October 2021

Response to the United Nations (UN) Working Group on the Use of Mercenaries

Microsoft is grateful for the opportunity to provide input to the United Nations (UN) Working Group on the Use of Mercenaries[1] on the provision of military and security cyber products and services by 'cyber mercenaries'. We are particularly appreciative of the Working Group's focus on the impact these actors can have on individual rights online, but also note with growing concern that unscrupulous use of these technologies can have a much broader and inadvertent effect, putting large parts of cyberspace at risk.

Microsoft has observed trends related to cyber conflict for years, focusing both on the evolving threat landscape and the political processes designed to keep the gravest attacks in check. While discussions at the UN First Committee have resulted in some progress, more needs to be done to keep up with constantly evolving technology and its uses. It is clear that, over time, what used to be the tools of a small set of highly sophisticated state actors a decade ago has significantly proliferated in numbers. Moreover, we have reasons to believe that at least certain state actors increasingly outsource some of their activities to groups that can then act on their behalf. This method of operation has been fueled by the emergence of a growing grey market for "cyberweapons".

For the purposes of this submission, we will use the term 'cyber mercenaries' to mean private military and security companies (PMSCs) that manufacture and sell cyber weapons, or what we call 'private sector offensive actors' (PSOAs). The type of activity that cyber mercenaries could engage in includes breaking encryption on particular devices, phones, or network infrastructure, and then surveilling specific targets (e.g., those critical of a particular regime). We believe these activities and associated tools represent a dangerous trend that must be curbed as soon as possible.

As a founding member of the Cybersecurity Tech Accord[2], a leading cybersecurity alliance bringing together over 150 technology companies, Microsoft has committed to not engaging in offensive operations online. We believe that the overall stability of our online world is endangered by cyber mercenaries, which are incentivized to profit from introducing risk into the digital ecosystem. We stand by that commitment and by our human rights responsibilities[3] in this space. Beyond that, we affirm our responsibility to act when we see others violate those rights. This is one of the areas where human rights and abuses are prevalent online and offline, including on the rights to privacy, freedom of expression, freedom of association, and the right to security. This led to our filing of an amicus brief in a legal case brought by WhatsApp against the NSO Group[4]. Earlier this year[5], we also proactively disrupted the use of these tools by another actor.

Against that background, we encourage the UN Working Group to issue a set of recommendations that help limit the use of these technologies. With that aim, our recommendations include:

- ***Advocate for responsible government action:*** States have tools in their toolboxes to curtail the destructive impact of these technologies. If and when governments procure these technologies, they can request to assess the vulnerabilities in their use to determine whether the exploit is one that is of a critical nature to the computing ecosystem, requiring it to be turned over to the technology provider.

---

[1] OHCHR | Report Cyber Mercenaries 2021

[2] https://cybertechaccord.org/

[3] Human rights statement | Microsoft CSR https://www.microsoft.com/en-us/corporate-responsibility/human-rights-statement?activetab=pivot_1%3aprimaryr5

[4] https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf

[5] https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/

With this framing, governments should make their procurement of these technologies more transparent and the control of their use subject to regulation.

