15

ORF SPECIAL REPORT

JULY 2016

The Case for Cyber and Cyber-Physical Weapons: India's Grand Strategy and Diplomatic Goals

ARUN MOHAN SUKUMAR

Observer Research Foundation (ORF) is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by by providing informed and productive inputs, in-depth research and stimulating discussions.

To know more about ORF scan this code

The Case for Cyber and Cyber-Physical Weapons: India's Grand Strategy and Diplomatic Goals

ARUN MOHAN SUKUMAR

This briefing document articulates a grand strategy for India to pursue the development of cyber and cyber-physical weapons, with a view to manage conflicts and the future balance of power in Asia.

Definitions

Cyber Weapon

A cyber weapon is any code-based instrument that relies exclusively on digital networks, capable either of damaging their integrity or penetrating them to gather sensitive information that would be advantageous in a kinetic attack.

Cyber-physical Weapon

Cyber-physical weapons are physical platforms, partly or fully autonomous, that use code, computer algorithms or digital networks as a central constitutive element. This term covers a wide range of intelligent technologies, from humanoid robots to unmanned aerial vehicles capable of autonomous engagement in theatres of war.

BACKGROUND

A number of countries today possess offensive cyber capabilities, notably the United States, Israel, Russia, China, North Korea, Syria and Iran. Their range and sophistication vary widely: no two cyber weapons are likely to be the same, as they are conceived and deployed for a specific project or purpose. Using or maintaining an arsenal of such weapons, however, does not necessarily signal the presence of a cyber doctrine. For instance, while the United States has numerous official directives to guide its cyber-offensive operations, it is unclear whether China or Syria, which possess limited capabilities in this area, has comparable strategies. In particular, no Asian country has declared either its cyber capabilities or doctrines to manage their cyber and cyber-physical weapons. Given this lack of clarity, Indian military and policy planners should assess whether geo-political tensions in Asia will spill over into cyberspace, or if the inter-connected character of digital networks raises the economic stakes too high for a cyber conflict.

Using three possible scenarios, this briefing note illustrates the heightened risk of cyber-instability today in Asia.

SCENARIOS

SCENARIO 1

The Permanent Court of Arbitration has declared that China has lost its dispute against the Philippines over its claims on the South China Sea (which the other party calls 'West Philippine Sea'). Immediately after the announcement, media outlets in the Philippines suffer sustained cyber attacks. As a consequence of these sophisticated attacks – perpetrated by non-state actors – TV stations are forced to shut down for a week, preventing them from broadcasting news of the arbitration.

SCENARIO 2

After what is perceived as a successful Indian effort to block a multi-million-dollar sale of defense equipment by the United States to Pakistan, hackers based in Rawalpindi target the Bombay Stock Exchange. The cyber attack, which manipulates trading information, prompts BSE administrators to close down the exchange for 24 hours, but not before billions of dollars are liquidated.

SCENARIO 3

North Korea deploys a cyber weapon that targets the radars and tracking systems of oil tankers passing through the Strait of Malacca and destined for South Korea. The ensuing chaos stalls maritime traffic in the Strait and forces South Korea – among the biggest importers of oil in the world – to dive into its limited strategic reserves.

GRAND STRATEGY

All three scenarios illustrate cyber attacks on sensitive information infrastructure, but they do not necessarily constitute thresholds to retaliate by means of a kinetic attack. In the second scenario, for instance, India may well launch air strikes in Pakistan in response to the attack on the Bombay Stock Exchange, but New Delhi would struggle to:

a) attribute the attacks to the Pakistan government; and

b) justify the action as an "armed attack" under Article 51 of the UN Charter, necessitating self-defense.

