The Missing Option: India, Pakistan and Armed Conflict in Cyberspace

Arun Mohan Sukumar

Likely to be among the options weighed by India's National Security Advisor (NSA) in response to Pakistan's alleged complicity in the Uri terrorist attack of September 18, 2016 is coercive cyber action. In theory, a cyber attack could be swift, minimise the risks of causalities, offer plausible deniability and could likely inflict serious damage on Pakistan's economic infrastructure. In reality, however, the picture is more complicated. Any assessment by New Delhi of this option should account for the following:

1. India's offensive cyber capabilities
2. The defensibility of such action under international law
3. The desirability of coercive cyber measures against Pakistan's networks

Capacity

Coercive cyber measures, like any military option, should be the culmination of extensive assessments by India of its intelligence and technical capabilities. Take as two possible targets, the Hub Power Station in Karachi and the Karachi (now Pakistan) Stock Exchange. The Hubco plant is among the largest thermal power-generating projects in Pakistan, capable of "provid[ing] 10+% of [the] country's electricity demand".[1] The KSE (now Pakistan Stock Exchange) is its premium financial trading platform. To mount a cyber attack against either installation, military planners should be supported by intelligence inputs from the ground, providing valuable information about:

i) personnel who may (wittingly or otherwise) introduce a vulnerability into the facilities, and;
ii) the physical location of computers/servers which form part of the network to be infected

Both require an assessment of the installation that goes well beyond aerial or satellite reconnaissance. Without strengthening India's intelligence networks in Pakistan, therefore, a serious attack on its digital networks will be difficult to conceive or execute.

Then there is the matter of the 'cyber weapon' itself. Not many government agencies in India, including the National Technical Research Organisation, have the in-house expertise required to build and exploit vulnerabilities that can manipulate or destroy the integrity of electronic data. India's armed forces fare marginally better, having deployed 'red teams' that do penetration testing to protect their own networks. But the military too may not be in a position to create a sophisticated cyber-weapon designed for the specific purpose of bringing down, say, Pakistan's electricity grid.

It is worth remembering that Stuxnet was the product of an inter-agency effort involving the United States and Israel. Stuxnet owes its origins in no small part to the United States' well-developed bug bounty programme, which invites hackers to identify vulnerabilities in operating systems and communications platforms. Having a bug bounty programme (which in the US is tightly regulated by the White House) contributes to a strategic culture that can co-opt technical expertise in India into the national security narrative. There is no reason why New Delhi should shy away from a programme for its defence and intelligence agencies, given the talented pool of computer scientists in the country. In fact, internet giants like Facebook and Google routinely rely on Indian citizens to identify fixes and flaws in their products through their own bug bounty schemes. Today, Indian agencies rely on private expertise on an ad hoc basis, or buy zero-day vulnerabilities from the 'dark net'.[2]

An evaluation of coercive cyber measures against Pakistan by the NSA – the last step in the chain of decision-making before it is presented as a credible option before the Prime Minister – can be done only if he is able to lean on multi-agency coordination that will supply both human intelligence and technical expertise.

The tail, however, should not wag the dog. Conceiving and creating a cyber weapon will likely involve months, but this process should be guided by a political strategy as to its specific objective, likely impact, and potential fallout. Unlike conventional weapons or weapons of mass destruction, it is impossible to create an 'arsenal' of cyber weapons that can be deployed at will.

The first step for India's defence planners, then, would be to absorb coercive cyber measures as a central pillar of its Pakistan policy. This would involve:

1. An identification of targets, and their potential vulnerabilities
2. Assessing the deterrence value of a declared 'cyber doctrine'
3. Enhancing capabilities, in ways referred to above

Defensibility

Cyber attacks are difficult to attribute to governments, as they often originate from non-state actors and sometimes, through servers based in a third country. Links between non-state actors and the governments of the territory in which they are based can at best be established using circumstantial evidence. In India's case, military planners need to walk a fine line between denying any involvement in a cyber attack, and signalling to Islamabad that its so-called 'asymmetric' actions will be met by similar responses. Were New Delhi to be implicated in a coercive cyber manoeuvre against Pakistan, Indian diplomats should be prepared to defend the legality of its conduct in multilateral venues like the United Nations.

In essence, India's legal defence against a cyber attack on Pakistan would be to claim an act of reprisal. Given the UN's visible lack of enthusiasm in enacting a Comprehensive Convention on International Terrorism, India will have to rely on traditional principles of state responsibility to hold Pakistan responsible for the actions of groups like the Jaish-e-Mohammed and Lashkar-e-Taiba. Without wading into the vast and rich jurisprudence on the subject, it is sufficient to say that even if India should produce evidence linking terrorist groups to the Pakistani government, it may be difficult to satisfy purely legal requirements.

Article 8 of the draft articles on Responsibility of States for Intentionally Wrongful Acts[3] states:

"The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct." (emphasis added)

The 'direction/control' test is a high standard to which India or the international community may never hold Pakistan. The first hurdle for India is to meet this threshold, absent a 'smoking gun'.

