**Questionnaire on the position of military and security products and services in cyber space by cyber mercenaries and related actors and its human rights impact – Contribution of the Greek Government**

We believe that state actors or non-state actors may contract cyber mercenaries to take over cyber espionage operations on their behalf, seek valuable information, steal intellectual property or defend infrastructure, particularly in cases of:

a. Clients not having sufficient capability to conduct such operations or lack the specialized tools.

b. Clients wishing to avoid immediate interference with their targets by leasing security and cyber operation services and misleading their targets when they try to estimate operations source.

c. Clients wanting to avoid costs of maintaining fully capable operational elements, offensive or defensive and thus resort to outsourcing solutions.

Recruiting "cyber mercenaries" by state or non-state actors aims at disassociating cyber activity from true interested parties and leading to erroneous hypothesis about adversaries' motivation and assumed identity. “Cyber mercenaries” would operate under the tolerance and strict control of their recruiters, since this can be considered the less risky approach, particularly when mutual trust, secrecy and discretion cannot be positively achieved.

According to international humanitarian law, mercenaries do not have the right to receive asylum for their actions; The six criteria of the Protocol of 1977 must be met, in order for an individual to be characterized as mercenary. Following these criteria, it is difficult to be able to qualify an individual or a group of individuals as “cyber-mercenaries”, and for this reason their identity as well as their motivation in case of cyber war activities may be difficult to clarify. When groups operate under the tolerance or encouragement of a state, it is impossible to distinguish their actions and characterize these groups as mercenaries or cybercriminals.

It goes without saying that the existing international humanitarian and human rights legal framework should apply to the illegal activities carried out by cyber-mercenaries, since a series of fundamental freedoms and human rights are being violated during these operations. However, and given the ever-evolving and high tech nature of these attacks, new international legal instruments are needed which will lay emphasis on the cyber nature of crimes committed by cyber-mercenaries.

Developing and illegally using cyber capabilities, operations and services may amount to violation of the right to privacy, right to property, right to freedom of expression, to mention just a few of them. In the framework of both armed conflicts and in non-conflict situations, attacks against critical infrastructure are harmful for public safety, health and population well-being.