Source : www.thehindu.com Date : 2021-04-07

REDEFINING COMBATANTS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Representational image. | Photo Credit: Reuters

A report in *The New York Times* on the October 2020 breakdown of the Mumbai power distribution system points a finger at Chinese cyber hackers. While the truth may remain hidden, the discussion points to a macro issue. When, and under what conditions, would a non-kinetic strike, say a cyberattack, be considered an attack on the state? And under international rules of self-defence, what response would be considered legal? Would only a cyber counter-attack be justifiable or a kinetic response also be acceptable? Would a pre-emptive strike be kosher? These and other questions are knocking at our door, even as the definition of combat and combatants undergoes fast mutation.

The universally accepted Lieber Code of 1863 defines a combatant. It says, “So soon as a man is armed by a sovereign and takes the soldier’s oath of fidelity, he is a belligerent...”; all others are non-combatants. An organised group of “belligerents” constitutes a regular armed force of a state. The 1899 Hague Convention brings in further clarity of what constitutes a regular force. First, the force should be commanded by a person responsible for his subordinates. Second, it must have a distinctive emblem recognisable at a distance. Third, it must carry arms openly. And last, it must conduct operations in accordance with laws and customs of war.

Those who conducted the (yet unproven) Mumbai ‘cyberattack’ or the 2007 attack on Estonia’s banking system did not meet any of the four conditions of being called combatants, but still wreaked havoc. A combatant, thus, needs to be redefined due to three reasons. First, a cyber ‘army’ need not be uniformed and may consist of civilians. After the cyberattack on Estonia, the government set up a voluntary Cyber Defence Unit whose members devote their free time towards rehearsing actions in case of a cyberattack. A rogue nation could well turn these non-uniformed people into cyber ‘warriors’. Second, cyber ‘warriors’ do not carry arms openly. Their arms are malicious software which is invisible. And finally, the source of the attack could be a lone software nerd who does not have a leader and is up to dirty tricks for money, blackmail or simply some fun. None of these meet the requirements of The Hague Convention but the actions of these non-combatants fall squarely in the realm of national security.

This raises two very basic inquiries that need deliberation. First, would the nation employing civilians in computer network attacks not be in violation of the laws of war? And second, if these people are considered as combatants, would the target country have the right to respond in self-defence? A response would be reactive, after the attacker has conducted his operation; hence, as a right of self-defence, would an act of pre-emption (through kinetic means and/or through cyber) be in order? This argument may appear far-fetched now but needs to be examined as India seems to have a new view on the concept of the right to self-defence.

In a February 24, 2021 UN Arria Formula meeting on ‘Upholding the collective security system of the UN Charter’, the Indian statement says, “...a State would be compelled to undertake a pre-emptive strike when it is confronted by an imminent armed attack from a non-state actor operating in a third state.” It adds that “this state of affairs exonerates the affected state from the duty to respect, vis-a-vis the aggressor, the general obligation to refrain from the use of force.” In a perceptive analysis of the statement, in *Opinio Juris*, Srinivas Burra, an Assistant Professor, opines that in a clear departure from established practices, “India... expressly contextualises its position on the question of the right of self-defence against the acts of non-state actors in international law.” Though used with reference to an “armed attack”, the implications of the

statement, when viewed vis-à-vis cyberattacks done by faceless persons who are non-combatants as per international law, open up an avenue that requires careful examination; cyberattacks may not kill directly but the downstream effects can cause great destruction.

International actions against hackers have been generally limited to sanctioning of foreign nationals by target nations. In 2014, for the first time, a nation (the U.S.) initiated criminal actions against foreign nationals (five Chinese operatives of Unit 61398 of the People's Liberation Army) for computer hacking and economic espionage. The question is, how long before this escalates to covert and/or overt kinetic retaliation. India seems to have made its intentions clear at the UN meet, but this is a game that two can play; if not regulated globally, it could lead to a wild-west situation, which the international community should best avoid by resolute action.

Air Vice Marshal Manmohan Bahadur (Retd) is Additional Director General, Centre for Air Power Studies. Views are personal

To reassure Indian Muslims, the PM needs to state that the govt. will not conduct an exercise like NRC

END