The second (and related) difficulty is to establish that attacks by terrorists are not only attributable to Pakistan but that they also violate a prohibition on the "use of force" enshrined in Article 2(4) of the UN Charter. If that seems incredulous, there's more. For India to claim "self-defence" in international law under Article 51 of the Charter, attacks such as the one in Uri should constitute an "armed attack" by the Pakistani state, a legal threshold that is generally accepted to be higher than the plain "use of force".[4]

In the aftermath of the 9/11 attacks, the United States invoked its "clear right of self defence"[5] under Article 51 to bomb Afghanistan -- a decision that polarised international opinion on the legality of its claim. In that instance, however, the US had the overwhelming support of the UN Security Council, which subsequently legitimised the intervention through the establishment of the International Security Assistance Force in 2001. In India's case, no such support from UNSC members will be forthcoming. In any case, New Delhi has no appetite for an armed intervention of the scale seen in Afghanistan.

Simply put, it is improbable that India can convincingly make the case for "self-defence" through a cyber attack against Pakistan. Reprisals on the other hand involve the use of force, but need not be reported[6] to the UN Security Council, and constitute an act akin to self-defence for attacks of a lesser degree.

Amidst this legalese, it is important not to miss the larger, political picture. For India to offer a convincing defence of retaliatory cyber measures against Pakistan requires coordinated planning between the Ministry of External Affairs (MEA) and the National Security Council Secretariat. Irrespective of what New Delhi may term its actions, the cyber attack should be a proportionate response to Pakistan's transgressions. The MEA and its lawyers should advise the NSA on this count and thoroughly review the cyber weapon's impact on civilian populations. To help mould the evolving body of international law in its favour, India must also step up engagement with international platforms such as the UN Group of Governmental Experts on ICT security and the Tallinn Manual consultations on the law of armed conflict in cyberspace.

Desirability

Coercive cyber measures offer some advantages to a policy planner where conventional military options appear limited, as in India's case against Pakistan. Nevertheless, several concerns persist, which should prompt New Delhi to examine the desirability of this option.

1. Such measures will have the same impact as the use of conventional weapons in turning the world's attention to the Kashmir conflict. Were India to target critical infrastructure in Pakistan, New Delhi can be certain the rhetoric across the border would escalate. In its aftermath, India may find it difficult to manage heightened international concerns, especially as the risks of cyber warfare are relatively unknown.

2. Coercive measures against Pakistan may give away India's presence in digital networks that have been penetrated for the primary purpose of espionage and surveillance. For instance, were New Delhi to target Pakistan's telecommunications infrastructure, it will reveal vulnerabilities in such networks that enabled the attack, prompting Pakistan to fix them. In the short and medium term, India may lose some valuable channels of intelligence gathering which must be weighed against the impact of the cyber weapon.

3. It would be reasonable to expect an escalation of low-intensity cyber attacks from China immediately following the incident. The creation of a cyber-weapon, or malicious tools to damage the integrity of Pakistan's digital networks, needs extensive planning but it is a project that involves a select group of parties. India's preparedness to defend its own networks, on the other hand, is a national conversation that needs to be continually had with organisations from the public and private sectors. As things stand, India has not fully assessed the resilience of its critical sectors and may not be able to limit the damage from a retaliatory attack. Deepening of the China-Pakistan strategic relationship, leading to eventualities like the co-development of cyber weapons, can further limit the political and military options available to India in the event of conflict.

4. The United States is unlikely to offer India material support in planning or executing the attack, or shield New Delhi from political criticism in its aftermath. At the UN Security Council, however, both Russia and the US can be expected — for reasons purely driven by self-interest — to veto any proposal from China condemning the use of cyber weapons. India has not reached out to possible interlocutors like Israel to begin collaboration on the creation of sophisticated cyber instruments.

5. Whether or not the attack on Pakistan's digital networks forces its military to revisit the country's sponsorship of terrorist groups, the overall stability of cyberspace in South Asia will be seriously called into question. Denial of service attacks, large-scale hacks, and disruption of internet services could become the norm, if the Pakistani state pursues a strategy of continuous, low-intensity engagement against New Delhi. A cyber attack is only as effective as the lure of the digital economy, and India stands to lose big in this game of chicken.

The lesson here, perhaps, is that a declared doctrine on the use of cyber weapons, pursuant to the building of capacities, can signal deterrence to Pakistan more effectively than the use of such instruments in isolation by India. It will likely take years to bring such a strategy to fruition: after the May 1998 tests, it took India nearly 5 years to articulate a nuclear weapons doctrine. The rapid advancement of digital technologies suggests that a cyber doctrine, if articulated, should be flexible, and open to review and possible restatements. Pakistan's nuclear weapons capability is often cited as a dead-end for India's conventional superiority, but cyberspace opens a new theatre of conflict. But it is critical this process begins now, failing which India could be drawn towards an inevitable confrontation in digital spaces with Pakistan without a clear assessment of its goals or outcomes.