CYBERWARFARE IN RUSSIA UKRAINE WAR LESSONS FOR INDIA

Flt Lt Shobhit Mehta & Gp Capt Umang Kumar

Abstract

Russia invaded Ukraine on 24 February 2022, however the inevitable happening could have been predicted post the War in Donbas 2014. This 10-year-long ongoing struggle is a major testament to the importance of Cyber Space in the battlefield arena. Ukraine neglected its importance for the initial 8 years and was finally paralysed after the ViaSat compromise by the Russian hacktivists. This reactive approach cost Ukraine billions of dollars due to multiple cyber-attacks namely Operation Armageddon, Operation Snake, Ukraine Power Grid attack, and the famous ViaSat attack. It was finally on 26 February 2022, when Mykhailo Fedorov, Minister of Digital Transformation pioneered the formation of the IT Army of Ukraine.[1] The step was very reactive; however, the Ukrainian IT Army has subjugated Russian hacktivists by launching five major cyber-attacks in 2024 only, thus proving that the power of cyberspace lies not in the quantity of minds but the quality. The paper takes us through major cyber-attacks from both fronts and brings out the vital lesson i.e. Self-Reliance. The paper houses two terms at the core, i.e., Cyber Warfare and Information Warfare. Both the terms are closely interlinked as Cyber Warfare provides a platform for large information warfare campaigns. It would not be wrong to comment that Elon Musk has been the knight in shining armor for Ukraine as all forms of military and commercial communication in Ukraine depend entirely on Starlink, a subsidiary of SpaceX. The population of Ukraine is 3.5 times of Israel, still what makes Israel tempestuous is the self-

confidence. Self-confidence comes from self-reliance, bringing extreme sovereignty to decision-making. Today, Ukrainian decision-making is bound to be affected not only by the interests of the West but also by private players like SpaceX. Through the course of the paper, it could be learnt how regulated OSINT, extreme self-reliance, focused Psy-Ops and an armored cyberspace could become the most lethal form of deterrence in this modern warfare.

INTRODUCTION

Cyberwarfare is no longer an alien term in today's geopolitical scenario. It is a tool for highly disruptive Information Warfare (IW) campaigns. Although it is tough to differentiate between cyber-warfare and IW, IW covers propaganda, psyops, and influence campaigns while cyber warfare encompasses DDoS attacks, deploying malware, Zero-day exploits, etc. Countries have recognised cyber-warfare as an important dimension of warfighting with superpowers slicing a huge percentage of defence budget into the same. 46 percent of global digital transactions happen in India. India being the second most populous country plays a significant role in cyberspace and can be a decisive factor in PSYOPs. Recently, a prudent move by the Union Government to train 5000 cyber commandos in the next five years while strengthening the I4C wing of the Ministry of Home Affairs speaks about the potential of cyberwarfare. The paper briefly discusses the various cyber-attacks undertaken by both Russia and Ukraine and bring out important lessons for India.

BACKGROUND OF THE CYBER WAR

Cyberwarfare has been an important confrontation component in the ongoing Russia-Ukraine Conflict since the invasion of Russia on February 24, 2022. After the end of the Cold War, it was the fourth time Russia used military power against its neighbour. However, it was the seventh time Russia used cyberwarfare as a part of a larger campaign that encompasses economic disruption, propaganda, cyber sabotage, DDoS attacks, MiTM attacks, and cyber espionage. Although the physical invasion into the Ukrainian territory happened in 2022, the first cyber-

attack dates back to 2013 with major Russian weapon Uroboros being in sensation since 2005.

The Russia-Ukraine War has been widely covered in various Global broadcasts. Social Media has been a boon and a bane depending on which front exploits it logically and in a regulated manner. The existing evidence on the war has been collected via Open Source. The timelines of cyberattacks during the ongoing Russia-Ukraine are discussed in the following paragraphs:

- **Operation Armageddon**. The operation has been active since mid-2013. Russia opposed the Ukrainian inclination towards the EU. Extensive phishing emails lured the victim to open a malicious attachment. Cybercriminals exploited previously obtained confidential documents to entice Ukrainian targets into downloading malicious payloads from a remotely compromised Control server. The final payload was some form of RAT (Remote Administration Tool) that caused Cyber Espionage.[2] Additionally, the early campaign has also included malware which redirects traffic by disrupting the DNS servers used by the victim machines. The modus operandi involved targeted phishing emails, self-extracting archives, and disruption of Critical Information Infrastructure. More than 5000 cyber attacks were launched against around 1500 Ukrainian entities including the Ministry of Foreign Affairs. It is a perfect example of Russia's broader hybrid warfare strategy combining conventional military tactics with cyber operations.

