The Citizen Lab's response to the questionnaire of the Working Group on the use of mercenaries *on the provision of military and security products and services in cyber space by cyber mercenaries and related actors and its human rights impact*

In a recent report to the General Assembly (A/75/259), the Working Group on the use of mercenaries identified "cyber mercenaries" as one category of actors that can generate mercenary-related activities. This entails 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.

The Working Group welcomes any information deemed pertinent to the issue, and is particularly interested in the below mentioned areas. While addressing the questions, please provide **examples, good practices and recommendations** to the extent available that you consider important in the context of this questionnaire, as well as any analysis on future developments in this area.

Current trends and developments

1. Who are the clients and/or beneficiaries of cyber-capabilities and operations?

These 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.

We have developed only an imperfect and incomplete picture of how State and non-State actors contract for cyber-capabilities and what kind of services they are purchasing. This incomplete picture is the result of a number of factors, including that most companies operating in this space are private companies (non-listed), the environment in which these business actors operate lack transparency, and there are significant challenges in researching and tracking the deployment of cyber-capabilities.

Despite these challenges, the Citizen Lab's research has helped shed light on what State and non-State clients are likely contracting for cyber-capabilities sold by the private sector. These findings show that a range of State actors have contracted with private companies (such as Gamma Group, FinFisher, Hacking Team, Cyberbit, and NSO Group, or through third-party resellers) in order to acquire sophisticated cyber-capabilities, such as highly intrusive spyware and malware. For example, the Citizen Lab has identified the use of NSO Group's Pegasus spyware by State actors against a range of targets in civil society, as well as Ethiopia's deployment of the PC Surveillance System spyware produced by Cyberbit against Ethiopian dissidents. These are just two examples of many, with additional cases described in this resource document which summarizes the Citizen Lab's research regarding the deployment of network traffic management and device intrusion for targeted monitoring technology against civil society.

Further, State and non-State actors also engage in less technically sophisticated forms of cyber campaigns (e.g., disinformation and phishing campaigns, rather than the deployment of expensive spyware technologies) and are contracting with private actors for some of these capabilities. In 2020, for example, the Citizen Lab revealed a massive hack-for-hire phishing operation which targeted advocacy groups and civil society in the US, among other targets, and relied on the services of an India-based company called BellTroX InfoTech Services. Private cyber security companies have also attributed cyber activities against civil society and human rights organizations to non-State actors. For example, FireEye has observed an operator called TEMP.Periscope undertaking cyber operations, including against human rights organizations in Cambodia, and concluded there is "little doubt" that the group works on behalf of the Chinese state.

There is no obvious and apparent unifying theme among the State and non-State actors that purchase these technologies, other than perhaps the fact that these technologies are prone to abuse and have been used to target journalists, human rights defenders, civil society, and members of the political opposition. For example, the Citizen Lab's research shows that countries interested in this technology include both democratic and non-democratic regimes, as well as countries that have in-house offensive cyber development capabilities (such as the US) along with those that likely do not have such extensive resources (such as Ethiopia). Further, it is clear that a range of different agencies and institutions within a State may have an interest in this technology. For example, in a report on the exploitation of SS7 vulnerabilities by a company called Circles—which is an affiliate of NSO Group, the developers of the Pegasus spyware—we identified a total of 25 governments likely to be customers of this company, including directorates of intelligence and security services, police, armies, and navies.

Actions that could lead to greater insight into the different State and non-State actors that contract for cyber-capabilities and the businesses engaged in this market include robust transparency requirements in export licensing for the sale and transfer of cyber-capabilities and real enforcement to ensure compliance with such transparency requirements as well as the substantive rules of export control. Further, the imposition of regulation on private actors that develop and sell cyber-capabilities—such as specifically-tailored mandatory due diligence obligations, legally-imposed limitations and controls on end-users through mandatory contractual terms and technical specifications, independent oversight boards, and public reporting requirements—could also serve to mandate much needed transparency.

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?**

Due to the same challenges highlighted in Question 1 in researching the marketplace for cyber-capabilities, insight into how actors develop, maintain, sell, deliver cyber-capabilities to third parties, and carry out cyber espionage, is relatively limited. However, publicly-available contracts between actors that develop cyber-capabilities and government agencies or between third-party

resellers of such capabilities and government agencies help shed some light on the dynamics of this marketplace. In short, these documents suggest that companies that develop spyware and malware also provide professional services to purchasing States (such as set-up and deployment and maintenance and support) and likely have some insight (or maintain the capacity to have insight) into how customers deploy these technologies and against what types of targets.

For example, a contract between a company reselling NSO Group's technology (Infralocks Development Limited) and the Government of Ghana shows that a private actor may have significant responsibilities in terms of infrastructure set-up, deployment, and providing troubleshooting and other services (see Exhibit 11 to the *WhatsApp v. NSO Group* litigation in N.D. Cal in the US, starting at p 67). The terms of the contract provided that the Government of Ghana purchased not only the equipment and technology itself, but also a variety of associated services. These services were defined to include the "[d]eployment of the System at the End-User's site", a two-week training course, and a one-week side handover (p 74). Similarly, product documentation for NSO Group's Pegasus spyware—also filed in the same litigation—confirmed that NSO Group is responsible for deployment of the technology at the client's site, training sessions, and system testing prior to hand-over to the client (see Exhibit 10 to the *WhatsApp v. NSO Group* litigation, p 61 and following). Further, Pegasus spyware comes with one year of maintenance, support, and upgrade services (p 64). Of course, this is just one example; contracting practices likely differ between various businesses and clients and the details of related contracts.

