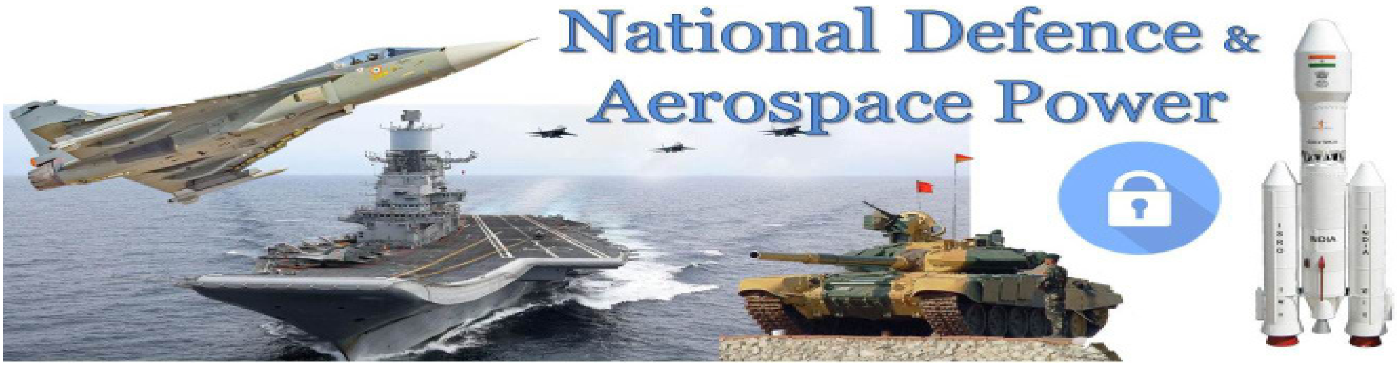
Centre for Air Power Studies



Centre for Air Power Studies ISSUE BRIEF

27/23

20 December 2023

CONFLICT, CYBER-ATTACK, AND CRITICAL INFORMATION INFRASTRUCTURE: TRACING TRENDS AND THE LESSONS FOR INDIA

Abhishek Sharma

Research Associate, Centre for Air Power Studies

The world is witnessing the increasing application of hybrid warfare, be it in the case of the Russia-Ukraine or Israel-Hamas conflict. Although Hybrid warfare occurs in all domains, one domain that has attracted less attention in its application is—cyberspace. In cyberspace, particularly Critical Information Infrastructure (CII), has been the most vulnerable to destructive and disruptive attacks. The objective of attacking CII is to disrupt, disable, disturb, harm, and cripple systems that play an essential role in the state's everyday work. Today, CII forms the foundations of a state's functioning and plays a fundamental role in its economic growth and security. It broadly includes infrastructure systems related to water, transportation, healthcare, energy grids, dams, and financial and communications sectors. States attack these civilian infrastructures as a tactic to develop psychological distress among the population to create direct and indirect pressure on their government and, at the same time, break the infrastructure backbone that runs a country. Following the recent conflicts in cyberspace, three trends have affected CII, providing lessons that India can learn.

> **The objective of attacking CII is to disrupt, disable, disturb, harm, and cripple systems that play an essential role in the state's everyday work. It broadly includes infrastructure systems related to water, transportation, healthcare, energy grids, dams, and financial and communications sectors.**