- **Operation Snake.** The cyberespionage 'toolkit' called Snake or Ouroboros(Serpent in Greek mythology) attacked classified Ukrainian systems like the famous Pentagon plaguing. Post massive Kiev protests due to Mr. Yanukovych's unexpected inclination towards Russia in 2014, 14 cases of Snake were registered with a total of 32 in Ukraine itself since 2010 out of 56 worldwide.[3] Snake gives full remote access to the compromised systems leading to siphoning data from local computers to

remote servers. The attacks were linked with the Moscow time zone and compromised computers of the Ukrainian PMO and at least 10 Ukrainian embassies making highly sensitive diplomatic information available to the perpetrators of the attack. Snake has been recognised as a far more precise weapon than Stuxnet and is an extremely targeted piece of malware that initially infected 84 prominent public websites that were regularly visited by top officials of public and private enterprises. During the initial stage of the attack, users who visited the compromised websites were asked to update their Shockwave player software. Information was collected from thousands of individuals who consented to this request. During the secondary stage of infection, users with IP addresses linked to government entities were targeted with an initial malware called 'wipbot'.[4] This software enabled Snake operatives to assess the rank of infected individuals within the government hierarchy. Finally, a highly targeted malware attack was launched onto the computers of identified higher officials. The modus operandi involved the covert operation of the toolkit enabling it to remain undetected. Snake became active only when the system connected to the internet. It acted as an intermediary point in a network of compromised devices, to exfiltrate data. The attack targeted government networks, critical infrastructure, and private enterprises. The FSB's deployment of Snake signals a long-term strategy to gather critical military intelligence.

- **Interference in Ukrainian Parliamentary Elections (2014).** CyberBerkut, a pro-Russian hacktivist group having ties with Fancy Bear (GRU hacker group) compromised the Ukrainian Central Election system, four days before the national vote.[5] Within 24 hours, the compromised data was uploaded to the internet depicting the success of the operation. The Malware delineated a false result onto the internet, post which DDoS attacks hung the Election Commission website. Ukrainian cybersecurity personnel were able to remove the malware 40 minutes before the election results went live, preventing it from releasing erroneous results.[6]

The modus operandi involved propaganda to discredit the legitimacy of the elections and project Ukraine as a failed state. The Kremlin claimed Ukraine to be controlled by 'fascists' and 'neo-Nazi sympathisers'. The scaling of the attack involved citizens in Crimea and certain areas of Donetsk and Luhansk losing their ability to participate in elections. Widespread misinformation campaigns undermined public faith in the integrity of the voting process.

- **Ukraine Power Grid Hack.** On December 23, 2015, there was an unscheduled power outage in Ukrainian power companies affecting 2.5 lakh personnel.[7] Further technical analysis revealed the presence of BlackEnergy (BE) malware in the computer systems of power companies. In the event mainly three power distribution companies (Oblenergos) were impacted. The cyber-attack at each company was exercised within 30 minutes. Remote operation of breakers was conducted either by remote Industrial Control System (ICS) via VPN or by existing Remote Administration Tool (RAT) at the operating system level.[8] For both possibilities, it is pertinent that actors were able to acquire legitimate credentials via suspected social engineering. KillDisk malware was executed after a cyberattack that corrupted the master boot record of the infected system. The firmware of serial to Ethernet devices was also corrupted. The modus operandi involved complete control of SCADA systems through phishing emails, thus causing remote shutdowns. Unlike data theft attacks, this was aimed at actual physical disruption leading to temporary blackouts affecting roughly 230,000 consumers.[9]