Novalpina Capital and NSO Group have made certain statements in correspondence between the companies, the Citizen Lab, and civil society regarding their relationship with government clients. However, these statements have been contradictory, leading to confusion regarding the true nature of the relationship between this company and its client. These contradictions were highlighted by former UN Special Rapporteur David Kaye in a communication dated 20 February 2020 to NSO Group. The Special Rapporteur noted that NSO Group has claimed that the company is limited by "technological and commercial boundaries…to track each specific usage" and that "operational visibility is simply not permitted." At the same time, the company has stated that it conducts "a thorough inspection" of its clients and that the "systems have records and it is impossible to act against a target [such as murdered Saudi journalist Jamal Khashoggi] without [NSO Group] being able to check it."

Other publicly-available contracts for spyware include that between the US Drug Enforcement Agency and Cicom USA for the purchase and sale of Hacking Team's spyware technology. This contract included not only specific hardware and software, but also that certain services were to be provided by Hacking Team to the purchaser including technical support and equipment set-up. In the 2015 hack of the Hacking Team website, a number of other contracts between Hacking Team and/or third party resellers and governments (including countries like Sudan and Morocco) were also divulged. While a complete analysis of these contracts is beyond the scope of this submission, the provision of professional services and maintenance was a part of some of these contracts with authoritarian states, such as Ethiopia.

Without mandating greater transparency and oversight of the practices and business activities of companies like NSO Group, there remains limited insight and information regarding the relationship between companies that develop and sell cyber-capabilities and their clients and the companies' role in developing, maintaining, selling, and delivering cyber-capabilities to third parties and carrying out cyber espionage. In addition to the actions suggested in Question 1, it would be beneficial to ensure that companies engaged in developing and selling specific types of cyber-capabilities are required to sell directly to government agencies and are prohibited from selling through third-party resellers. The use of third-party resellers of cyber-capabilities further complicates and obfuscates the true end-user of a technology and may provide companies with corporate structuring options to circumvent export control rules or complicate the enforcement of such rules. For example, after the US Drug Enforcement Agency contracted for Hacking Team spyware, the contract for these services was left undiscovered for a period of time possibly in part because of Hacking Team's use of a third-party reseller in the US to sell the technology rather than a direct contract between Hacking Team and the US government. Further, an extension or adaptation of the "know your customer" regulations covering financial institutions to companies selling commercial spyware and related services could also bring welcome transparency to such transactions.

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.

The Citizen Lab's research is concerned with how the development and use of cyber-capabilities violates international human rights law and impacts human rights defenders, journalists, and other members of civil society. For example, the Citizen Lab's research has shown that NSO Group's Pegasus spyware—along with cyber-capabilities developed by companies like Hacking Team, FinFisher, and Gamma Group—have been used against targets that are opposed to the State and are challenging the social and political *status quo* (e.g., journalists, opposition politicians, and dissidents residing abroad and within the country).

Within this scope of research, we have seen that States (and non-State actors, who are likely working at the direction of or with the support of States, although proving this State support may be challenging) are motivated by a desire to acquire information regarding individuals engaged in social, political, and human rights advocacy work, which can then be used for various nefarious purposes (e.g., to execute online smear campaigns with personal communications or pictures collected from the target, to blackmail targets, to identify and persecute other individuals who may be linked to the target through the information collected from the target, to understand an activist's network, or to use information to mount malicious prosecutions). Such actors may also be motivated to acquire and deploy cyber-capabilities in order to proactively silence dissent

through the chilling effect that these technologies have regardless of whether or not they are deployed successfully.

Because end-to-end encryption increasingly makes State access to digital communications difficult, and because online communication is dominant, there is also a general growing appetite among State and non-State actors for technological solutions that circumvent this type of digital security feature. While State and non-State actors may be able to build technologies of circumvention in-house or enact regulation that facilitates the use of legally-mandated backdoors, State and non-State actors are also likely motivated to rely on private companies developing this technology because this offers cheaper options than building out the same capabilities within an organization or government itself or enacting (likely unpopular) legislation that mandates such entry points. Further, as technology is quickly evolving and government development capacities may operate at a slower pace, private companies developing cyber-capabilities may provide a greater range of technological solutions than can be developed in-house in the same time frame.

Companies developing cyber-capabilities are likely motivated to participate in this market because of the existence of a strong business case for these types of companies, namely that the market for offensive cyber-capabilities is rapidly growing, is subject to little regulation, and offers an opportunity to make a significant profit. It is also likely that some of these companies receive State support and benefit from close connections to government military and defense. For example, it is common knowledge that graduates of Unit 8200 in the Israeli military have direct pathways towards joining the offensive cyber-capabilities sector in Israel after leaving the military.

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?

The Citizen Lab studies digital technologies and how they impact human rights. Through this research, the Citizen Lab has detailed numerous deployments of a range of surveillance technologies—from sophisticated spyware and malware to less technically complex phishing campaigns—in various conflicts (e.g., Syria) and non-conflict settings around the world. While the specific purpose of each operation may not be evident on its face, it can be inferred from the profiles of the operators studied by the Citizen Lab that they are generally seeking information regarding specific targets in order to silence a target or a target's friends, family, and colleagues, to gather evidence to aid in the persecution of a target or individuals within that the target's network, or to interfere, subvert and/or neutralize in some way their political and social advocacy. Below is a brief summary of the various targets researchers at the Citizen Lab have encountered:

- In 2012, the Citizen Lab documented the deployment of the FinFisher suite against Bahraini pro-democracy activists.
- In 2013, the Citizen Lab documented the use of this same technology in Ethiopia against opposition members. Amnesty International has also documented the use of FinSpy against Egyptian human rights defenders.

- In 2014, the Citizen Lab described the deployment of Hacking Team's Remote Control System (RCS) spyware against members of the Ethiopian Satellite Television Service.