Several countries have indicated to the United Nations through their legal advisers that a cyber attack could invite kinetic retaliation, but confusion persists on the exact threshold that can trigger a "necessary and proportional" response. In the absence of clear international norms or rules of engagement, states are likely to exploit their cyber capabilities for both low and high-intensity conflicts. This situation may lead to twin outcomes in Asia. Smaller Asian countries will puruse the development of cyber weapons with a view to offset disadvantages in conventional warfare. Meanwhile, many powers in the region, including India, may find their military options foreclosed due to a lack of enhanced cyber capabilities. The tendency for a cyber conflict to "spill" into the kinetic realm may therefore be higher, calling into question the stability of the region as a whole.

The normative framework for cyber-physical weapons is even more clouded, as states are divided on how best to regulate

India's ability to develop and purchase cyber and cyber-physical weapons will be reliant on export control regimes already in place to regulate dual-use technologies.

them. The applicability of international humanitarian law is currently contested, as are the question of "meaningful human control" of such systems, and the designation of certain autonomous platforms as Lethal Autonomous Weapons Systems (LAWS). The *interregnum* is likely to see a rapid scaling up of LAWS capabilities to augment conventional platforms. Governments may also be inclined to deploy them in battle more frequently, given the reduced risk of casualties. As a result, the cyber-physical weapons race could lead to the dramatic deterioration of regional stability in Asia.

India's grand strategy on cyber and cyber-physical weapons must pursue three objectives.

i) Facilitate the indigenous development and where necessary, the purchase of such weapons.

ii) Articulate a national security doctrine to guide their use.

iii) Help create a non-proliferation regime that limits the deployment of cyber and cyber-physical weapons in Asia.

These three goals are not pursued in isolation.

India's ability to develop and purchase cyber and cyber-physical weapons will be reliant on export control regimes already in place to regulate dual-use technologies. Indian negotiators should engage their foreign counterparts to ensure the broad restrictions imposed by the Wassenaar

India should enter cyber non-proliferation regimes as a manager, and not as their subject, while disaggregating any link with the global nuclear order.

Arrangement do not limit the co-development or purchase of cyber platforms. This is best done through bilateral diplomacy with the United States, Russia and the European Union. New Delhi also has good reasons to steer clear of any sanctions arrangement that not only targets emerging technologies but also individuals and organisations within India who could develop them. A licensing regime will severely constrain Indian actors and institutions who are currently able to purchase and co-develop cyber capabilities. Indian diplomacy should thus desist from making any policy commitments on non-proliferation or export controls until its cyber and cyber-physical weapons are at an advanced stage of development.

Second, there is merit in articulating a cyber doctrine, both for the purposes of deterrence or clarifying India's rules of engagement during a conflict. Developing a cyber weapons doctrine is complicated by a project-specific character, but it can highlight the following important concerns:

1) Under what circumstances will India deploy cyber weapons?

2) Does India maintain a first-use or no-first use policy on cyber and cyber-physical weapons?

3) Would India use kinetic means to respond to a cyber attack on its critical information infrastructure?

4) In the event of an all-out conflict, will India target the critical information infrastructure of an adversary?

Finally, India must work towards creating a new legal and political architecture around cyber and cyber-physical weapons. Were such an order to emerge, India should enter it as a manager and not exclusively as a subject, disaggregating any links with the extant nuclear non-proliferation regime. The objective of regime creation can be pursued at an advanced stage of capabilities, with a view to limit their actual deployment in conflict. New Delhi should help ensure that cyber and cyber-physical weapons are not accessible to actors who pose a strategic threat in Asia. Indian diplomacy must effectively communicate the high costs of low-intensity cyber-skirmishes in the region, while maintaining that it will not hesitate to deploy such weapons where necessary.

About the Author

Arun Mohan Sukumar heads the Cyber Initiative at the Observer Research Foundation, New Delhi.

Observer Research Foundation **(ORF)** is a public policy think-tank that aims to influence formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, academics and business leaders.

Observer Research Foundation
20, Rouse Avenue Institutional Area,
New Delhi — 110002
INDIA

Phone: +91 011 43520020
Fax: +91 011 43520003
Email: contactus@orfonline.org

DESIGNED BY **SHANTANU SALGAONKAR**