- **2017 Cyber Attacks on Ukraine.** On 27 June 2017, Colonel Maksym Shapoval, a Ukrainian intelligence officer was assassinated in a car bomb in the capital city of Kiev.[10] Post the assassination, the largest known hacker attack in world history was launched. The cyberattack was carried out using the NotPetya virus which used EternalBlue exploits. Soon after NotPetya was executed, the computer underwent a forced

restart as the Masterfile Table of the hard drive was executed, which further displayed the text that files had been encrypted and access could only be granted in exchange for Bitcoins.[11] Also, the Server Message Block protocol in Windows got exploited thus infecting local computers connected to the same network. During the attack, the servers at Ukraine's Chernobyl Nuclear Power Plant and Ukrainian Railways were affected thus handicapping an entire nation. Within 24 hours, the attack was halted and on technical investigation, it was found that the attack was initiated from MeDoc update which is a tax accounting software with over 4 lakh downloads. Servers at the State Savings Bank of Ukraine and Boryspil International Airport were also compromised.[12] Although there is no evidence of a direct connection between the killing of Colonel Shapoval and the NotPetya virus attack, the same couldn't be a mere coincidence. Colonel Shapoval was a senior Ukrainian Security Service (SBU) official and head of a key counterintelligence unit involved in uncovering Russian spies. The incident reflected the Russian Hybrid warfare strategy combining Psyops with Electronic invasion. The modus operandi involved utilising the EternalBlue vulnerability. It was clearly an example of Hybrid Warfare. Scaling of the attack involved targeting over 80 Ukrainian entities, including financial institutions and government agencies. The attack quickly expanded globally, impacting organisations in Europe and the United States. 10% of Ukrainian computers were impacted. The attack resulted in significant operational disruptions and worldwide financial losses exceeding $10 billion.[13]

- **2022 Cyber attacks on Ukraine.** On 14 January 2022, a cyber-attack occurred on 70 government websites including Foreign Affairs and Defence Ministry.[14] Before this on 13 January, Microsoft Threat Intelligence Centre (MSTIC) identified Whispergate carrying out cyber sabotage on various public, private, and non-governmental organisations. Later on 19 January 2022, the Russian hacktivist group Primitive Bear tried to attack a top

Western public entity in Ukraine. A significant distributed denial-of-service (DDoS) attack struck the websites of Ukraine's defence ministry, army, and two major banks, PrivatBank and Oschadbank, on February 15, 2022.[15] This cyberattack compromised the online presence of these key institutions. Various mobile apps and ATMs of various banks were also compromised. Russian Main Intelligence Directorate (GRU) was suspected behind the attack since there was high traffic flow from GRU-based IT infrastructure towards Ukrainian IP addresses. On 23 February 2022, a wiper malware attack was identified on computers belonging to defence, aviation, IT, and banking sectors in Ukraine. On 24 February 2024, thousands of ViaSat modems went offline after hackers targeted a VPN installation in Turin thus pushing wiper malware into multiple KA-SAT broadband modems of ViaSat. This disrupted Ukrainian networks since they used ViaSat's network for communication. Internet services too were crippled in Ukraine post the attack.[16] On March 9, 2022, the Quad9 recursive resolver, which blocks malware, thwarted 4.6 million cyberattacks targeting devices in Ukraine and Poland.[17] A surge in phishing and malware activities was detected as the majority of blocked DNS requests originated from Ukraine. Since 1.4 million Ukrainian refugees were present in Poland, figures for Poland were also elevated. In the ViaSat Modem hack, a VPN appliance misconfiguration was exploited to gain unauthorised entry into the ViaSat network's management segment. The cyberattack utilised a wiper malware called 'AcidRain', which erased data on targeted devices. The attack impacted thousands of modems and resulted in the shipment of approximately 30,000 new modems. Further upgraded version 'AcidPour' was released to have an even greater impact.[18]

- **Attack on Starlink in Ukraine.** After the disruption of ViaSat Networks, on 26 February 2022 Minister Mykhailo Fedorov, requested Elon Musk for Starlink assistance in Ukraine.[19] The response was swift and positive. Within two days, the first shipment of Starlink terminals arrived. Unlike conventional

satellite internet, Starlink used fragmented networking using narrow beams of Ku and Ka bands. Starlink is the lifeline of military and business communication in Ukraine which uses a high degree of defence-in-depth concept.[20] However, there were many videos of careful dismantling of the Starlink terminal. Russian hacktivists got Starlink terminals from the dark web and used the OSINT to first dismantle the terminal and finally place a Modchip in the PCB which provided them access into the highly secure layers of Starlink communication, thus interfering with the available bandwidth. Ukraine has reported degradation in Starlink connectivity over time.[21] The operational approach relied heavily on open-source intelligence (OSINT) and sophisticated electronic warfare systems. As Russian military operations escalated, interruptions became more common and intense, especially in the vicinity of Kharkiv, leading to major communication breakdowns among Ukrainian military units. This is a perfect example of Russian Hybrid Warfare.