- In 2016, the Citizen Lab documented how Ahmed Mansoor, an Emirati human rights defender who has been sentenced to ten years in jail, was targeted with NSO Group's Pegasus spyware. The Citizen Lab has also described a broader campaign of targeted spyware against Emirati journalists, activists, and dissidents.

- Between 2017 and 2019, the Citizen Lab published a series of reports regarding the use of Pegasus spyware in Mexico against a number of targets, namely a scientist at the Mexican National Institute for Public Health and employees at non-governmental organizations working on obesity and soda consumption; journalists and lawyers working on a range of issues including investigations of corruption by the Mexican President and the government's participation in human rights abuses, along with the minor child of one of the targets; senior politicians with the National Action Party; investigators into the 2014 Iguala Mass Disappearance; lawyers representing the families of three slain Mexican women; the director of a Mexican anti-corruption group; and the director of the publication *Río Doce*, a colleague of slain journalist Javier Valdez Cárdenas (who was also a journalist with that same paper as well as its founder), and Javier Valdez Cárdenas' wife.

- In 2018, the Citizen Lab documented how an Amnesty International researcher and a Saudi activist based abroad were targeted with NSO Group's technology. The Citizen Lab also documented how Omar Abdulaziz, a Saudi dissident and permanent resident in Canada, was targeted with Pegasus spyware.

- In 2019, the Citizen Lab, along with WhatsApp, confirmed over a hundred cases where NSO Group's technology was deployed using a now-patched vulnerability in the WhatsApp encrypted communications application against human rights defenders, activists, journalists, and politicians around the world.

- In early 2020, the Citizen Lab showed how *New York Times* journalist Ben Hubbard, who had conducted extensive reporting on Saudi Arabia, was targeted with NSO Group's Pegasus spyware in 2018.

In addition to the above-described deployment of commercial-grade spyware and malware, the Citizen Lab has also outlined the deployment of malware linked to the Burmese government against non-governmental organizations; malware and phishing campaigns against political opposition in Latin America; malware campaigns against the Syrian opposition during the ongoing conflict in Syria; extensive espionage campaigns against Tibetans; and phishing campaigns against Egyptian civil society.

Drawing on two decades of research into the deployment of cyber-capabilities against human rights defenders and civil society, the Citizen Lab has categorized at least three distinct models that characterize the capacities and tactics of actors carrying out targeted digital attacks. The **first model** can be described as situations where State and non-State actors have the in-house capabilities and resources to develop their own customized malware and conduct wide scale

operations (also referred to as Advanced Persistent Threats within the industry). Such operations are generally the purview of well-resourced States, or cyber mercenary groups engaged (formally or informally) by State actors. A **second model** involves attacks based on Remote Access Trojans (RATs) circulated among criminals and hobbyists, but which are then deployed for political reasons, such as during the Syrian conflict. These operations are conducted by State actors or groups that may be directly sponsored, encouraged, or accepted by States. Finally, the **third model** engages the procurement and use of commercial "lawful intercept" products and services (such as Pegasus's NSO Group) that provide turnkey surveillance capabilities. The high cost of these products and the claim by vendors that they transact only with State actors suggest that these technologies are likely to be used by State actors, although there is evidence that such businesses also sell through third party resellers and that non-State actors may obtain these capabilities (for example, there are allegations that the Mexican cartels have obtained spyware sold to the Mexican government).

The Citizen Lab has compiled an annotated resource describing the technology it has documented as being deployed against human rights defenders and other members of civil society in violation of international human rights law. Privacy International has also developed a resource—the Surveillance Industry Index—which categorizes and documents a broader range of cyber-services and products.

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"?

A. Harms associated with new technologies in cyber operations

A range of harms arise from the use of new technologies in cyber operations. The Citizen Lab's research is particularly focused on how such technologies detrimentally impact international human rights. The deleterious human rights impact of new cyber technologies such as sophisticated one-click or no-click spyware, malware, deep packet inspection (DPI) systems, and Internet filtering technologies have been discussed in detail by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, in multiple reports to the UN. In his 2017 report to the UN Human Rights Council, the Special Rapporteur addressed the role played by private actors engaged in the provision of Internet and telecommunications. He observed that the "multiple uses" of design network equipment and technology raised freedom of expression and privacy concerns. For example, DPI technologies, which could be used for innocuous purposes, "have also been employed to filter Internet content, intercept communications and throttle data flows."

As the Special Rapporteur stated, the improper use of DPI and Internet filtering technologies to mediate publicly-available Internet access by States poses a significant threat to human rights when that filtering is applied covertly, arbitrarily, without due process, or without regard for legitimate forms of expression. The practice of Internet filtering most directly threatens the right to freedom of opinion and expression (UDHR Art. 19, ICCPR Art. 19). This right includes the absolute right "to hold opinions without interference" (ICCPR Art. 19(1)), as well as the "freedom to seek, receive and impart information and ideas

of all kinds, regardless of frontiers" whether online or otherwise (ICCPR Art. 19(2)). While freedom of expression is not an absolute right, State restrictions on freedom of expression are subject to strict conditions (ICCPR Art. 19(3)).

The use of malware and spyware to engage in targeted surveillance also poses a significant threat to freedom of opinion and expression, particularly in the context of facilitating the targeted surveillance of human rights defenders, civil society activists, and political dissidents. As Special Rapporteur David Kaye noted in his June 2019 report to the UN Human Rights Council, 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 the Special Rapporteur summarized: "In short, interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression." Further, technology like DPI systems, Internet filtering technologies, and spyware and malware also impacts the right to privacy (UDHR Art. 12, ICCPR Art. 17). While restrictions on the right to privacy are permissible, such restrictions are subject to strict limitations under international law. Further, given that targeted surveillance disproportionately impacts vulnerable groups, including racial, religious, ethnic, gender, and sexual minorities, State surveillance practices arguably may also violate international human rights prohibitions on discrimination and protections for minority rights (UDHR Art. 7, ICCPR Arts. 26 and Art. 27) and may infringe upon other rights such as the rights to liberty and security of the person (UDHR Art. 3, ICCPR Art. 9).