- ***Establish greater transparency of cyber mercenary business practices***: Given the opaque nature of this market, the information regarding the relationship between companies that develop and sell cyber-capabilities and their clients is limited. To address this, it is vital to mandate greater transparency and oversight of their business practices. Governments should demand standards and transparency procedures that are clear and unambiguous, preventing the use of these tools within their borders without lawful process and clear guidelines that adhere to human rights protections.
- ***Urge all private sector actors, including cyber mercenaries, to respect human rights.*** Cyber mercenaries frequently threaten human rights, spanning from the right to privacy to freedom of expression. Encouraging all private sector entities to have a corporate responsibility policy in place would help clarify their obligations to human rights, due diligence, transparency and remedy.
- ***Advocate for international law to protect against the most egregious acts:*** Mercenaries have typically been regulated by international humanitarian law (IHL). However, in cyberspace, most of their operations, and those of their clients, take place during peace time and do not raise to the level of armed conflict. Ensuring that obligations and protections that apply under IHL are extended to circumstances under which these attacks occur would be a welcome step forward.
- ***Clarify the key question of legal immunity***: Certain cyber mercenaries have claimed that as they act on behalf of foreign governments the latter's legal immunity should apply to them. Should this argument be allowed to stand, it would enable the cyber mercenaries to continue their dangerous business without legal repercussions. As such, the need to address legal immunity in this context is essential.
- ***Encourage technology companies to raise the bar of access***: Responsible technology players have a key role to play in curbing the negative effects of these operations, which aligns with their commitment to respecting human rights. With that in mind, all technology players should be encouraged to shutdown infrastructure and accounts linked to cyber mercenaries and more proactively call out malign use of services and products.
- ***Determine accountability frameworks***: It is important to recognize that agreements around particular norms, while valuable, are not in themselves enough and that much stricter accountability frameworks need to be established. In the context of the use of cyber mercenaries, we urge states to highlight norm violations, introduce cases at the International Criminal Court to establish appropriate legal standards and pursue multilateral consequences for particularly egregious acts.

Current trends and developments

1. *Who are the clients and/or beneficiaries of cyber-capabilities and operations? Clients and beneficiaries can include for instance both State and non-State actors who contract "cyber mercenaries" and other actors operating alone or through private military and security companies (PMSCs) to acquire cyber-capabilities, including military and security services and products.*

   Cyber mercenaries provide services and capabilities for nation states that are otherwise not available to the nation state. Traditionally, as cyber capabilities grew, adversarial activity tended to come from states that could afford to do so – both financially and with sufficient competence. What has been troubling is that cyber mercenaries bring world-class capabilities to countries with low human rights protection, rule of law, and good governance. Countries that have been identified in public reporting as clients of cyber mercenaries include Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Mexico, Morocco, Nigeria, Oman, Saudi Arabia, and Sudan. As a result, it creates an environment that enables abuse.

The market cyber mercenaries operate in is opaque, and as a result their clients are difficult to identify. Groups selling malicious tools are private sector entities that apply strong confidentiality practices around the products, services and pricing associated with their offensive tools and services. Government entities acquiring these capabilities are likely to include intelligence services, police, or the military, ensuring that any procurement contracts are subject to national security restrictions and not public.

The impact of these companies' tools on the computing ecosystem is clear. When a cyber mercenary exploits a vulnerability in a product or service, they are putting the entire computing ecosystem at risk. Rather than reporting the vulnerability to the platform they exploit, they leverage the vulnerability in an attack. When the vulnerabilities are identified by third parties or identified publicly, companies are in a race against time to release protections before broad based attacks are released. This is a dangerous and difficult cycle.

Most of the information that we have about the actors involved, both on the provider and client side, comes from painstaking and difficult research into the tools used and understanding who the victims are. As highlighted above, Microsoft has conducted research into specific groups[6] that have used our software to deliver their weapons. By examining the malware and documenting how it works, we were able to discern that the attacks have largely targeted consumer accounts, indicating that particular individuals, rather than organizations, were targeted.

Organizations, such as the Citizen Lab[7] at the University of Toronto's Munk School and the CyberPeace Institute[8] work with the victims of such attacks to not only identify the malware, but to help individuals secure their devices and protect themselves in the future. Through their work, we know that some actors have targeted human rights defenders, journalists and other private citizens with negative impacts on their human rights. We saw this in our own research, with a group we call SOURGUM attacking over 100 victims around the world, including politicians, human rights defenders, journalists, academics, embassy workers, and dissidents. By understanding who the victims were, it was possible to speculate who the clients were – as the use of cyber mercenaries tends to indicate taskings or missions - a requirement to collect information about a person, or surveil an individual or their network and associates. Reported clients include state actors, some from authoritarian regimes and some from liberal democracies. With that in mind, we strongly urge the UN Working Group to encourage states to uphold their state duty to protect human rights online, in particular as it relates to the use of surveillance technologies.