- **Ukrainian Attack on Planet**. In mid-January 2024 Ukrainian hacktivists sabotaged 2 petabytes of data and compromised 280 servers at Planet which is a state space hydro-meteorology Research Centre that aided the Russian military in analysing satellite imaging.[22] The damage was the US $10. Further, a Russian Arctic outpost on the Bolshevik Island was cut off from Russian communication networks. The attack involved extensive reconnaissance of the facility's operations, security measures, and personnel. Ukraine attacked deep into Russian territory and was a major confidence booster and resulted in increased Western aid as the world witnessed Ukraine's ability to strike back.[23]

- **HUR Attack on Bureaucrats.** On February 4, 2024, hackers from the Main Directorate of Intelligence of Ukraine's Defence Ministry (HUR) compromised a digital document management platform called 'bureaucrats'.[24] This infiltration revealed multiple confidential files belonging to high-level Russian officials, especially Russian Minister Timur Ivanov. Additionally, the HUR hackers disrupted

Russian military technology for modifying commercial DJI drones, effectively disabling the servers operating Russia's 'friend or foe' recognition system.[25] The attack method involved Advanced Persistent Threat (APT) techniques.

- **Attack on Moskollector.** In April HUR targeted Interregional Transit Telecom (MTT) disarraying critical configuration files leading to network disruptions in Moscow and St. Petersburg. Further Sewage Monitoring and Control System of Moscow was disrupted after 87,000 sensors of communication giant Moskollector were shut down.[26]

- **DDoS Attack on Russian Aerospace .** In early June 2024, HUR launched a DDoS attack on various government websites like the Ministry of Justice, Defence, Finance, IT and Communication, Industry and Energy, etc. Website of United Aircraft Company (UAC), was rendered inaccessible for an extended period.[27] On June 12, 2024, hackers from Ukraine disrupted the online systems of several Russian airports, including Yuzhno-Sakhalinsk, Saratov's Gagarin Airport, etc. causing delays for flights primarily bound for Sochi, Moscow, etc. Before this incident, HUR compromised the official website server of the Stavropol Region's State Duma, inserting the message 'Hold on, we will liberate you!'. Subsequently, HUR along with the BO Team hacker group attacked Russian municipal web resources, disabling two hypervisors and multiple communication devices.[28]

- **Attack on Russian Banking Establishment.** On July 23, 2024, Ukraine's Ministry of Defence Main Intelligence Directorate launched an operation to identify financial institutions that were funding military operations against Ukraine.[29] Subsequently, cyber attack was launched disabling customers of several major Russian banks to access cash from ATMs. The databases of numerous prominent banks, including RSHB Bank, iBank, Alfa-Bank, Raiffeisen Bank, Tinkoff Bank etc. were compromised, followed by service interruptions at multiple large Russian

telecommunications and internet service providers, such as Tele2, Beeline, MegaFon, and Rostelecom.[30]

UNMASKING RUSSIA'S CYBER ONSLAUGHT : AN ANALYSIS

Various cyber warfare tactics were employed by Russia including DDoS attacks, phishing attacks, and malware deployment across various Ukrainian Critical Information Infrastructure. The attacks however lacked planning, coordination, and quality. Despite being a well-established superpower, Russia was unable to tone down its adversary's morale in the initial days of invasion. Although Russian planning was a combined effort by both military units and pro-Russian hacking groups highlighting the importance of public-private partnership in times of distress, still the quality was not up to the mark. The ViaSat's KA-SAT satellite attack caused considerable disruption, however, could not provide the required tactical advantage thus causing a disconnect between cyber actions and military outcomes.[31] The research paper brought out a series of cyber-attacks launched by Ukraine since January 2024. This shows the inability of Russia to adapt to the changing warfare arena and its trivial attitude towards Ukraine considering it a weak adversary. The major issue with the Russian forces was the unchecked use of social media by military personnel thus revealing information about their movements and deployment. Also, the Russian forces relied on poorly secured communication systems including consumer-grade technology and Ukrainian telecom infrastructure. Even the disciplined units relied on poorly secured systems and had no choice but to share data over insecure channels. There are shreds of evidence that Russian investment toward ensuring an armored communication channel never saw the light of day due to prevailing corruption within the Russian procurement channel.[32]