B. Other risks of new technologies in cyber operations

In addition to human rights harms, there are a number of other risks that arise in States' use of new technologies in cyber operations, with a specific focus on spyware and malware. These highly intrusive technologies rely on vulnerabilities in software that is generally used by a large segment of the public (e.g., the WhatsApp application, which was used to deliver NSO Group's spyware in an attack against hundreds of human rights defenders in 2019). States' purchasing of these technological 'solutions' to get around end-to-end encryption necessarily requires that the vulnerabilities used to inject spyware are left open, and thus constitute a security risk for the general public. In particular, there is a risk that such vulnerabilities, and the associated technologies that facilitate access to communications, may be obtained and leveraged by non-State, criminal actors and outside the bounds of any legal framework.

There is also the risk—which has evidently materialized numerous times—that a government agency will purchase these technologies and use them in a manner considered an illegal purpose under international human rights law, such as for spying on human rights defenders, the media, lawyers, and civil society more broadly. Governments may use access to these technologies to suppress dissent both within and outside their borders. Governments—including States generally considered to be rights respecting and with adequate rule of law—may also deploy these technologies in the absence of public transparency and appropriate legal frameworks calibrated to the intrusive nature of these technologies. Finally, governments may acquire these tools and then provide them to non-State actors.

Regulatory frameworks and their application

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).

This question is answered in two parts. First, it considers non-binding 'norm-setting' frameworks regarding conduct in cyberspace. It is within these broader frameworks and discussions that progress is made towards binding instruments and the developments of substantive and procedural legal norms. Second, it considers binding regulatory and legislative frameworks that may directly or indirectly address cyber conduct. This answer is not intended to be exhaustive, but rather to provide an initial indication of the variety of frameworks that apply to conduct in cyberspace. A more exhaustive account of cyber norms is available from the Carnegie Endowment for International Peace here and the Hague Program for Cyber Norms here.

A. Non-binding, 'norm-setting' frameworks

Non-binding frameworks and forums for the advancement of norms applicable to conduct in cyberspace take place in a variety of international, regional, and national forums. Stakeholders include not only States, but also technology companies and private actors. The following is a high-level selection of different types of forums and frameworks for engagement, and is not intended to be exhaustive. Rather, it illustrates the diversity and scale of discussions regarding this issue.

International:

The UN has provided a forum in which States have been discussing and debating the application of international law to the use of ICTs and cyberspace, as well as broader issues of international security and ICTs. In particular, these discussions have taken place through a series of UN Groups of Governmental Experts (UN GGE) first starting in 2002. Other organizations have also sought to prompt multilateral processes of their own, including the Shanghai Cooperation Organization, the G7, and the G20. Further, the UN has provided a forum to discuss the role of international human rights law in cyberspace. For example, reports and communications by the Special Rapporteur on the promotion and protection of freedom of opinion and expression have engaged with State conduct in cyberspace through the lens of international human rights law.

The *Tallinn Manual*, authored by international law experts, was first published in 2013 (with a second version issued in 2017 and a third version being discussed). While a non-binding document, it is considered as an exhaustive and authoritative account of the application of international law in cyberspace.

In September 2011, Russia, China, Tajikistan, Kazakhstan, Kyrgyzstan, and Uzbekistan submitted to the UN General Assembly a proposal for an *International Code of Conduct for Information Security*, a series of politically binding measures designed to maintain international stability and security. The chief undertaking would be a commitment by States "not to use Information and

Communication Technologies… to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies." A revised *Code* was circulated in January 2015 that retained the bulk of the measures directed at prohibiting cyber interference "in the internal affairs of other States or with the aim of undermining their political, economic and social stability."

At the 2016 G7 Ise-Shima Summit, G7 Member States issued the *G7 Principles and Actions on Cyber*, which focuses on promoting security and stability in cyberspace. Further, in 2017, the G7 issued the *G7 Declaration on Responsible State Behaviour in Cyberspace,* which "encourages all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT." In 2019, the G7 issued the *Dinard Declaration on the Cyber Norm Initiative*, which affirms its willingness to establish a Cyber Norm Initiative "dedicated to sharing best practices and lessons learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behaviour." Also in 2016, NATO issued the *Cyber Defence Pledge,* which aims to "ensure the Alliance keeps pace with the fast evolving cyber threat landscape" and that NATO Member States "will be capable of defending themselves in cyberspace."

The *Paris Call for Trust and Security in Cyberspace*, issued by President Macron in 2018, articles nine principles to secure cyberspace. The *Paris Call* is supported by a selection of States, public authorities and local governments, organizations and civil society members, and private companies. In 2018, the Commonwealth Heads of Government Meeting released the *Commonwealth Cyber Declaration,* which commits to (1) a cyberspace that supports economic and social development and rights online, (2) building the foundations of an effective national cyber security response, and (3) promoting stability in cyberspace through international cooperation.

In 2019, the US and 27 other States issued the *Joint Statement in Advancing Responsible State Behaviour in Cyberspace,* which "call[s] on all states .. [to join in ensuring] greater accountability and stability in cyberspace." In February 2020, the International Committee of the Red Cross proposed a new norm that would prohibit States from knowingly conducting or supporting cyber operations against the health care sector.

