**Submission to the Working Group on Mercenaries**

**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.*

Clients / beneficiaries of cyber capabilities and operations include

1. Nation states who want to achieve their strategic goals through cyber operations but do not want the operations to be attributable to them, or they want plausible deniability, or they lack in-house cyber capabilities
2. Cyber criminals who want to use cyber capabilities to carry out crimes on a major scale (of volume or of complexity) but lack in house capabilities

Unlike traditional forms of conflict, improvements in cyber-capabilities can benefit all users and actors – both benign and malicious – in cyberspace. Technology is inherently neutral; it is the action of users that assign the level of malignancy of its use. Improvement in cyber-capabilities can lead to better cybersecurity for users, but the same improvement can also mean that malicious actors are better equipped to conduct hostile cyber operations against networks.

1. 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?

(a) Developing cyber capabilities – cyber mercenaries can purchase zero-day exploits and vulnerabilities in criminal markets (e.g., on the dark web); it would be unwise for nation states to do this directly

(b) Maintaining cyber capabilities – cyber mercenaries can keep malware updated with new features and security patches, provide technical support for deployment of malware, and provide command and control servers, using staff and resources which are not owned by a nation state

(c) Selling cyber capabilities – cyber mercenaries already provide turnkey solutions such as RAAS (ransomware as a service) and user-friendly dashboards for deploying malware.

(d) Delivering cyber capabilities – I attended a briefing by a PMSC who said his company, based in Germany and the US, sold their malware “to democratic nations only”

Both state and non-state actors can develop, maintain, sell, deliver, and carry out cyber espionage activity by themselves or through PMSCs. These actors can potentially carry out more damaging activity such as the deletion of data, destruction of networks, or distributed denial-of-service (DDoS) attacks.

1. 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 reasons why both state and non-state actors use mercenaries are similar. First, the lack of capacity within the organisation, but the capacity is needed immediately. Training up cyber capacity takes time, skills, aptitude, and resources.

Second, the use of mercenaries can provide deniability to the client.

Unfortunately, it is difficult to define who mercenaries are in cyberspace. The lines between individual hackers, vendors, contractors, penetration testers, and state-sponsored threat actors are increasingly being blurred. There is little to differentiate in terms of military and civilian use of malicious tools in cyberspace, but the differences can be found in the motives of non-state and state actors.

Both states and non-state actors can use mercenaries to further their objectives. For states, these may be to monitor and conduct espionage activity on adversary networks over a longer period of time. The activity is typically not profit driven, but driven by motivations of its own security and power considerations. Non-state actors typically have no such concerns, being motivated by its own relative competitiveness and profit.

1. 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?

There are services and products available both as a legitimate service and in an illicit setting. Legitimate services include penetration testing, red-teaming, threat monitoring companies. Illegal services available on the Dark Web include hacking-as-a-service, data broking, cybercrime as a service.

Tools developed for cybersecurity can be misused or hijacked for nefarious purposes. Hackers can steal the tools that legitimate penetration testing teams use to potentially compromise other systems. An example is how FireEye had its penetration testing tools stolen by actors that are suspected to be state-sponsored in December 2020.

Non-exhaustive list of services that mercenaries can carry out for clients, and intended purpose

* Ransomware – obstruction and interference
* Denial of service / botnets – obstruction and interference
* Website defacement – signalling or information operations
* Credential theft – used to infiltrate an adversary’s network, either for espionage or sabotage or both
* Zero-days / vulnerabilities – same as above
1. 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”?

New technologies tend to prioritise speed to market rather than security, which may bring about security risks. The key however is the willingness of private sector companies to provide software patches to update these risks as and when they are known. If left unpatched these vulnerabilities in these new technologies may be exploited by malicious actors.

Example: New technologies like Internet of Things (IOT) devices are often connected to the Internet as well as the users’ networks, with inadequate cybersecurity protections e.g., CCTVs with simple or no default passwords, or with no means to upgrade security. This makes them an easy entry point into users’ networks.

As mentioned earlier, there are many different actors in cyberspace and it is difficult to pinpoint who a mercenary is in cyberspace. However, in my opinion, the individuals (or group) that are most immediately involved in a cyber operation and those who have commanded the cyber operation should be considered as the people “directly participating in cyber operations.

**Regulatory frameworks and their application**

1. 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).

Domestically, the Singapore is guided by the [Singapore Cybersecurity Strategy](file:///C%3A/Users/iseegtan/Downloads/SingaporeCybersecurityStrategy.pdf) published in October 2016. The strategy consists of four main pillars: Strengthen the resilience of Critical Information Infrastructures (CIIs); make cyberspace safer; develop a vibrant cybersecurity ecosystem; and, forge strong international partnerships.

The strategy is supported by two key pieces of legislation: [the 2018 Cybersecurity Act](https://sso.agc.gov.sg/Acts-Supp/9-2018/) and [Computer Misuse Act (Cap 50A)](https://sso.agc.gov.sg/Act/CMA1993). The Cybersecurity Act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to: first, strengthen the protection of Critical Information Infrastructure (CII) against cyber-attacks; second, authorise the Cyber Security Agency of Singapore to prevent and respond to cybersecurity threats and incidents; third, establish a framework for sharing cybersecurity information; and, fourth, establish a light-touch licensing framework for cybersecurity service providers. The Computer Misuse Act establishes the criminal framework for for securing computer material against unauthorised access or modification and for matters related.

Internationally, Singapore has been a strong advocate for the norms of responsible state behaviour recommended by the 2015 United Nations Group of Governmental Experts both regionally and internationally. ASEAN, the regional organisation, prides itself as the first regional organisation that agreed in principle to be guided by the 2015 UNGGE norms as part of a rules-based international order.

