**Questionnaire on the provision of military and security products and services in cyber space by cyber mercenaries and related actors and its human rights impact**

Please note that we have provided responses to only some of the questions, where we have input to provide.

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

***These can include for instance 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.***

**2. What is the role of actors, operating alone 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?**

**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.***

From our perspective in countering cyber threats, through the operation of CSIRT-CY, the two main motivational factors and strategic intentions of “cyber mercenaries” are financial gain and intelligence gathering for political leverage.

**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?**

AI technologies are currently evolving, and they increasingly become adopted by the industry. In terms of AI related malicious cyber services, AI technologies could be used to analyse massive datasets in a small amount of time and conduct accurate analyses without significant effort. They could also be used to automate procedures by helping computers and robots to learn how to solve complicated problems, communicate with humans or imitate human behaviour. Attackers could use AI technologies to collect and analyse information about their targets and to automate attacks. Chatbots could also be used to perform social engineering or phishing attacks, without significant effort. In conflict settings, AI could be used in a strategic level to collect information, run simulations and analyse the behaviour of a hostile army, but also to conduct unarmed military operations, eventually replacing trained soldiers or pilots with AI-based machines.

We have observed the use of spyware/malware, in a non-conflict setting, against the country’s critical infrastructure for the purpose of intelligence gathering.

**5. What role do new technologies play in causing harm remotely in the context of cyber operations, and what are the risks involved?**

As new technologies are implemented, possible attack vectors and the attack surface continues to increase. This eventually leads to widening the cyber threat landscape. Therefore, critical infrastructures are more likely to suffer from cybersecurity vulnerabilities if they don’t take the appropriate security measures, as they are increasingly more dependent on digital technologies and internet provision. At the same time, attackers can take advantage of new technologies to develop advanced attacking tools and methods. It is considered very likely that the critical information infrastructures of a country will form the first (and main) targets of attack from coordinated cyber campaigns from hostile actors.

**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).**

The EU NIS Directive requires that Member States ensure that operators of essential services (critical information infrastructures) are identified, and that they take appropriate and proportionate technical and organisational security measures to protect the confidentiality, integrity, availability and authenticity of the essential services that they provide. At the national level, these measures are codified in Decision 389/2020, with key provisions related to (among others) formal risk assessments, business continuity planning and a number of specific horizontal security measures to be applied based on the identified risks. Also, based on Decision 218/2019, all operators of essential services, critical information infrastructure providers and digital service providers, are required to share with the Digital Security Authority any incident that has a serious impact to the continuity of the services they provide.

Additional frameworks include the OSCE Confidence Building Measures (CBMs).

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

N/A

**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 Budapest Convention on Cybercrime, along with the various national laws that accompany its ratification in a number of countries, include relevant provisions for investigation and accountability for criminal activity in cyberspace.

**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 right 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.***

Development and use of cyber-capabilities, operations and services by actors operating alone or through PMSCs can cause and contribute to human rights abuses and violations in non-conflict settings in several ways. There will be a breach of Article 8 of the European Convention of Human Rights, which is the right to privacy, with the surveillance of individuals as they interfere with privacy and regardless if users are aware of it or not, it is still considered an intrusion. There may be an interference with Article 10, which is the right to freedom of expression, if the attacks on digital/physical infrastructures and data limit individuals from having the opportunity to freely express their opinion or their opinion might have been deleted as a consequence of these operations. Article 10 grants individuals to receive and impart information and ideas without interference by public authority and other, if there are attacks on digital/physical infrastructure and data then this right will be violated.

Additionally, the use of AI technologies and personality analysis techniques could also lead to violations of human rights and interceptions of personal data. Recent studies have shown that even public data posted in social media such as Twitter, could be used to predict the personality and personal beliefs of a person with remarkable accuracy.

For example, AI could be used to predict the political and religious affiliations and the favourite colours of citizens, as well as the words that they subconsciously relate to positive feeling and experiences. Similarly, the less favourite colours and the words that cause more negative feelings to citizens could also be predicted based on their posts and experiences. This data could be used during a pre-election period in order to personalize advertisements of political candidates. A candidate that collaborates with the data provider may create personalized advertisements, using the favourite colour of each citizen as background and the words that each citizen has strongly associated with previous positive experiences as text. The candidate can also ask the data provider to sabotage her opponents, by using colours and words in their advertisements, which subconsciously cause negative feelings.

This strategy may not only be used to manipulate election trends but also to subconsciously impose any kind of message to citizens. This may cause a violation of the citizens’ freedom since their personality traits and experiences are used, to subconsciously manipulate their opinions.

Moreover, modern AI and NLP (Natural Language Processing) technologies enabled the development of fake news detection systems, which are extensively used in popular social media platforms and on the internet in general. Undoubtedly, fake news detection tools are valuable since they allow platforms to restrict the spread of false allegations and improve the quality of news for citizens. Nevertheless, these technologies should always be used with caution, without censoring the opinions of journalists, opposition leaders and other groups or individuals with underlying expediencies.

**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 use of cyber capabilities, operations and services can lead to the violation of the right to privacy. Through the use of satellite and different tracking systems the PMSCs could track locations of individuals and surveil them which goes against civilian’s right to privacy. By tracking individuals and finding them at times of armed conflict, can lead to complications if the armed forces do not distinguish between soldiers and civilian population. This may lead to civilian casualties, capturing of civilians or. This goes against the right to life and the prohibition of torture and also takes away the civilians right to liberty as they will be captured and detained unlawfully.

Additionally, nowadays there is the possibility of conducting unarmed military operations, using relatively cheap but technologically advanced weapons such as military drones. Therefore, technology gaps could lead to unfair armed conflicts between technologically developed and developing countries. Military drones could be used to violate citizens' privacy and commit war crimes against civilian populations, which are difficult to detect and record.