2. *What is the role of actors, operating alone or through PMSCs, in a) developing, b) maintaining, c) selling, d) delivering cyber-capabilities (incl. military or security products or services in cyber space) to third parties, or e) carrying out cyber espionage?*

These companies are meeting a market need. States are looking for surveillance, access, or exfiltration capabilities against targets of interest. They are providing a service to regimes that cannot obtain access through their own capabilities. How the tools, services, or capabilities are leveraged depends on the need of the government customer. Cyber mercenaries have the ability to provide solutions for a government agency to manage on its own, or manage the service or operation on behalf of the agency.

This market suffers from an endemic lack of transparency, however we are able to speculate about how far the relationship can go with some certainty, based on the few occasions that contracts between

[6] https://blogs.microsoft.com/on-the-issues/2021/07/15/cyberweapons-cybersecurity-sourgum-malware/

[7] https://citizenlab.ca/

[8] https://cyberpeaceinstitute.org/

actors that develop cyber-capabilities[9] or third-party resellers[10] and government agencies were made publicly available. For example, during the legal case brought by WhatsApp against the NSO Group, the latter appealed to a lower court finding that they are not immune from claims that they violated the US Computer Fraud and Abuse Act by accessing mobile devices without permission. In doing so, they revealed their contractual relationship with their client. Their argument was that they were immune from US law because they were acting on behalf of a foreign government and hence share that government's legal immunity. That indicates that the cyber mercenaries' role is not limited to just selling the weapons to particular state groups, but that they provide support beyond that – in the execution of the actual operation.

3. *What are the motivational factors and strategic intentions of a) clients to recruit "cyber mercenaries" and the type of relationships they may have with them; and b) "cyber mercenaries" and other actors operating alone or through PMSCs in cyber space? Motivational factors can include for instance private gain, material compensation, ideological and other reasons.*

   It is our assessment that there are multiple drivers that are fueling demand for these types of services, as indicated in the first answer. The use of offensive tools by governments varies greatly. Some states use these tools for legitimate law enforcement access or national security purposes, pursuant to lawful process, and subject to the rule of law. More broadly, these tools and capabilities are used to enhance the capabilities of an agency to enable surveillance, access, or exfiltration for geopolitical purposes.

   What is driving the growth in the cyber capabilities markets is the fact that the market can provide turn-key surveillance capabilities without the law, policy, and technical overhead to grown capabilities organically and domestically. Instead of investing in developing those and associated frameworks, entities outsource it all to a private company that can not only offer specific hardware and software, but also provide certain services to the purchaser including technical support, equipment set-up and deployment. Outsourcing can sometimes also help government entities avoid difficult questions or skirt the edges of legal authority or oversight. Secondly, relying on private companies to develop this technology may offer a cheaper and faster option than building out the same capabilities within an organization or government.

   On the other hand, cyber mercenaries developing these capabilities are likely motivated by financial gain. The market for offensive cyber-capabilities is rapidly growing, is subject to little regulation, and offers an opportunity to make a significant profit.

4. *What are the types of cyber-services and products available (e.g., spyware/malware, AI), including their intended purpose in both conflict and non-conflict settings?*

   This is an adaptable and quickly evolving market that adjusts to the need of the customers, as well as the increased investments in cybersecurity that we are witnessing on the defensive side. As highlighted in our 2020 amicus brief[11] mentioned above, what we were able to observe were cyber-surveillance as a service, commercial-grade spyware (to obtain sensitive information / infringe privacy), and malware.

[9] Exhibit 1 through 11 – #1, Att. #1 in WhatsApp Inc. v. NSO Group Technologies Limited (N.D. Cal., 4:19-cv-07123) – CourtListener.com

[10] Here's the DEA Contract for Hacking Team's Spyware (vice.com)

[11] Draft Amicus Brief 12.20.2020 - FINAL (microsoft.com)

Moreover, earlier in the summer when we disrupted the activity of an actor we call Sourgum,[12] we published a detailed overview of the techniques and exploits used in that particular case.