Hybrid Warfare and its Application on CII: Trends to Acknowledge

The first trend is the attack on CII by the state actors during the conflict. In Ukraine's case, the Russian military has specifically targeted[1] more civilian critical infrastructure, even in some phases coordinating[2] between kinetic[3] and cyber means. Similarly, a simultaneous cyber-attack was carried out in coordination with missile attacks at the start of the recent 'Operation Al-Aqsa flood' by Hamas. Israel was targeted with cyber-attacks on its CII—government websites, electricity power grid, and emerging warning systems.[4] These attacks disrupted and disabled access for civilians. Attacks on the Israeli government's official websites constituted almost approx. 36 per cent of all claimed attacks.[5] Other attacks include the Jerusalem Post website, which was shut down for two days, the Noga Independent Electric system,[6] and the Israeli President's Telegram channel,[7] both of which were briefly unavailable. Many of these are an attempt by state actors to curtail the dissemination of important information, spread misinformation, and, at times, engage in cyber espionage. The exfiltration of Israeli soldiers' information on social media was one such attempt. The attacks on CII vary throughout the lifetime of conflict, shaped by the respective strategies of states. In the case of Ukraine, the attacks can be separated into five phases starting before the onset of war, as stated in a report by Google Threat Analysis Group.[8] These attacks started with the cyber-attack on the Viasat satellite that disturbed the communication access of thousands of people in Ukraine and across Europe.[9] The objectives of attacking CII are twofold: threatening a country's national security and weaponising public opinion against dispensation. There is likely a coordinated attempt between Kinetic and Cyber operations in conflict, as seen recently during Operation Al-Aqsa Flood.

The second common trend observed is hacktivism—hackers who engage in targeted cyber operations driven by different motivations.[10] They form a more extensive ecosystem in hybrid warfare operations. Attacks from hacktivists can inflict serious short-term cyber damage on CII. The Israel-Hamas war is a recent example.[11] However, this was also observed in the Ukraine-Russia war.[12] In the Israel-Hamas conflict, non-state actors from the region, but also beyond, have participated in conducting targeted Distributed Denial-of-Service (DDoS) attacks on Israel's CII. Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, which are responsible for proper management and efficient working of industries, were targeted.[13] In addition, Real Time Streaming Protocol (RTSP) Cameras were hacked for 'surveillance, reconnaissance, or gathering sensitive information' for which the Israeli government advised people to secure their home cameras, as they may be hacked to disclose information about the military movement.[14] These hacktivist groups include Killnet, Blackfield, Anonymous Sudan from Russia, Imperial Kitten, Muddy Water, Agonising Serpens from Iran, and other independent hacktivists like AnonGhost. For example, Killnet attacked and took down some Red Alert Apps, which warn citizens about incoming rocket strikes.[15] These hacktivist activities may not have destructive consequences in the short term. However, if they continue unabated in the long term, it may have severe implications for states' CII, as Israel Cyber head Gaby Portnoy expressed.[16]

The third factor is the support from the third-party states[17] and the participation of big-tech[18] companies— Meta, Google, Microsoft, Amazon, and Starlink. Technology companies have played a critical role in capacity building and strengthening defensive cyber strategy, supporting the state in defending cyber-attacks on CII. Ukraine has countered attacks from Russian and Russian-aligned hackers by working with private sector companies like Microsoft, Google, and Apple and Western countries like the UK, the US, and other EU members. However, this is also a double-edged sword, which gives these tech companies access to their CII, giving them great power in their hands. For example, it was reported that Elon Musk scuttled an attack on a Russian ship by refusing to give communication access through a stark link satellite.[19] This shows the power of private actors and big tech interfering and controlling cyberspace.

Ukraine has countered attacks from Russian and Russian-aligned hackers by working with private sector companies like Microsoft, Google, and Apple and Western countries like the UK, the US, and other EU members.

Lessons for India

India is particularly vulnerable to cyber-attacks on its CII, which currently includes seven sectors: government services, healthcare, banking, transport, telecom, power and energy, strategic and public enterprises, and financial services and insurance—from China and Pakistan. In 2018, the Ministry of Electronics and Information Technology reported that most attacks on India came from China, amounting to 35 per cent. China, which has superior and sophisticated capabilities, stands at the top of the list. These cyber-attacks on India's CII have severely compromised its national security. India's critical infrastructures increasingly depend on cyber tools for proper functioning and operations across the public and private sectors, making them more prone to cyberattacks. In 2023, India featured sixth in the Asia-Pacific region on cyberattacks.[20] The Chinese cyberattacks have targeted multiple sectors—banking and finance, power grids, transmission infrastructure, and healthcare.[21] These attacks can potentially disrupt India's CII, harming its security and economic growth. Such attacks have particularly increased after the 2020 Galwan conflict, mimicking the deteriorating relations between the two countries and representing Beijing's changing perception towards New Delhi. For example, China attacked seven State Load Dispatch Centres and four Regional Load Dispatch Centres that control grid and electricity dispatch.[22] These attacks work as a probing exercise to identify potential loopholes and weaknesses in India's CII for future exploitations. With increasing risk, India has expanded its CII ambit

