Roundtable 2: Accountability for Cyber War Crimes

Co-Authored by: Dinesh Napal & Jackson Colling

Moderated by Arthur Traldi, Senior Fellow for the Tech, Law & Security Program, the second roundtable discussion centered on holding Russians accountable for war crimes committed in the cyber realm. The panel featured Liina Lumiste from NATO CCDCOE, Adam Hickey of Mayer Brown, and Lindsay Freeman from the Berkely Human Rights Center. The panel mainly touched on the ICC's announcement of its investigating cyber war crimes, charges that may result from its investigation, how the ICC may investigate and prosecute cyber war crimes, and how the panelists would advise states considering investigating cyber actions.

ICC's Investigating Cyber War Crimes

The ICC recently announced that it is including alleged cyber war crimes in its investigations into Russian war crimes in Ukraine. Freeman touched on her team's work compiling a report on Russian cyber war crimes which she provided to the ICC. The panel discussed how the Rome Statute provides the basis of ICC action and procedure and how the issue of bringing charges of cyber war crimes is not completely settled. This issue largely stems from ambiguity of the term "attack" in the cyber context. Relatedly, the panel discussed the applicability of Art. 22 of the Rome Statute which favors the defendant in cases where the crime is not fully defined or is ambiguous. The panel noted that if the crime of aggression is charged, cyber dimensions will be considered even though cyber-attacks are not currently considered constitutive of crimes of aggression. Although cyber incidents can fall below the threshold of an attack, they can still serve as evidence of war crimes, enhancing accountability.

Process of Investigating Cyber War Crimes

Investigators must start with the 'breadcrumbs' on the victims' network – IP addresses, types of malwares etc. – then follow them, hoping they cross friendly nations' networks. Ultimately these breadcrumbs should clearly point to a foreign state, whether it is a building, email address, or a clear individual – whatever can clearly point to the state or individual responsible. Difficulties for the ICC include relying on unfriendly states to cooperate in the investigation if the investigation crosses into that state's network, lack of subpoena power and search warrant power, and difficulty of arrest. Alternatively, the panel discussed pros to the ICC's process of investigating cyber war crimes which include the ICC's criminal standard being more lenient than that of the U.S., the ICC not being bound by the same evidentiary rules as the U.S., being able to rely on hearsay and educated testimony from third parties such as tech companies. The ICC is making steady progress in building its capacity to investigate cyber war crimes and has relied on states providing voluntary assistance and states conducting their own investigations.

Advising a state considering investigating cyber actions and investigatory red lines

In the U.S., unauthorized access to a computer connected to the internet is a crime – bringing charges against an individual is a moral judgment to an extent and it would be hollowed slightly if a state was engaged in the same practices it is seeking to investigate and charge. States should offer their own perspectives on what the law should be and what the lines are. Domestic legislators may consider ICC's desire to investigate cyber-crimes as an impetus to undertake their own drafting of guidelines and regulations for investigating cyber-crimes. The sooner states define how international law applies to such crimes, the more likely customary international law will reflect those states' aims.