The political declaration by ASEAN leaders to accept the 11 norms proposed by the UNGGE was made in both the ASEAN Leaders’ Statement on Cyber Security at the 32nd ASEAN summit in April 2018 and the 2018 ASEAN Ministerial Conference on Cybersecurity (AMCC). Apart from the declaration, the 32nd ASEAN Summit further elicited statements from leaders recognising that norms and the rule of law is needed for cyberspace, and as a basis for advancing economic growth in the region. The 2018 AMCC called for a more formalised mechanism for ASEAN cyber coordination.

At the 2020 AMCC, ASEAN member states reiterated their collective commitment to take practical steps to enhance the cybersecurity of the region, in particular, the urgent need to protect national and cross-border Critical Information Infrastructure that serve as the backbone for regional communications trade, transportation, and logistics links. At the same time, Ministers and heads of delegations have also agreed to develop a long-term regional cybersecurity action plan to implement the norms of responsible state behaviour in cyberspace, taking into account the national priorities and cyber capacities of individual ASEAN member states.

In other words, ASEAN is moving from the political commitment to broad principles toward the finding of practical ways forward to operationalise the 2015 UNGGE norms. In part, this move towards practical adoption of the 2015 UNGGE norms is reflected in Singapore’s support of the recently submitted Food for Thought paper to the OEWG and the UNGGE to create a Programme of Action for Advancing Responsible State Behaviour in Cyberspace.

1. 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.

The Cyber Security Agency of Singapore (CSA) has launched the Cybersecurity Labelling Scheme (CLS) for consumer smart devices, as part of efforts to improve Internet of Things (IoT) security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.

The CLS is the first of its kind in the Asia-Pacific region. Under the scheme, smart devices will be rated according to their levels of cybersecurity provisions. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions.

The CLS also aims to help manufacturers stand out from their competitors and be incentivised to develop more secure products. Currently, consumer smart devices are often designed to optimise functionality and cost. They also have a short time-to-market cycle, where there is less scope for cybersecurity to be incorporated into product design from the beginning.

The CLS was first introduced to cover Wi-Fi routers and smart home hubs. These products were prioritised because of their wider usage, as well as the impact that a compromise of the products could have on users. It has since been extended to include all categories of consumer IoT devices, such as IP cameras, smart door locks, smart lights and smart printers.

1. 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.

Spying (or espionage) activity on the Singapore government is covered under Section 3 of the Official Secrets Act. Acts of espionage covered under the act include:

* **Approaching, inspecting or entering a “prohibited place”.**Under [section 2(1) of the OSA](https://sso.agc.gov.sg/Act/OSA1935#pr2-), most “prohibited places” are related to Singapore’s armed forces. They could be things (e.g. telephones, ships) or locations (e.g. camps, offices) belonging to or occupied by Singapore’s armed forces, or a place used for storage of war munitions. Any areas declared and published in the *Gazette* as being, or specified in any notice under any law to be, “prohibited places” under section 2(1) of the OSA, are also included.
* **Making photographs, drawings, plans, or notes** that might be, or are intended to be, useful to a foreign Power or enemy.
* **Obtaining, collecting, recording, or communicating confidential information** that might be, or is intended to be, useful to a foreign Power or enemy.

The accused person must have also carried out these acts with a purpose prejudicial to Singapore’s safety and interests in order to be guilty of spying.

Persons found guilty of spying can be fined up to $20,000 and jailed up to 14 years.

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

1. 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.*

The question has three layers that needs to be unpacked. The first layer is where a state is competing with another state and uses the data for espionage purposes; the second layer is where a state targets a non-state actor overseas to disrupt their actions in their own territory; and the third layer is where the state directs its data collection efforts to stifle, stymie, and sabotage its own citizens.

All three scenarios have the same risk, but may have very different outcomes. The concentration of data in the hands of untrusted actors puts individuals at risk of becoming a victim of cybercrime and potentially lose their right to privacy should the data be used in a coercive manner. These can be done by the state apparatus itself or be contracted out to PMSCs to conduct such action.

For state on state action, the compromise on individual liberty and privacy is relatively lower than that of the other two more targeted scenarios. For the latter two actions, the state is willing to conduct surveillance of the groups or individuals because the state has put limits on the freedom of association and expression. This level varies among states, and while some have very high thresholds e.g. terrorist groups, some states look unfavourably on anything that does not fit their agenda.

1. 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.

International Humanitarian Law is a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare. International humanitarian law in particular covers two areas: first, the protection of those who are not part of conflict; and second, restrictions on the means and the methods of warfare.

The development of cyber-capabilities can potentially cause widespread disruption to essential services. For example, the hack on the Ukrainian power grid in early 2016 was unrestricted and was not restricted to combatants in the contested regions in Eastern Ukraine and Crimea. While there was no loss of life in the incident, there was also no attempt made to control the disruption. The attack has however not been attributed to a state actor or a PMSC, but shows the potential effects a cyber operation can bring to the civilian population and not those who are involved in the armed conflict in Crimea or Eastern Ukraine.

Other examples of uncontrolled episodes of global disruption by cybered means include the DDoS on the Mirai Domain Name Servers (DNS) by IoT devices and the WannaCry ransomware attack.

Written by Eugene E.G.Tan, Associate Research Fellow

Submitted by Benjamin Ang, Senior Fellow, Cyber Homeland Defence and Dy Head, Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Email: isbang@ntu.edu.sg