CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 24/2023

23 April 2023

Learning from a Distance: Cyber Lessons for India from Russia-Ukraine War

Khyati Singh

Research Associate, Centre for Air Power Studies

Keywords: Cyber Security, Russia-Ukraine War, Cyber Attack, Atmanirbhar Bharat

Source: imgurl:https://portswigger.net/cms/images/01/86/450e-article-190101-india-cybercrime-body-text.jpg - Bing

Conventional wisdom argues that 'it is best to learn from others' mistakes,' and this is the underlying operating mechanism of international arena. States are constantly engaging with each other on different parameters based entirely on their security calculations. These calculations are a result of various variables, including perception, hard power capabilities, and how a state is positioned in the international order. These calculations and their results keep changing purely because states continue to thrive for the betterment, and the world order never remains the same. While on this transition journey, states often take note of similar events, as episodes in international politics are recurring where only the actors change. This paves the way for strategies, diplomatic turns, alliances, competition, and rivalry.

The states so far have excelled in their understanding of conventional warfare, owing to the fact that the world has seen far too many wars on all levels, from domestic to international. And despite knowing the odds, states refuse to let go of war as an instrument. The latest entry in this list of conflicts is the one between Russia and Ukraine. This war, in particular, has gone into the zone of 'hybrid' warfare and has left ample lessons on the floor to collect. The war has an explicit side where tanks, missiles, aircraft, troops, and artillery are being used. However, a shadow war that runs parallel often falls short of attention. A reason for this can be the 'out of sight' domain of these operations, as they occur mainly in the unconventional spaces of cyber, information, intelligence, espionage, etc. They have changed the security balance indicators as they allow even small powers to operate beyond their conventional strengths.[1]

The first thing that evolved was the involvement of state-sponsored, non-state actors. It is not just meant for Ukraine-Russia, but other actors like North Korea, Iran, and China might further their actions in this 'fog of war.'[2] These situations bring down the rate of attribution and make it difficult to assess them. Moreover, the Russian actors have managed to break into the 'air-gapped' networks of several US companies.[3] Therefore, advancing the nature of attacks. Hence, India needs to develop a mechanism where it can reduce the effects of the 'fog of war' if a situation like this arrives, especially when it has China as an adversary.

In addition, the network of hacktivists is active in various domains, crossing several red lines, and there have been cyclic episodes of ransomware incidents. Another tool that has surfaced around this time is the ability of intelligence services to interfere in the elections. Their method of 'hack and dump'[4] information to unleash economic and political unrest has been a repeated practice.[5] Therefore, in democratic states like India, where public opinion is the backbone of state structure, safeguarding the social fabric becomes crucial. For instance, France and the US were worried about Russia's attempt to interfere in their elections to counter their support for Ukraine.

The cyber activities are not just operational on land; they have also reached the realm of space. Government and commercial satellites and assets in space are essential because they incorporate ever-evolving technologies for broadband services, global positioning systems (GPS), imaging, and communications.[6] Russia has been maintaining a range of anti-satellite (ASAT) weapons that are meant to disrupt the US and other allies' space capabilities. In addition, Russia is testing, fielding, and developing various destructive and non-destructive counter-space weapons that include cyberspace capabilities, jamming, directed energy weapons, ground-based ASAT capabilities, and on-orbit capabilities. This has been a particular lesson for all the states alike, especially when it comes to linking cyber with space.[7] Some states are still working to build primary-level offensive capabilities, while cyber as an offensive tool has breached all possible security layers. Hence, it becomes important for states to consider these aspects and develop counter-capabilities against them. A technology pool can be a possible way out for countries that are not advanced in their cyber capabilities. While the West has been pulling its resources together, India needs to chip in and make security alliances on these fronts.

