IMPROVING TRANSPARENCY
INTERNATIONAL LAW AND STATE CYBER OPERATIONS.
QUESTIONNAIRE

1. Has your Government previously issued an official paper, speech, or similar statement summarizing how it understands international law applies to cyber operations? Please provide copies or links to any such statements.

2. Do existing fields of international law (including the prohibition on the use of force, the right of self-defense, international humanitarian law, and human rights) apply to cyberspace? Are there areas where the novelty of cyberspace excludes the application of a particular set of international legal rights or obligations?

3. Can a cyber operation by itself constitute a use of force? Can it constitute an armed attack that triggers a right of self-defense under Article 51 of the UN Charter? Can a cyber operation qualify as a use of force or armed attack without causing the violent effects that have been used to mark such thresholds in past kinetic conflicts?

4. Outside of armed conflicts, when would a State be responsible for the cyber operations of a non-State actor? What levels of control or involvement must a State have with respect to the non-State actor's operations to trigger the international legal responsibility of that State?

5. Are the standards of State responsibility the same or different in the context of an armed conflict as that term is defined in Articles 2 and 3 common to the 1949 Geneva Conventions?

6. Under international humanitarian law, can a cyber operation qualify as an "attack" for the rules governing the conduct of hostilities if it does not cause death, injury or direct physical harm to the targeted computer system or the infrastructure it supports? Could a cyber operation that produces only a loss of functionality, for example, qualify as an attack? If so, in which cases?

7. Is a cyber operation that only targets data governed by the international humanitarian law obligation to direct attacks only against military objectives and not against civilian objects?

8. Is sovereignty a discrete rule of international law that prohibits States from engaging in specific cyber operations? If so, does that prohibition cover cyber operations that fall below the use of force threshold and which do not otherwise violate the duty of non-intervention?

9. Does due diligence qualify as a rule of international law that States must follow in exercising sovereignty over the information and communication technologies in their territory or under the control of their nationals?

10. Are there other rules of international law that your government believes are important to highlight in assessing the regulation of cyber operations by States or actors for which a State is internationally responsible?