ANALYSING UKRAINE'S CYBER STRIKES

Initially, Ukraine was ignorant to the power of cyberwarfare and faced many hostilities since its communication resources were compromised by Russian forces. In any war, timely communication is a highly decisive factor. Despite initial hostilities, what happened next is an inspiring case study for generations to come. Ukraine swiftly adapted to cyberwarfare,

exploited OSINT to its peak and gathered critical information about Russian movement and deployment. Within two days Starlink terminals were imported and communication facilities were restored. The HUR carried out significant operations, exposing classified Russian files and disrupting essential services within Russia.[33] Ukraine's cyber potential is evident from the fact that it was able to penetrate into Russian networks and extract classified information. Ukraine also employed robust EW techniques to intercept unsecured transmissions. This has enabled them to acquire real-time intelligence on Russian troop movements and locations, providing a strategic edge despite their numerical disadvantage in combat.[34] Ukraine not only fostered its cyber potential in times of distress but also operated successfully which is highly commendable. As Ukraine persists in its cyber campaign against Russia, it encounters several policy challenges. Furthermore, Ukraine could consistently engage in combating narrative warfare, a strategy Russia has employed since and even before February 24, 2022.

INDIA'S TAKEAWAYS FROM THE CRISIS

Russia-Ukraine war taught us many lessons on adaptability, resilience, emotional intelligence, indigenisation, geopolitical relationships, and most importantly grit. Some of the key lessons can be summarised as follows:

- **Strengthening the Communication Infrastructure.** Ukraine was entirely dependent on ViaSat Communications based in Carlsbad, California for its military and commercial communication. After the satellite modems got compromised, Ukraine was left crippled. Communication is the most important factor in today's digital-dominant arena. Even during the 2014 invasion of Russia into the Crimean Peninsula, it was the communication infrastructure that was disrupted and OFC lines were cut down thus amputating the Crimean Peninsula. It is a matter of pride that both the internet service giants of India, i.e., Airtel and Jio are India-based and thus have an emotional connection with maintaining resilience to any cyberattack on the Indian subcontinent, unlike ViaSat which

chose to withdraw the service to avoid further security breach thus affecting their services in other nations as well. It is of utmost importance that Indian Government works in close coordination with these internet giants and sensitise the decision makers on strengthening their physical and cyber security of servers. It is of utmost importance that every employee instills a soldierly attitude. In a similar vein, Reliance Industries has launched a commendable initiative. Rather than hiring random individuals without background checks to protect high-value industrial servers, the company has established a specialised security division called Reliance Global Corporate Security (GCS).[35] The Agnipath scheme is a fresh induction in the military set-up of the nation. The aim has always been a leaner and younger army, however, critics can argue about the non-secure future of recruits. India could draw lessons from nations where military service is compulsory and appreciate their quality of human resources. New Delhi is not providing an insecure future and definitely not imposing compulsory military service, rather bringing down the average age of armed forces and helping individuals instill ramrod posture by giving on-field practical exposure, unlike online platforms educating on how to get up early in the morning and stay motivated. Even after 4 years of engagement, the lessons learnt are going to stay forever with the recruits. Corporate giants like TATA Group, Bharti Airtel, Mahindra Group, Adani Group, etc. should definitely draw motivation from Reliance and ponder upon developing their own credible security arm for safeguarding high-value industrial assets employing the ones who gave their youth to the nation.

- **Investment into Cognitive Warfare.** Cognitive warfare represents the non-traditional conflict that employs psychological and information-centric strategies to affect the subconscious thus manipulating thoughts, convictions, and sentiments of individuals, groups, and countries.[36] One method of conducting cognitive warfare is the use of Software Defined Radios (SDR) for dynamic audio messaging. The first step in the project will be to develop

an SDR for handling wide-bandwidth signals and handling data in real-time. Then specialised software must be developed to embed subliminal messages in audio streams. The SDR will then be placed in areas to continuously sniff enemy frequencies. Machine learning will pick up on trends and psychological loopholes. These habits and weaknesses will be analysed, and subliminal messages will be created and, via Digital Signal Processing, delivered to the enemy via audio streams in a way that conscious perception can't hear. SDR will be programmed to change frequencies and modulation schemes and track the alteration of enemy behaviour and morale to provide feedback that can help tailor future subliminal messaging attacks.