There were attacks on the US communications satellite KA-SAT, which impacted the coverage of the war in several European countries, including Germany and France. Furthermore, Europe's windmill turbines, which produced nearly 11 gigawatts of energy, were disrupted. This affected the country's energy supply and flagged the issue of critical infrastructure being increasingly pulled into conventional warfare.[8] This leaves states with an important lesson about how best to safeguard the lines of critical infrastructure and, in case of their rupture, what can be the minimum possible time to fix it. Countries like China are trying to address this issue by deploying artificial intelligence (AI). AI helps bring down the time of revamping such casualties drastically. It also strengthens the overall security architecture at multiple levels. At present, India is using AI in its defence sector at a marginal level. This includes surveillance and reconnaissance capabilities by deploying unmanned aerial vehicles (UAVs) and drones that are equipped with AI-powered sensors and cameras. These drones can conduct intelligent analysis of the images and data captured during their operation, helping the defence forces to identify threats, monitor remote locations, and gather intelligence. In addition, AI-enabled autonomous weapons that are being developed, such as unmanned ground vehicles (UGVs), drones, and combat robots, can conduct military operations autonomously with minimum human interference, training, and simulation. AI-powered simulation tools can create realistic training environments that closely mimic real-life scenarios, helping the forces prepare for a range of situations. Although these developments are going in the right direction, their pace is relatively slow.

Countries are increasingly incorporating their private sector into the larger security framework by working with them on technological lines. For instance, in its guidance for the Office of the Director of National Intelligence's Science and Technology for 2022 to 2026, the US has brought out the need to remove barriers and connect programme managers with private industries and technology developers.[9] This would help it maintain an edge in the technological domain. With its schemes like '*Aatmanirbhar Bharat*' or 'Make in India,' India tried to provide a push for such practices, but the realisation of these goals is far from near. India still relies on imports for essential products and resources such as crude oil, coal, electronic components, and machinery.

India's domestic manufacturing sector suffers from inadequate infrastructure, such as power, transport, and connectivity, which can increase production costs and delay the delivery of goods. Additionally, the country faces a shortage of skilled labourers and engineers, which can limit the quality and innovation of indigenous goods. Lastly, the channels of communication and operations are extremely bureaucratic in nature. This demotivates the private sector from stepping in. The government needs to ease these processes and bring down hurdles that hinder smooth collaboration between the private and public sectors, especially in the defence sector.

The following are recommendations that the state can work upon in order to improve its cyber profile. Time is a luxury that the state cannot afford during a cyber-attack, India should get rid of long processes in rulemaking and decision-making in case of a cyber breach. This action should also involve sharing expedited information with stakeholders from the various government branches along with the private sector.

The critical infrastructure needs to be 'cyber-proof' along with training and maintaining cyber resources, capabilities, and a workforce, and consider signing a Memorandum of Understanding (MoU) with states for feasible sharing of information. The critical infrastructure that is privately owned is brought into the fold when devising policies and actions for firms. A common error that often happens is that too many agencies are involved in a single issue. The approach largely is 'one-size-fits-all,' and a policy is carved. This leaves out the scope of expertise that is required in each domain. Hence, this issue needs to be rectified.

India has still not fully tapped into the potential of its private sector to nourish a sound public-private partnership, which might include better research and development (R&D), cyber exercises, and better defence. The government should roll out plans to conduct 'cyber storm' exercises along with preparing resilience and remedies for cyber-related situations. Countries like the US and China are also including several exercises that can help them fix critical infrastructure in case of a

cyberattack, especially on the power grid. They have also included firms like Microsoft to detect viruses and recover accordingly. India needs to put more resources and thoughts into these lines and bridge this gap between the private and public sectors.