However, those two examples are likely to only be the tip of the iceberg. The types of services and products available today are likely to be supplemented by new offerings tomorrow. For example, in Apple's September 2021 release of emergency software updates for a vulnerability under exploit by NSO Group's Pegasus software,[13] the method used is known as "zero click remote exploit". This can turn on a user's camera and microphone, record messages, texts, emails and calls without tipping off the victim and then sends back information to NSO's clients at governments around the world.

5. *What role do new technologies play in causing harm remotely in the context of cyber operations, and what are the risks involved? How would you define "directly participating in cyber operations"?*

There are a range of harms that arise from the use of new technologies in cyber operations. In terms of human rights, the use of malware and spyware to engage in targeted surveillance or conduct offensive cyber operations pose a significant threat to freedom of opinion and expression, particularly in the context of facilitating the targeted surveillance and attacks of human rights defenders, civil society activists, and political dissidents. Even the threat of surveillance can have chilling effects on people's online activities and can shape and restrict "*their capacity to exercise the rights to freedom of expression, association, religious belief, culture and so forth*", as mentioned by Special Rapporteur David Kaye in his June 2019 report to the UN Human Rights Council.[14] This is coupled with an infringement on an individual's privacy.

Moreover, there are broader implications for the overall security and stability of the online environment. While some governments may share high-consequence vulnerabilities they discover with impacted technology providers so the providers can patch the vulnerability and protect their customers, cyber mercenaries are primarily incentivized to keep these vulnerabilities to themselves so they build weapons and profit off them. This dynamic creates reverse incentives for security and an insecure digital environment for the broader online community, exposing users to become vulnerable given the lack of security patches and measures. This is also alarming given that the vulnerability that is being exploited is not being fixed, impacting victims more broadly and exposing customers to harm.

New technologies, particularly cloud computing, help address risk from these types of cyber weapons. It is unfortunately too often up to the victim to manage the security of their own devices and data and they are ill-equipped to do so against an advanced and persistent threat. When customers migrate to the cloud, they benefit from the fact that companies like Microsoft have large teams of threat intelligence experts and security personnel who can identify and mitigate risks at scale. That makes it a much harder fight for the adversaries.

Lastly, we define directly participating in cyber operations as knowingly and intentionally developing tools and offering services that allow unauthorized access to data and computer systems.

Regulatory frameworks and their application

[12] https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

[13] Apple Security Update Closes Spyware Flaw in iPhones, Macs and iWatches - The New York Times (nytimes.com)

[14] OHCHR | The Special Rapporteur's 2019 report to the United Nations Human Rights Council

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

7. *Please provide information on specific national or regional norms and/or regulations governing the provision of security products and services in cyber space by actors operating alone or though PMSCs and other relevant actors.*

8. *Please provide information on existing national, regional or international frameworks and mechanisms to investigate, and hold individuals, groups, States or companies accountable for abuses in cyber space, including for espionage, cyber-operations, illegal services or products, and their effectiveness.*

The questions on the regulatory frameworks and their applications are closely aligned. As such, we will answer them as part of a single response.

Export Control & the Wassenaar Arrangement

Export control laws have largely been the foundation for attempting to address risks from cyber mercenaries. The Wassenaar Arrangement has been utilized as a convening location for governments to discuss the dissemination of tools and techniques used by cyber mercenaries. The Agreement, not originally developed with the digital world in mind, was established to contribute to international security and stability by promoting transparency in transfers of conventional arms and dual-use goods and technologies. Over the past decade, participating states took on the difficult task of trying to regulate surveillance software to limit human rights abuses. States defined intrusion software as "*software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures*" and that either extracted data from a computer or network device or modified the "*standard execution path*" of a program to allow "*the execution of externally provided instructions*."

Following an agreement of a specific text under the Wassenaar umbrella, participating states must then implement national policies that ensure that the transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals. The EU, for example, in 2021 adopted Dual-Use Regulation[15], which introduces a new end-use control on cyber-surveillance equipment, where the exporter is aware or has been informed that the exported items are or may be intended for use in connection with internal repression or the commission of serious violations of human rights and international humanitarian law. This applies to items (whether or not listed) that are specially designed to enable the covert surveillance of natural persons by monitoring, extracting, collecting or analyzing data from information and telecommunication systems. Many other states have not yet implemented the rules.

