Cyber-Warfare and International Rule of Law

Aneeqa Safdar

Cyberspace is now an officially declared domain of warfare and states are methodically indulging in this new form of war to achieve their political objectives. States are conducting cyber-attacks on high-value targets of enemy state/s comprising critical infrastructure or on state secrets. The significance of such attacks has alarmed even modern and technologically advanced states such as the US, China, Russia and the UK. While cyber-crimes have caused significant losses to states and international businesses as high as, $1 trillion in 2020, interstate cyber aggression has become more sophisticated, practiced and innovative.

In an age of hybrid warfare, the practice of cyber-warfare, i.e., to weaken, disrupt or destroy the adversary state through cyber means is also gaining traction. Due to the increasing number of cyber-attacks by government-linked entities, states are establishing red lines to ensure cyber defense. This can intensify the risk of cyber escalations and retaliation taking place outside of the cyber domain. Cyber powers, like the US and Israel, have already set a precedent in this case wherein airstrikes were undertaken against Hamas and ISIS in retaliation to cyber-attacks.

The first-ever Biden-Putin summit held in June 2021 at Geneva effectually highlighted this emerging threat of cyber-security. Given ongoing US-Russia cyber rivalry, the US President in the historical (cyber) summit categorically established red lines in cyberspace. He handed down a list of 16 critical infrastructure sectors considered vital to US' national security and said they must be off-limits to any kind of attack, including cyber-attacks. He told his Russian counterpart that if Moscow did not refrain from attacking these sectors through cyber means, the US would retaliate. The threat of cyber-attacks leading to consequences-driven escalation and retaliation between cyber powers and technologically advanced states is very real.

According to President Biden, responsible countries need to take action against criminals who conduct illegal activities from their territory. The same holds true for nation states. Unfortunately, while all states expect responsible behavior in cyberspace, they have failed to embrace joint responsibility of formulating a legal framework for cybersecurity, including cyber-warfare. Numerous countries are building their cyber warfare capabilities by establishing cyber commands/ cyber warfare divisions, but there is little in terms of an international agreement or legal regime to regulate cyber conflicts.

Currently, the only treaty that governs cyberspace is the Budapest Convention on Cybercrime. It was opened for ratification in 2001 and serves as a guideline for developing comprehensive national legislation against cybercrime, and as a framework for international cooperation between the signatories. However, no such legal instrument is available for cyberwarfare. The Tallinn Manual is one effort by a group of experts in the field to establish the applicability of international law on cyber warfare. However, it is an academic work with no legal standing.

Nation states are still struggling with how to respond in case of a massive cyber-attack that they may perceive as a national security crisis. The existing scholarship broadly analyses cyber operations in the context of *jus ad bellum*, the international law governing the right to resort to force; and *jus in bello*, the international law regulating the conduct of armed conflicts. There is broad consensus among experts that if the consequences of a cyber-attack resembles that of a conventional one, the act may justify use of force by evoking the right to self-defense. Hence, some states, like the US, advocate keeping unilateral measures open, like pre-emption through offensive cyber operations, or retaliation and counter-attacks through non-cyber means. However, others like Russia and China advocate developing a common understanding on the application of international law and norms in cyber space through the United Nations, with key focus on attribution and substantiation. Besides, it is also accepted that the law of armed conflict or *jus in bello* applies to cyber operations with all its central principles, discrimination, proportionality and precaution.

Responsible behavior during any cyber conflict is an obligation on all states. With cyber-attacks intensifying in number and impact, states should endeavor to put their differences aside, and start a concrete strategic dialogue to establish international rule of law in cyberspace and build a 'peaceful and secure cyberspace.'

The writer is a researcher at the Centre for Aerospace & Security Studies (CASS) Islamabad, Pakistan. She can be reached at cass.thinkers@gmail.com. ***The article was first published in South Asia Journal.***