In terms of cooperation, India and the US set up the United States-India Cyber Dialogue in 2015, which aims to promote cooperation on cybersecurity and cybercrime issues. Both countries have also signed a cybersecurity agreement to enhance information sharing and capacity building; an MoU with Japan on cybersecurity cooperation aims to jointly address the issues of cyber threats, capacity building, and exchange of information. Another MoU has been signed with the European Union on cooperation in the field of cybersecurity, which focuses on enhancing cooperation on incident management, public-private partnerships, and research and development. In addition, India also has a cybersecurity agreement in place with Israel to promote cooperation in cyberspace, exchange information on cyber threats and best practices, and strengthen capacity building, along with a joint declaration with ASEAN on cooperation in cybersecurity, which aims to promote dialogue, capacity building, and cooperation in addressing cybercrime and other cyber threats. Albeit this is a step in the right direction, it can expand and evolve manifolds by including joint cyber defence exercises, technology sharing, and R&D.

India should invest in the operational technology (OT) and cybersecurity of military and commercial platforms. The threats to nation-states are growing, and they are intertwined with OT platforms.[10] Energy production, water and waste management, airlines, pipelines, freight trails, etc., all heavily rely on the OT platform, along with the defence weapons system. They would go through a multitude of challenges in the wake of electronic warfare and cyberattacks. For instance, China entered the US defence industrial base through cyber espionage to collect data on US capabilities. This put the US at a disadvantage.[11] Hence, the government should look out for funding and implement measures to tackle OT cyber-attacks.

India has not fully tapped into the potential of open-source intelligence (OSINT). If India manages to scale the use of OSINT, it will help build better capabilities. The state must review and expedite its use. In addition, the state should conduct periodic interagency reviews of all threat actors, capabilities, actions, and policies. Finally, all the stakeholders should be involved in bringing a resilient system. The possibilities in cyberspace remain endless; wisdom is in tapping them before the enemy does.

Notes:

[1] Hal Brands, "Paradoxes of the Gray Zone," *Foreign Policy Research Institute*, February 5, 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone/. Accessed on April 7, 2023.

[2]Ciaran Martin, "Cyber Realism in a Time of War," *Lawfare Blog*, March 2, 2022, https://www.lawfareblog.com/cyber-realism-time-war. Accessed on April 7, 2023.

[3] Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," *The Wall Street Journal*, July 23, 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110. Accessed on April 7, 2023.

[4] Jean-Baptiste Jeangène Vilmer, The "Macron Leaks" Operation: A Post-Mortem, *The Atlantic Council and L'Institut de Recherche Stratégique de l'École Militaire*, June 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf. Accessed on April 7, 2023.

[5] Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," *Wired*, February 27, 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/. Accessed on April 7, 2023.

[6] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community 2022*, February2022, pp. 12–13, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf. Accessed on April 7, 2023.

[7] Morgan Meaker, "High Above Ukraine, Satellites Get Embroiled in the War," *Wired*, March 4, 2022, https://www.wired.com/story/ukraine-russia-satellites/. Accessed on April 8, 2023.

[8] Joseph Henry, "Europe Cyberattack Results to 'Massive' Internet Outage: About 5,800 Wind Turbines Went Offline," Tech Times, March 5, 2022, https://www.techtimes.com/articles/272624/20220305/europe-cyberattack-results-massive-internet-outage-5-800-wind-turbines.htm. Accessed on April 8, 2023.

[9] Dustin Carmack and Michael Ellis, "For Cybersecurity, the Best Defense Is a Good Offense," *Heritage Foundation Backgrounder No. 3670*, November 10, 2021, https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense. Accessed on April 8, 2023.

[10] James DiPane, "Cybersecurity: Policymakers Need a Consistent Means to Assess Capabilities," *Heritage Foundation Issue Brief*, August 25, 2021, https://www.heritage.org/defense/report/cybersecurity-policymakers-need-consistent-means-assess-capabilities. Accessed on April 8, 2023.

[11] Luis Martinez et al., "Major U.S. Weapons Compromised By Chinese Hackers, Report Warns," *ABC News,* May 28, 2013, https://abcnews.go.com/Blotter/major-us-weapons-compromised-chinese-hackers-report-warns/story?id=19271995. Accessed on April 9, 2023.