The broader point about export control and Wassenaar is that neither are the right places to have discussions about the domestic use, procurement, or production of advanced cyber weapons that enable surveillance, exfiltration, obfuscation, or destruction. Countries should be having open discussions about the appropriate metes and bounds for law enforcement and national security agencies to use offensive technologies domestically and internationally. Hiding the national discussion behind back-door conversations about export control guarantees that these issues languish in the dark. That benefits countries that want to continue offensive use without meaningful restraint or management, but fails to address the broader global impact when offensive tools are used in truly offensive ways. It is time to move away from export control, and into the arena of direct regulation for these types of technologies and the companies that develop or use them on behalf of customers.

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0821

United Nations processes

More broadly, states in the United Nations First Committee processes have focused on this space, and in particular the responsibilities of states, for over a decade. Throughout a series of convenings of the Group of Governmental Excerpts (GGE), in 2021 it agreed on the *Framework for Responsible State Behavior* in Cyberspace, building on the broad agreement that international law and the 11 norms of behavior adopted by the GGE in 2015[16] apply to cyberspace. Of the 11 norms, there are a few specific ones that are relevant to cyber mercenaries, such as i) states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions; ii) states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age; and iii) states should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices.

Moreover, the Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) is a parallel working group in the UN First Committee. It is also focused on international cybersecurity rules, norms and principles for responsible behavior, regular institutional dialogue, confidence building measures, capacity building and the application of international law in cyberspace, bringing together all members of the general assembly. Much like the GGE, it has adopted a consensus report in 2021[17], but will continue its work over the next few years.

Also worth noting are the UN Guiding Principles on Business and Human Rights[18], which set out a framework under which business actors must respect human rights. These also apply to companies engaged in the provision of security products and services in cyberspace. In this regard, the work[19] of the Special Rapporteur on the Freedom of Expression is also particularly important to highlight.

Though evident that there are multiple processes at the UN that are relevant to the use of cyber mercenaries, this forum needs to do more to effectively address the growing and unrestrained dark market in which PSOAs operate. Broad obscurity on these topics benefits countries that want to continue offensive use without meaningful restraint or management, failing to address the broader global impact when offensive tools are used in truly offensive ways.

Industry led initiatives

- Broad investigations: Efforts like Citizen Lab's recent work on NSO Group, and WhatsApp's lawsuit against them, highlight the impact of offensive products and services on Internet users globally. Continued support and funding for deeper investigations and understanding into offensive tools and their impacts is essential to driving a broader public discussion about the impacts of this space.
- Disrupt Actors: Microsoft's disruption of the SOURGUM actor is a recent example of how the identification of vulnerabilities in use by PSOAs can be stopped when the vulnerabilities are identified or disclosed to the vendor, and then patched. Disabling accounts or malware used by PSOAs are also essential to having global impact. Apple's recent updates to mitigate vulnerabilities from NSO Group are another example of ways in which the private sector can help disrupt PSOA action.

[16] https://undocs.org/A/70/174

[17] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[18] https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

[19] https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/SR2019ReportToHRC.aspx

- Cybersecurity Tech Accord: Industry initiatives like the Cybersecurity Tech Accord[20]– a coalition of over 150 technology global technology firms working to be the industry's voice on peace and security online– are an important way the private sector can take greater responsibility. Through a shared commitment and collective action, signatories aim to more effectively:
    - Provide their customers, users and the developer ecosystem with information and tools that enable them to understand current and future threats and better protect themselves.
    - Protect their customers and users everywhere by designing, developing and delivering products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.
    - Work with each other and likeminded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure and threat sharing, as well as ensuring flexible responses for the wider global technology ecosystem.
    - And particularly pertinent, oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution and use.