There are also private processes in which experts from diverse backgrounds offer recommendations on cyber norms for States and other actors. Examples include the Bildt Commission and the Carnegie Endowment for International Peace's Cyber Policy Initiative. Relatedly, industry-focused efforts to identify norms vis-a-vis cybersecurity include *Cybersecurity Tech Accord*, initiated by Microsoft, and the *Charter of Trust*, led by Siemens. Both efforts have signed on to the *Paris Call*. The *Cybersecurity Tech Accord* contains four core principles for companies: (1) strong defense, (2) no offense, (3) capacity building, and (4) collective response. Similarly, the *Charter of Trust* contains three major commitments: (1) protect the data of individuals and companies, (2) prevent damage to people, companies, and infrastructures, and (3) create a reliable

foundation on which confidence in a networked, digital world can take root and grow.

Regional:

The European Commission's *Blueprint for coordinated response to major cyber-attacks* outlines the objectives and modes of cooperation between Member States and EU institutions in responding to such incidents and explains how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at the EU level.

The Commission also works with the European External Action Service and Member States on the implementation of a joint diplomatic response to malicious cyber activities. The cyber diplomacy toolbox, as it is known, includes diplomatic cooperation and dialogue, preventative measures against cyberattacks, and sanctions against those involved in cyberattacks threatening the EU.

In 2013, the Organization for Security and Cooperation in Europe (OSCE) adopted a set of 11 confidence-building measures relating to cybersecurity information sharing. In 2016, it added five additional measures to protect critical infrastructure and establish protected channels of communication. The OSCE has also established an ongoing working group for discussion relating to the implementation of the confidence-building measures identified by the UN GGE. Other regional organizations include the Association of Southeast Asian Nations (ASEAN) Regional Forum *Work Plan on Security and the Use of Information and Communication Technologies (ICTs)*, which has considered cybersecurity confidence building measures as well.

Additionally, in 2018, ASEAN members subscribed in-principle to the UN norms of responsible State behaviour and agreed to focus on regional capacity building to implement these norms. The Fourth ASEAN Ministerial Conference on Cybersecurity was also held in October 2019 in which the ASEAN Member States discussed key cybersecurity matters including the option of a cybersecurity coordination mechanism.

Other regional initiatives include the African Union *Declaration on Internet Governance*, which contains provisions on cooperation in cyber security. Additionally, in 2009, the Shanghai Cooperation Organization published its *Agreement on Cooperation in the Field of Ensuring the International Information Security*, which specified main areas of cooperation including countering threats of using ICTs for terrorism countering information crime, and exchanging expertise and training.

National:

Some States have issued specific statements regarding their position on the application of international law in cyberspace and State conduct in cyberspace.

In November 2011, the UK hosted the international London Conference on Cyberspace. Foreign Secretary William Hague characterised the conference as an

opportunity to discuss norms of acceptable behaviour in cyberspace and to explore mechanisms for giving such standards "real political and diplomatic weight." Further, in May 2018, UK Attorney General Jeremy Wright delivered a speech on the UK's position on applying international law to cyberspace. The Attorney General stressed the role of States in "be clear about how our international law obligations bind us," including in cyberspace. Three particular articles of the UN *Charter* are key to the UK's position: (1) the rule prohibiting interventions in the domestic affairs of States both under Article 2(7), (2) Article 2(4), which prohibits the threat or use of force against the territorial independence or political integrity of any State, and (3) the inherent right to take action in self-defence, as recognised in Article 51.

Additionally, in September 2019, the UK published its efforts to implement the 11 norms of responsible State behaviour that were part of the 2015 UN GGE report and endorsed by the UN General Assembly. It emphasized that international law applies in cyberspace and stressed four principles underpinning the UK's approach to cyber deterrence: (1) the UK will always seek to discover which State or non-State actor is behind any malign cyber activity, (2) the UK will respond, e.g., via public attribution, (3) the UK will aim to prosecute those who conduct cybercrime, and (4) with partners, the UK will consider further steps consistent with international law.

In 2015, German Ambassador Norbert Riedel, the Commissioner for International Cyber Policy at the Federal Foreign Office, made a statement advocating for greater security in cyberspace. In particular, Germany suggests three areas of engagement: (1) working towards a common understanding of responsible State behaviour in cyberspace, (2) promoting confidence and trust, and (3) undertaking efforts to increase cyber-resilience.

In 2016, Brian Egan, a Legal Adviser at the US Department of State, made a speech on the application of international law in cyberspace in which he articulated four norms which the US has identified and promoted: (1) a State should not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent of providing competitive advantages to its companies or commercial sectors, (2) a State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide service to the public, (3) a State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents, and (4) a State should cooperate, in a manner consistent with its domestic and international obligations, with requests for assistance from other States in investigating cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

More recently, in March 2020, Paul Ney Jr, General Counsel at the US Department of Defense, made a speech in which he "summarize[d] the domestic and international law considerations that inform the legal reviews that DoD lawyers conduct as part of the review and approval process for military cyber operations." Importantly, "[i]t continues to be the view of the United States that

existing international law applies to State conduct in cyberspace. Particularly relevant for military operations are the Charter of the United Nations, the law of State responsibility, and the law of war."

In July 2019, the Dutch Minister of Foreign Affairs wrote a letter to the President of the House of Representatives outlining the international legal order in cyberspace. Importantly, the Netherlands "aims to play a leading role in the application and strengthening of an international normative framework for the regulation of cyber operations between states" and "is also pressing for international agreements on voluntary, non-binding norms of behaviour by states and the development of a system of confidence-building measures." The Appendix to the letter outlines the Netherlands' interpretation of the application of existing international law in cyberspace.

In October 2019, the French Ministry of the Armies released a statement articulating France's view of how international law applies in cyberspace. Notably, "compliance with international law is a precondition for the emergence of an appropriate regulation of cyberspace." France's interpretation of the international law applicable to actions in cyberspace is based primarily on compliance with the conclusions arising from UN GGE negotiations since 2004.

