuals

While all of the categories listed in this Annex are composed of people, it's worth highlighting the role of individuals when acting either on their own initiative or on behalf of a beneficiary but not necessarily within a larger group, such as an individual troller within a troll army, described above.

For example, quite a lot of individual hackers or information technology experts undertake to find software vulnerabilities, or "bugs".[123] Their work is crucial in order for software providers to keep their programmes safe from intrusions or manipulations. These "bug bounty hunters" can receive significant financial compensation for their work either from the software manufacturer, or any of the vendors who depend on those systems for their day-to-day operations.[124] While some bug hunters engage in this lucrative work for helpful reasons (so-called "white hat hackers"), others take advantage of the vulnerabilities that they uncover to either run up the price tag on them, or sell the information to competitors, criminals, militaries, and governments.[125] The legal and illicit trade in zero-day vulnerabilities in particular is lucrative and global; in 2013 the United States spent an estimated $25.1 million on "covert purchases of software vulnerabilities" from private vendors[126] such as French firm Vupen.[127]

---

[122] To learn more, see "How do you solve a problem like troll armies?" *Access Now,* 21 April 2017, https://www.accessnow.org/solve-problem-like-troll-armies/; or Fruzsina Eordogh, "The Russian Troll Army Isn't The Only One We Need To Worry About," *Forbes*, 11 April 2018, /the-russian-troll-army-isnt-the-only-one-we-need-to-worry-about/?sh=677ca7172334.

[123] Steve Ranger, "Meet the hackers who earn millions for saving the web, one bug at a time," *ZD Net*, 16 November 2020, https://www.zdnet.com/article/meet-the-hackers-who-earn-millions-for-saving-the-web-how-bug-bounties-are-changing-cybersecurity/.

[124] As one example, the company HackerOne connects hackers with a client base that range from PayPal to Starbucks. See https://www.hackerone.com/.

[125] Kathleen Metrick, Parnian Najafi, Jared Semrau, "Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill — Intelligence for Vulnerability Management, Part One," *FireEye*, 6 April 2020, https://www.fireeye.com/blog/threat-research/2020/04/zero-day-exploitation-demonstrates-access-to-money-not-skill.html.

[126] The responsibility of states to disclose rather than stockpile zero-day vulnerabilities that they have uncovered is a separate source of significant discussion and debate within the international community.

[127] Collier, p. 28.

Some individuals also move from working in governmental intelligence agencies to the private sector and back again, including for foreign governments. A 2019 Reuters report on Project Raven reveals how former US National Security Agency employees were recruited by the UAE "to engage in surveillance of other governments, militants, and human rights activists" through hacking and other activities.[128] Reporting on the Raven case revealed that most of these individuals were largely comfortable with these functions, provided that they were not targeting other US citizens.

5. Private military and security companies

Many of the traditional PMSCs that grew out of the post-9/11 counter-intelligence surge are expanding their existing services into areas of cybersecurity. Some build their own cybersecurity teams while others acquire smaller, boutique firms specialising in cyber tools and services.[129]

TigerSwan is a US PMSC that targeted and suppressed the Indigenous-led environmental activist movement opposing the Dakota Access Pipeline through "military-style counter terrorism measures."[130] It was hired by the pipeline's owner, Energy Transfer Partner, and colluded with US state and national authorities, focusing some of its most intense efforts on people of colour. Leaked documents have revealed that TigerSwan used a wide range of digital tools such as Stingray mobile phone tracing, hacking, and social media surveillance in order to infiltrate the movement, collect intelligence, create dissent among activists, and actively intimidate or deter further activism, alongside physical tactics.[131] "Our devices would stop working for periods of time, hard drives would be cleared

[128] Christopher Bing and Joel Schectman, "Project Raven: Inside the UAE'S secret hacking team of American mercenaries," *Reuters*, 30 January 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/.

[129] Maurer and Hoffman, p. 5.