Accountability

Investigations and prosecutions for cyber activities that negatively impact human rights have been relatively limited to date. However, ongoing litigation and complaints show that there are potentially several different legal avenues for pursuing accountability for such activities. One example is a lawsuit by WhatsApp against spyware vendor NSO Group, which Microsoft also joined[21]. WhatsApp sued NSO Group in 2019, alleging that its software was used to hack 1,400 devices, some of which belonged to journalists and human rights campaigners.

Separately, industry is also taking concrete operational measures to aid efforts on this front. As mentioned, in 2021 Microsoft disrupted[22] the use of certain cyberweapons manufactured and sold by a group we call *Sourgum*— what we believe to be an Israeli-based cyber mercenary. The weapons disabled were used in precision attacks targeting more than 100 victims around the world including politicians, human rights activists, journalists, academics, embassy workers and political dissidents.

States also have tools in their toolboxes to curtail the destructive impact of these technologies. If and when governments are procuring these technologies, they can request to assess the vulnerabilities in use, to determine whether the exploit is one that is of a critical nature to the computing ecosystem, requiring it to be turned over to the technology provider. Governments can demand standards and transparency procedures that are clear and unambiguous, preventing the use of these tools within their borders without lawful process and clear guidelines. Governments can make their procurement of these technologies more transparent, and the control of their use subject to regulation.

Finally, it is important to recognize that agreements around particular norms, while valuable, are not in themselves enough and that much stricter accountability frameworks need to be established. With that in mind we urge states to:

[20] Cybersecurity Tech Accord (cybertechaccord.org)

[21] https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

[22] https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/

- *Highlight norms violations*. The attribution of a cyberattack to a state that is in violation of international norms, even when using a third party, should always include an explicit and direct articulation of which norm was transgressed and how. Where reasonable, greater transparency in the underlying information used to draw conclusions will lend greater credibility to any attribution and will further strengthen the recognition of norms.
- *Introduce cases at the International Criminal Court (ICC)*: Bring cases before the ICC to help establish the appropriate legal standard for attributing a cyber-attack as an internationally wrongful act to a particular state.
- *Establish deterrence doctrines*. Rather than further escalating tensions, clear doctrines of measured consequences for cyberattacks in violation of international agreements will help deter further belligerence, as well as provide necessary clarity about what responses can be expected, and test the doctrines by supporting actual deterrence exercises.
- *Multilateral consequences*. Beyond deterrence doctrines established by individual nations or coalitions, the international community as a whole should pursue the establishment of clear, non-escalatory consequences for violations of established norms, rules and principles through existing forums and structures.

Human rights and IHL impacts of cyber-capabilities and operations conducted by actors operating alone or through PMSCs

9. *Please describe how the development and use of cyber-capabilities, operations and services (e.g., attacks on digital/physical infrastructure and data, surveillance of individuals) by actors operating alone or through PMSCs can cause and contribute to human rights abuses and violations in non-conflict settings. This includes for instance the rights to life, physical and mental integrity, self-determination, privacy, health, vote, freedom of movement, assembly and association that could be affecting individuals or groups, such as human rights defenders, opposition leaders, or journalists.*

   We know through our assessments of state and cyber mercenary actors that the majority of attacks are aimed against those that have knowledge or information that is useful to the attacking state. That often sweeps in journalists, human rights defenders, civil society leaders, and dissidents globally. We see non-profit organizations and academics targeted for information about COVID-19, we see prominent human rights defenders targeted around major geopolitical events or elections, and we see journalists targeted for insights related to their reporting. In each case, the actor either compromises the account or targets the victim by observing details about their accounts or other metadata that is exposed publicly, potentially for use in later attacks.

   At the same time, it is important to note that the tools and techniques used can impact a much broader community. For example, a particularly determined adversary might use a zero day, or previously undisclosed, vulnerability on a widely used platform to get access to information pertaining to a particular individual. However, this individual is not the only person using that platform and the vulnerability is not specific to him. As a result, the attacker has potentially exposed millions of other uses – private individuals and corporates, including in critical sectors - of the platform to attacks.