Also in 2019, France issued a statement welcoming UN General Assembly Resolutions 73/27 and 73/66 on "[d]evelopments in the field of information and telecommunications in the context of international security" and "[a]dvancing responsible State behaviour in cyberspace in the context of international security" respectively.

At the 2019 CyCon Conference, Estonian President Kersti Kaljulaid reaffirmed the applicability of international law in cyberspace and observed that sovereignty entails not only rights, but also obligations. She emphasized that States are responsible in law for "internationally wrongful cyber operations… whether or not such acts are carried out by state organs or by non-state actors supported or controlled by the state." Further, "[i]f a cyber operation violates international law, this needs to be called out."

In December 2020, New Zealand's Ministry of Foreign Affairs and Trade issued a statement on the application of international law to State activity in cyberspace. New Zealand "supports an international rules-based system that promotes an open, secure, stable, accessible and peaceful online environment and encourages responsible state behaviour in cyberspace." Accordingly, "[i]nternational law applies online as it does offline" and includes the UN *Charter*, the law of State responsibility, international humanitarian law, and international human rights law.

Finally, Finland "sees international law as an essential framework for responsible State behaviour in cyberspace." Importantly, sovereignty is "fully applicable in cyberspace." A hostile interference by cyber means may also breach the customary prohibition of intervention in the internal affairs of another State. Further, "States may ... not knowingly allow their territory, or cyber infrastructure within a territory under their control, to be used [for] ... cyber

operations that produce serious adverse consequences for other States." The "normal rules of State responsibility [also continue to] apply in cyberspace."

B. Binding regulatory or legislative frameworks

International:

While the international community agrees that international law applies in cyberspace, application and interpretation has been riddled by debate. For example, the *Cyber Law Toolkit* considers a variety of scenarios in cyber space and how international law applies. In particular, one of the assessed scenarios is how international law applies in the context of a State purchasing and deploying an exploit for the purposes of surveillance. The analysis shows that this type of conduct in cyberspace may give rise to several violations of international law, such as provisions of the *International Covenant on Civil and Political Rights* and possibly the principle of sovereignty, among others.

Regional:

In December 2020, the European Commission launched a new *Cybersecurity Strategy*, which covers the security of essential services, building collective capacities to respond to major cyberattacks, and working with global partners to ensure international security and stability in cyberspace. The *Strategy* outlines a Joint Cyber Unit to ensure the most effective response to cyber threats using collective resources and expertise available to the EU and Member States. One of its aims is to "advance international norms and standards" that reflect EU values in cyberspace. The legislation under the *Strategy* is two-fold: (1) the *NIS2 Directive*, which builds upon the *NIS Directive* in forming the rules on the security of network and information systems; and (2) the *Cybersecurity Act* (in force since June 2019).

The African Union *Convention on Cyber Security and Personal Data Protection* was adopted in June 2014, but the most recent signature was in May 2020. The *Convention* addresses three main areas: (1) electronic transactions, (2) personal data protection, and (3) cyber security and cyber crime. However, the treaty will only enter into force 30 days after the 15th instrument of ratification or accession is deposited. Currently, only 8 Member States have deposited their instruments.

National:

Many States have issued strategies outlining their approach to international law in cyberspace. Some of these strategies are implemented by way of binding legislation.

The US was the first leading power to pick up on the UN GGE's concept of norms for State conduct in its *International Strategy for Cyberspace*, issued by the Obama Administration in 2011. The policy document recognises the dangers that unchecked State cyber action could present, and affirms that the US will "engage the international community in frank and urgent dialogue, to build consensus around principles of responsible state behaviour."

Additionally, in General Counsel Ney's aforementioned speech, in the US, "domestic legal authority for the DoD to conduct cyber operations is included in the broader authorities of the President and the Secretary of Defense to conduct military operations in defense of the nation." The *Computer Fraud and Abuse Act* creates corresponding exceptions for lawfully authorized activities of law enforcement and US intelligence agencies, including military cyber operations.

Estonia is one of the few States to have released a third *National Cyber Security Strategy (2019-2022)*. Notable throughout all three strategies is a focus on the global nature of threats in cyberspace and the need for international, multilateral action. Estonia's position is that States "have the right to attribute cyber operations both individually or collectively according to international law" and "to respond to malicious cyber operations, including using diplomatic measures, countermeasures, and, if necessary, their inherent right of self-defence."

Also in 2015, France developed a *National Digital Security Strategy* to support the digital transition of French society. It emphasizes a strong response to malicious cyber activities and aims to make cyber security a competitive advantage for French companies. In December 2017, France's *International Digital Strategy* supplemented the *National Strategy* in setting out the principles and objectives that France is pursuing internationally in cyberspace. Based on three key pillars of governance, the economy, and security, the *International Strategy* focuses on (1) promoting an open, diverse and trustworthy digital space at a global level, (2) fostering a European model, striking a balance between economic growth, basic rights and security, and (3) strengthening the influence, attractiveness, security and trade stances of France and French actors in cyberspace.

In its 2017 *International Cyber Engagement Strategy,* Australia recognises that existing international law such as the UN *Charter* and associated norms provide the framework for responsible State behaviour in cyberspace. The 2019 *International Law Supplement* further elaborates Australia's position on applicable international law as expressed in the *Strategy*.

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.

This question is answered in two parts. First, it considers non-binding normative frameworks that may impact the provision of security products and services in cyberspace. Second, it considers binding regulatory and legislative frameworks with that same purpose (or related to it). A number of the identified frameworks below may not be specifically designed for addressing the "provision of security products and services in cyber space," yet may impact that activity and thus are worth mentioning. Once again, this response does not intend to be exhaustive, but presents an initial indication of the variety of binding and non-binding frameworks that could be applicable to the regulation of security products and services in cyberspace.