India's critical infrastructures increasingly depend on cyber tools for proper functioning and operations across the public and private sectors, making them more prone to cyberattacks.

to include new domains like—Paytm, National Crime Records Bureau, and All India Institute of Medical Sciences.[23]

To strengthen its CII, India must build its defensive and offensive cyber military capabilities and establish a robust and dynamic critical infrastructure security framework. India needs to make its established protocols more transparent and accessible by working with the private and public sectors.

To strengthen its CII, India must build its defensive and offensive cyber military capabilities and establish a robust and dynamic critical infrastructure security framework. At the same time, India needs to make its established protocols more transparent and accessible by working with the private and public sectors. In this endeavour, the private sector should be given more responsibility in shouldering cyber security initiatives, as we have seen in the US cyber security strategy released this year.[24] Attacks on CII are much more complex and are undertaken mainly by state or state-supported hackers and sometimes by non-state actors. However, with the role of non-state actors increasing, India must consider their role while strategising and focusing on increasing its cyber workforce. Another effort is strengthening global cyber partnerships with big tech and states like the US, UK, EU, Japan, and Australia on capacity building, information sharing, law enforcement, and prosecution. Support from cyber friends can play an essential role in deterring hybrid warfare from adversaries like China, particularly in the cyber domain. The safety of CII must be a national security priority, and the focus should be on developing their cyber resiliency and building capabilities to protect them. The important lesson is that preparedness done in peacetime will help India during conflict and war, and to implement this, India should follow the mantra of better cyber defence going forward.

Notes:

[1] Grace B. Mueller et.al., “Cyber Operations during Russo-Ukraine War,” CSIS, July 13, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war#h2-russian-cyber-operations. Accessed on November 27, 2023.

[2] Dan Peleschuk and Pavel Polityuk, “Russia fires barrage of missiles on Ukraine cities, energy grid,” *Reuters*, December 30, 2022, https://www.reuters.com/world/europe/russia-steps-up-kherson-shelling-dismisses-zelenskiys-peace-plan-2022-12-29/. Accessed on November 27, 2023.

[3] Luke Harding, Dan Sabbagh and Isobel Koshiw, “Russia targets Ukraine energy and water infrastructure in missile attacks,” *The Guardian*, October 31, 2022, https://www.theguardian.com/world/2022/oct/31/russian-missiles-kyiv-ukraine-cities. Accessed on November 27, 2023.

[4] Eduard Kovacs, “Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks,” *Securityweek*, October 9, 2023, https://www.securityweek.com/hackers-join-in-on-israel-hamas-war-with-disruptive-cyberattacks/. Accessed on November 27, 2023.

[5] "Background 2023: Israel-Hamas War," *Radware*, https://www.radware.com/security/threat-advisories-and-attack-reports/cyber-aggression-rises-following-the-october-2023-israel-hamas-conflict/. Accessed on November 27, 2023.

[6] "Cyber Warfare and Disinformation - Future Attacks Heightened Amid Israel-Hamas Conflict," Water Information Sharing and Analysis Center, November 7, 2023, https://www.waterisac.org/portal/cyber-warfare-and-disinformation-future-attacks-heightened-amid-israel-hamas-conflict-updated. Accessed on November 27, 2023.

[7] "Israeli President Targeted by Cyber Attack," *The Defense Post,* October 6, 2023, https://www.thedefensepost.com/2023/10/06/israel-president-cyber-attack/?expand_article=1. Accessed on November 27, 2023.

[8] Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," *Google (Threat Analysis Group),* February 16, 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/. Accessed on November 27, 2023.

[9] "Viasat," Cyberpeace Institute, June 2022, https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat. Accessed on November 27, 2023.

[10] Shane Huntley, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," *Google (Threat Analysis Group),* February 16, 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/. Accessed on November 27, 2023.