10. *Please describe how the development and use of cyber-capabilities, operations and services by actors operating alone or through PMSCs can cause and contribute to breaches of international humanitarian law during armed conflicts and its impact on civilian populations.*

    It is important to recognize that states have, until fairly recently, struggled to agree whether International Humanitarian Law (IHL) applies to cyberspace and that the topic continues to carry a level

of controversy. Microsoft has argued that IHL should and does apply do cyberspace, and indeed its application has been supported by liberal democracies, as evidenced by both the first[23] and second[24] editions of the Tallin Manual. The latter also provide useful examples of activity covered by definition of cyber mercenaries. Moreover, the community of states represented at the United Nations, have been able to include a reference to IHL's application to cyberspace in the 2021 report[25] of the UN Group of Governmental Experts, which we expect will shortly be confirmed by the General Assembly.

With that agreement in mind, the term 'mercenary' is defined by Article 47[26] of Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (Additional Protocol I). Under Protocol I, a mercenary is a person who directly takes part in hostilities; is specifically recruited to take part in such hostilities; is motivated by private gain; is neither a national of or a resident of a Party to the conflict; is not a member of the armed forces of a Party to the conflict; and has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces. We believe this definition should apply to cyberspace.

Moreover, there have been several cases that have dealt with when states are responsible for the behavior of the individuals or entities acting on their behalf. It is clear that this includes its own organs, personas acting under governmental authority (even when they exceed it), as well as persons or entities whose activities the state later endorses. The most discussed issue relates to entities operating under the direction, instruction, or control of the state[27]. In particular what constitutes control remains unclear and has not been well articulated in the cyberspace context. In the Nicaragua case, the International Court of Justice indicated that international law contains a rule imposing responsibility on a state for acts of those non-state actors over which it has "effective control", a fairly onerous standard involving ordering the behavior or directing an operation. On the other hand, the International Criminal Tribunal for Formal Yugoslavia established a looser standard of "overall control" in the Tadic case[28], which was also confirmed in the Lubanga case[29] at the International Criminal Court. This test requires "more than the mere provision of financial assistance or military equipment or training" but not going so far as to insist on the "issuing of specific orders by the state, or its direction of each individual operation."

However, it is our view that the application of IHL to this domain is not sufficient to help address the challenges we face, given the nature of conflict in cyberspace. The vast majority of attacks do not take place as part of armed conflict and do not raise to the level of armed attack. Under those circumstances, IHL protections and responsibilities do not apply. With that in mind have called out the prohibition of indiscriminate and disproportionate attacks and the obligation to take precaution to avoid or minimize incidental damage to civilian infrastructure or harm to civilians as needing to be extended to peacetime operations.

---

[23] https://ccdcoe.org/research/tallinn-manual/

[24] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (cambridge.org)

[25] https://www.un.org/disarmament/group-of-governmental-experts/

[26] Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts, 8 June 1977 (Additional Protocol I) U.N.T.S. 3

[27] Draft Articles on the Responsibility of States for Internationally Wrongful Acts" in Report on the Work of its Fifty-first Session (May 3-July 23, 1999), UN Doc A/56/10 55 [3] ("ASR")

[28] International Criminal Tribunal for the Former Yugoslavia (ICTY) adopted a looser standard of "overall control" for the purposes of IHL in the Tadić case. Prosecutor v. Dusko Tadić aka 'Dule' (Judgment) ICTY-94-1-A (15 July 1999) ¶¶131-145, 162.

[29] Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Trial Chamber, Judgement (Int'l Crim. Court, March 14, 2012) ¶541.

We hope these responses provide a helpful contribution in advancing a shared objective: achieving a rules-based and rights-respecting online world for all. More than anything else, we believe accomplishing this requires trust and cooperation across stakeholder groups with responsibilities in the digital ecosystem, underscoring the value of precisely this sort of outreach. Please let us know if we can provide any additional input or clarify any of the contributions provided here. We look forward to additional opportunities to collaborate in the future.