A. Non-binding, 'norm-setting' frameworks

International:

In addition to some of the frameworks mentioned in Question 6, the following also impact the provision of security products and services in cyber space.

The *Wassenaar Arrangement* sets out a non-binding and voluntary scheme that addresses the licensing and export of listed dual-use technologies. While voluntary, States are responsible for implementing the export rules set out in the *Wassenaar Arrangement* through domestic law.

The *United Nations Guiding Principles on Business and Human Rights* set out a framework under which business actors must respect human rights. These overarching norms apply to actors engaged in the provision of security products and services in cyberspace. The UN has also provided a forum for the discussion of how the provision of cyber-capabilities impacts international human rights through, for example, the UN Human Rights Council's Special Procedures and the work of the Special Rapporteurs (see, for example, David Kaye's 2019 report on the surveillance industry).

Additionally, the UN Office on Drugs and Crime's Global Programme on Cybercrime is mandated, as per General Assembly Resolution 65/230 and Commission on Crime Prevention and Criminal Justice Resolutions 22/7 and 22/8, to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance. To this end, the Global Programme is designed to respond flexibly to identified needs in developing countries by supporting Member States to prevent and combat cybercrime in a holistic manner. The main aims of the Global Programme in 2017 were (1) increased efficiency and effectiveness in the investigation, prosecution and adjudication of cybercrime, within a strong human-rights framework, (2) efficient and effective long-term whole-of-government response to cybercrime, and (3) strengthened national and international communication between government, law enforcement and the private sector with increased public knowledge of cybercrime risks.

The Organization for Economic Cooperation and Development (OECD)'s *Guidelines for Multinational Enterprise* serve to integrate responsible business conduct into business practices, including human rights practices. While the Guidelines are non-binding, the National Contact Points (NCP) are established by governments to promote the Guidelines and handle complaints. In 2015, the UK's OECD NCP found that Gamma Group breached human rights by selling spyware to Bahrain.

The Global Network Initiative (GNI) provides "direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment" of freedom of expression and privacy globally. In short, the GNI is intended to facilitate private actors' compliance with international human rights law, with a specific focus on ICT companies.

The BRICS countries, at their Fortaleza Summit in 2017, issued a *Declaration* which noted Member States' intent to explore cooperation on cybercrime, and the establishment of a group of national security advisors to explore practical proposals for cooperation and coordination of their activities in international fora.

Also in 2017, Russia proposed a *Draft United Nations Convention on Cooperation in Combating Cybercrime*. The *Draft Convention* has three purposes: (1) to promote and strengthen measures aimed at effectively preventing and combating crimes and other unlawful acts in the field of ICT, (2) to prevent actions directed against the confidentiality, integrity and availability of ICT, and the misuse of ICT, by criminalizing such acts, and by providing powers sufficient for effectively combating such offences and other unlawful acts, and (3) to improve the efficiency of international cooperation and to develop such cooperation, including in the area of personnel training and the provision of technical assistance for preventing and combating ICT crimes.

Regional:

In 2012, the Southern African Development Community (SADC) issued its *Model Law on Computer Crime and Cybercrime*. The *Model Law* serves as a guideline for States in the SADC to develop substantive and procedural cybercrime laws. The States that have and/or create cybercrime laws can utilize the SADC *Protocol on Mutual Legal Assistance in Criminal Matters* and the SADC *Protocol on Extradition* to facilitate cooperation and coordination in international cybercrime investigations.

From 2013 to 2016, the EU, in partnership with the Council of Europe, funded the Global Action Against Cybercrime (GLACY) project, which aimed to prevent and fight organized crime based on the *Budapest Convention on Cybercrime*. The GLACY + project explicitly focuses on capacity building in 12 priority countries in Africa, Asia-Pacific, Latin America, and the Caribbean.

National:

The US Department of State has issued a *Guidance on Implementing the 'UN Guiding Principles' for Transactions Linked to Foreign Governments End-Users for Products or Services with Surveillance Capabilities*. Under the human rights due diligence and risk mitigation considerations, the DOS suggests to "review, including through in-house or outside counsel, whether the foreign government enduser's laws, regulations, and policies that implicate products and services with surveillance capabilities are consistent with the UDHR." This includes looking out for red flags such as "[f]oreign government engagement in malicious cyber activities or arbitrary or unlawful data collection against individuals or dissident groups."

Other governments may have issued domestic guidelines intended to encourage the private sector to comply with the obligation to respect human rights abroad, without making this a legally-enforceable requirement. For example, the Canadian government has set forward a framework for responsible business conduct,

although it does not specifically address the activities of Canadian companies selling surveillance capabilities abroad as in the American guidelines.

B. Binding regulatory or legislative frameworks

International:

The *International Covenant on Civil and Political Rights* (*ICCPR*) imposes positive obligations on State actors to regulate the activities of private actors that impact international human rights in certain circumstances. As the Human Rights Committee (HRC) stated in *General Comment No. 31*, State Parties' duty to ensure Covenant rights will only be fully discharged if individuals are protected by the State not just against violation of the *ICCPR* by its agents, but "also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities."

The *Budapest Convention on Cybercrime* is a binding international instrument and serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation. This instrument is relevant because it requires State parties to implement domestic crimes against access to the whole or part of any computer system without right (Art. 2), interception without right by technical means of non-public transmissions of computer data (Art. 3), and the production, sale, procurement for use, import, or distribution of or otherwise making available a device that is designed to commit those types of offences and where the requisite intent is present (Art. 6), among other requirements.