[130] Alleen Brown, Will Parrish, and Alice Speri, "Leaked Documents Reveal Counterterrorism Tactics Used At Standing Rock To "Defeat Pipeline Insurgencies", *The Intercept*, 27 May 2017, https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/.

[131] The Intercept has undertaken significant research and reporting on the TigerSwan operation. Its series of reports is available at https://theintercept.com/series/oil-and-water/. See also C.S. Hagen, "Standing Rock's invisible enemy", *High Plains Reader*, 30 November 2016, https://hpr1.com/index.php/feature/news/standing-rocks-invisible-enemy/.

of information and footage, and from time to time camp security would identify infiltrators inside the camp who were working for Energy Transfer Partners."[132]

Wagner Group is a well-known PMSC with links to Russia whose mercenaries have been involved in conflicts throughout the Middle East and Africa. New research outlines information and influence campaign efforts linked to Wagner Group, as conducted through the establishment of Facebook pages.[133] The campaigns targeted Libya, Sudan, Central African Republic, Madagascar, Mozambique, and the Democratic Republic of the Congo. In some of the countries, the Facebook pages published general pro-Russian content or positions; in other countries, the pages published content relating to national political candidates or against specific United Nations inquiries.[134]

6. Weapons producers

Traditional producers of weapons and military equipment have also pivoted to the digital era and in ways that often deliberately blur offensive and defensive activities for the benefit of their clients. Raytheon Intelligence & Space "supports military operations and helps the cyber warfighting force defend critical infrastructure, protect network resiliency and synchronize cyber effects across all warfighting domains with unparalleled speed and precision."[135] Yet according to its website, it also specialises in developing advanced sensors, training, and cyber and software solutions to delivering the "disruptive technologies its customers need to succeed in any domain, against any challenge."[136]

A component of this pivot includes the production of surveillance and intelligence equipment, whether for national governments or PMSCs. As just one example, in 2017 it was revealed that UK weapons producer BAE Systems worked with a smaller Danish subsidiary called ETI to develop and sell a mass surveillance system called Evident to Middle Eastern and Gulf countries in the wake of the Arab Spring. Someone close to the project later explained that "You'd be able to intercept any internet traffic. If you

---

[132] C.S. Hagen, "Tigerswan Counterterrorism Tactics Used To Defeat Dakota Access Pipeline "Insurgencies"", *High Plains Review*, 30 May 2017, https://hpr1.com/index.php/feature/news/tigerswan-counterterrorism-tactics-used-to-defeat-dakota-access-pipeline-in/.

[133] Shelby Grossman, Daniel Bush, and Renée DiResta, *Evidence of Russia-linked influence operations in Africa*, Stanford Internet Observatory, 29 October 2019, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/29oct2019_sio_-_russia_linked_influence_operations_in_africa.final_.pdf.

[134] See https://www.csis.org/blogs/post-soviet-post/not-so-private-military-and-security-companies

[135] See, for example: https://www.raytheonintelligenceandspace.com/capabilities/products/cyber-warfare

[136] See, for example: https://www.raytheonintelligenceandspace.com/about.

wanted to do a whole country, you could. You could pin-point people's location based on cellular data. You could follow people around. They were quite far ahead with voice recognition. They were capable of decrypting stuff as well."[137]

The production and transfer of surveillance equipment and technology, which can overlap with the surveillance software described earlier in this aspect, has long been an issue of debate within the arms control community. The dual-use nature of some of these items have helped traditional weapons producers to circumvent some of the controls that are in place for their other products. In the case of Evident, the UK government objected to the export of the technology to the UAE—because of concerns that it could eventually lead back to sensitive British intelligence being decrypted, rather than concern about infringement on privacy rights in recipient countries. The Danish authorities did not object.[138]

[137] "How BAE sold cyber-surveillance tools to Arab states", 14 June 2017, *BBC News*, https://www.bbc.com/news/world-middle-east-40276568.

[138] Ibid.