11 Ingrid Lunden, "Ukraine Takes the resistance to cyberspace, assembling and 'IT army' to hack sites from Russia and its allies, calls on tech leaders to get involved," *TechCrunch*, February 28, 2022, https://techcrunch.com/2022/02/27/ukraine-takes-the-resistance-to-cyberspace-assembling-an-it-army-to-hack-sites-from-russia-and-its-allies-calls-on-tech-leaders-to-get-involved/. Accessed on November 27, 2023.

12 Lorenzo Franceschi-Bicchierai, "Hacktivism erupts in response to Hamas-Israel war," *TechCrunch*, October 10, 2023, https://techcrunch.com/2023/10/09/hacktivism-erupts-in-response-to-hamas-israel-war/?guccounter=1. Accessed on November 27, 2023.

[13] Jurgita Lapienytė ,"Hacktivists in Palestine and Israel after SCADA and other industrial control systems", *Cybernews*, November 15, 2023, https://cybernews.com/cyber-war/palestine-israel-scada-under-attack/. Accessed on November 27, 2023.

[14] Pierluigi Paganini, "Exposed security cameras in Israel and Palestine pose significant risks," *Security affairs,* October 10, 2023, https://securityaffairs.com/152265/hacking/security-cameras-israel-and-palestine.html. Accessed on November 27, 2023.

[15] Ryan Gallagher et al., "Israel is facing an onslaught of cyberattacks, including some tied to Russia, while battling Hamas," *Fortune*, October 10, 2023, https://fortune.com/2023/10/09/cyberattacks-israel-hamas-attack-russia-palestineddos/. Accessed on November 27, 2023.

[16] Sean Lyngaas, "Israel's cyber defense chief tells CNN he's concerned Iran could increase severity of its cyberattacks," *CNN*, November 6, 2023, https://edition.cnn.com/2023/11/06/politics/israel-cyber-defense-iran-concerns/index.html. Accessed on November 27, 2023.

[17] US Department of Defense, "Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say," December 3, 2022, https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/. Accessed on November 27, 2023

[18] Irene Sánchez and José Ignacio Torreblanca, "Ukraine one year on: When tech companies go to war," European Council on Foreign Relations, March 7, 2023, https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to. Accessed on November 27, 2023.

[19] Devin Coldewey, "Musk says he limited Ukraine's Starlink to prevent attack on Russia," *TechCrunch*, September 9, 2023, https://techcrunch.com/2023/09/08/musk-says-he-limited-ukraines-starlink-to-prevent-attack-on-russia/?cx_testId=6&cx_testVariant=cx_undefined&cx_artPos=2#cxrecs_s. Accessed on November 27, 2023.

[20] Sohini Bagchi, "India among top 3 most affected countries in APAC by cyber-attacks: Report," *Mosaic Digital,* October 6, 2023, https://www.techcircle.in/2023/10/06/india-is-among-top-3-most-affected-countries-in-apac-by-cyber-attacks-report. Accessed on November 27, 2023.

[21] Aihik Sur, "China-based threat actors target UIDAI, AIIMS, ICMR: Govt advisory," *Money Control,* June 9, 2023, https://www.moneycontrol.com/news/business/china-based-threat-actors-target-uidai-aiims-icmr-shows-cybersecurity-advisory-10769631.html. Accessed on November 27, 2023.

[22] "China hackers targeted power grids near Ladakh, says report," *Indian Express*, April 8, 2022, https://indianexpress.com/article/india/chinese-hackers-electricity-distribution-centres-ladakh-minister-rk-singh-7858001/. Accessed on November 27, 2023.

[23] Ministry of Electronics and Information Technology, "Gazette Notifications for declaring computer resources relating to identified Critical Information Infrastructure (CII) elements of various organisations under section 70 of IT Act, 2000, " https://www.meity.gov.in/gazette-notifications-declaring-computer-resources-relating-identified-critical-information. Accessed on November 27, 2023.

[24] The White House, "National Cyber Security Strategy 2023," March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on November 27, 2023.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Anil Chopra PVSM AVSM VM VSM (Retd).

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com
Formatting and Assistance: Ms Radhey Tambi, Ms Khyati Singh and Mr Rohit Singh

The views expressed in this brief are those of the author and not necessarily of the Centre or any other organisation.