Regional:

The Commonwealth of Independent States' *Agreement on Cooperation in Combating Offences Related to Computer Information* in 2001 calls on States to adopt national laws to implement the *Agreement*'s provisions and to harmonize national cybercrime laws.

The Arab League's 2010 *Arab Convention on Combating Information Technology Offences* aims to strengthen cooperation between States to enable them to defend against and protect their property, people, and interests from cybercrime. Further, the Shanghai Cooperation Organization's 2010 *Agreement on Cooperation in the Field of International Information Security* extends beyond cybercrime and cybersecurity to include information security of Member States as well as national control over systems and content.

The Economic Community of West African States' (ECOWAS) 2011 *Directive on Fighting Cybercrime* requires Member States to criminalize cybercrime in national law and facilitate mutual legal assistance, cooperation, and extradition in cybercrime and cybersecurity-related matters. ECOWAS also has a C*onvention on Mutual Assistance in Criminal Matters* and a *Convention on Extradition* to facilitate cooperation in cybercrime investigations and to extradite cybercriminals.

The African Union's 2012 *Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa* similarly promotes the provision and maintenance of human, financial, and technical resources needed to facilitate cybercrime investigations.

Regulation (EC) No 428/2009 addresses the regulation of dual-use technologies and implements the *Wassenaar Arrangement* for member states of the European Union. This framework is of particular interest because it was recently agreed that it would be amended to include greater transparency requirements and give greater consideration for human rights impacts associated with the export of cyber-capabilities.

National:

As noted above, national jurisdictions may be members of the *Wassenaar Arrangement* and thus should have implemented domestic legislation that regulates the export of goods listed in the *Arrangement*, which would include intrusion software and IP network surveillance systems or equipment, as defined by the *Arrangement*. Failure to comply with export requirements domestically may lead to certain penalties, including fines and imprisonment. For example, under the *Export and Import Permits Act* in Canada, contravention of the Act is punishable by summary conviction and a fine not exceeding $250,000 or to imprisonment of a term under 12 months or an indictable offence and liable to a fine set by the court or to imprisonment under 10 years, or both (s. 19(1)).

Some jurisdictions have specifically implemented national legislation that imposes certain due diligence requirements on business actors with respect to human rights. One commonly-cited example is *La loi sur le devoir de la vigilance* in France. While not specific to the provision of cyber-capabilities by private actors located in France, it may apply to such activities and serve as a part of a more comprehensive regulatory framework.

There are other legal avenues—once again, not necessarily specific to the provision of offensive cyber security products—that could impact the business of developing and selling cyber-capabilities. For example, national legislation may render illegal the development or deployment of spyware and malware in certain contexts (such as the *Criminal Code* in Canada or the *Computer Fraud and Abuse Act* in the US). However, there are numerous obstacles to criminal prosecutions for these offences, such as challenges in attribution, extraterritoriality, and foreign state immunity. In addition to criminal law, researchers have also highlighted the following potential avenues in domestic law for regulating the provision of offensive security products and services, such as spyware, in cyberspace: tort law, the development of statutory civil liability regimes, and drawing on consumer protection laws.

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.**

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 a number of different legal avenues for pursuing accountability for such activities. For the most part, whether these avenues will be successful in furthering accountability remains to be seen. The litigation identified below has also been summarized on the Citizen Lab's website.

Several actions have been pursued against NSO Group, an Israeli spyware company. In 2017, Mexico instituted a federal investigation against the spyware company. In 2018, various targets of NSO Group spyware initiated lawsuits in Cyprus and Israel, and Omar Abdulazziz, another target, started legal action in Israel. In 2019, Ghanem Almasarir, another target, also started legal action in the UK. Additionally, WhatsApp and Facebook sued NSO Group in 2019 in federal court in the US. This litigation, which was instituted in the Northern District of California, is ongoing, with an appeal by NSO Group to the Ninth Circuit currently pending. Further, 2019 also marked Amnesty International's support for an attempt in Israeli court to appeal the Israeli Ministry of Defence's decision not to revoke NSO Group's export license. The petition was rejected in 2020.

Gamma Group has also been the subject of legal action. In 2013, Privacy International and other civil society organizations filed a complaint against Gamma Group with the UK's NCP, which found that the company was in breach of the OECD Guidelines. In 2014, Privacy International and the European Center for Constitutional Rights called for an investigation into Gamma Group in Germany, but it was dismissed. Finally, in 2018, Bahraini targets of Gamma Group spyware instituted a legal action in the UK.

Further efforts to hold those committing abuses in cyber space accountable include the Electronic Frontier Foundation's (EFF) attempt, starting in 2014, to pursue legal action against the government of Ethiopia in federal court in the US, although lost due to a finding that Ethiopia was immune under the *Foreign Sovereign Immunities Act*. More recently, a criminal complaint was filed in Germany by a number of civil society actors against FinFisher in 2019. On October 14, 2020, DW reported that "German Customs Investigation Bureau (ZKA) searched 15 residential and business premises in Germany and abroad last week with connections to the Munich-based surveillance software firm FinFisher."

It remains to be seen how these various legal actions will play out and what the impact will be on accountability in cyberspace, if any. Both the WhatsApp litigation and EFF's failed action against the government of Ethiopia suggest that issues of foreign sovereign immunity remain a live issue and may continue to complicate—least in the case of defendants who are State actors—these types of litigation.

Further, it is worth underlining that, and setting aside the investigation in Mexico, there remains a stark absence of national investigations (whether formal or informal) into the deployment of NSO Group. For example, when permanent

resident Omar Abdulaziz was targeted with spyware in Canada, the police reportedly began to investigate the situation, but nothing further was reported.

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.

Please see the answer to Question 5.

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.

The Citizen Lab's work is focused on harms that arise under international human rights law and we have focused our responses in relation to that scope of research.