- **Investment in Hardware and Software Testing Labs and Skilled Force.** The creation and implementation of hardware and software testing facilities play a vital role in improving the quality, dependability, and efficiency of tech products. These facilities provide environments for thorough product evaluation, ensuring compliance with industry norms and user expectations. The establishment of testing facilities incorporates a number of steps, including identifying the technologies and hardware required, hiring skilled staff, and putting certified testing procedures into place. Physical product evaluation and software-integrated testing need to be carried out in efficient testing facilities. To find flaws and guarantee smooth cross-platform operations, software testing uses a variety of approaches, such as unit, integration, and system tests. Despite growing recognition of the importance of these testing facilities', India continues to face infrastructure challenges and a lack of skilled professionals in this field.[37] Investment in specialised training programs needs to be focused. As per the NASSCOM report, India will need over 1 million skilled software testing professionals by 2025.

- **Self Reliance.** The 2017 Cyber Attack on Ukraine taught us that India cannot afford any zero-day exploit and this is only possible if it goes for Make in India followed by extensive testing. Western

military aid is crucial for Ukraine's hardware supplies, while approximately 30 percent of Russia's defence manufacturing relies on components sourced from abroad.[38] A prudent move by Indian Defence Forces to discard Chinese cameras is a major step to prevent any cyber espionage by foreign agents. The example of PCB tampering and Modchip has been discussed. In this arena of the 'Internet of Things' where everything is connected via the internet to everything needs to be prevented from leaving digital footprints. Segregating from the internet is impossible, the only thing possible is going for products that are Made in India ranging from an earphone to automobiles that can tap the conversation via Android Play. India also quite behind in terms of an indigenous mobile company that is widely accepted and thus is a point of concern.

- **Evolution of Centralised Cybersecurity Framework.** Several ministries and agencies oversee cybersecurity in India, with the Ministry of Electronics and Information Technology (MeitY) developing cybersecurity policies, the Ministry of Home Affairs (MHA) handling cybercrime investigations and national security matters, the National Technical Research Organisation (NTRO) gathering technical intelligence, and the National Critical Information Infrastructure Protection Centre (NCIIPC) safeguarding critical infrastructure. Unlike Israel, where the Israel National Cyber Directorate (INCD) functions as a centralised authority for cybersecurity under the Prime Minister's office, India lacks a unified command structure. The INCD effectively coordinates national efforts and combines military and civilian resources. In contrast, India's decentralised approach may result in multiple agencies responding independently during a national emergency, without a single authority coordinating their actions. If given the authority to issue directives and manage responses during cybersecurity emergencies, the National Security Council Secretariat (NSCS) could potentially serve as the single point of contact (SPOC).

- **Need for Clearer Guidelines on Setting Offensive Posture.** India always had a defensive approach toward cybersecurity. The formation of institutions like CERT-In which focuses on incident response and mitigation is a testament to this. The country did not have clear policies to initiate cyber offensives. The introduction of the Joint Doctrine for Cyberspace Operations in June 2024 was a major shift in India's cybersecurity stance, recognising the need for incorporating offensive capabilities.[39] It provided frameworks for better cross-service collaboration but lacked clear guidelines for putting offensives into practice.

- **Need for a Robust and Ethical Framework.** India recently introduced its Joint Doctrine for Cyberspace Operations. The step clearly reflects the cyber awareness of the nation, however lacks clearer guidelines and accountability measures while carrying out an offensive cyber-attack. This incertitude will prevent a focused offensive posture. The UN Charter discusses the principles of state sovereignty and non-intervention which draw a very hazy picture regarding the legality of cyber operations.[40] For example, offensive cyber actions could be considered breaches of sovereignty, raising legal issues regarding escalation.[41] A well-defined legal framework would help in establishing accountability protocols for personnel engaged in offensive operations. This will ensure that actions align with both national and international laws.

- **Regulations on OSINT.** Starlink has been providing military and commercial communication in Ukraine after the ViaSat Modem Hack.[42] However, hacktivists have been able to penetrate the highly secure firewall systems of Starlink with the help of Modchip which is placed after careful dismantling of the terminal. There were many videos on dismantling the Starlink terminal on YouTube primarily from the West. It is an exemplar of acting against the interests merely for minuscule gains. It is of paramount importance to apprise Indian-based tech giants to share minimum resource data on an open platform. Ukraine exploited videos and selfies uploaded by Russian soldiers to target their positions, prompting

Moscow to implement legislation prohibiting smartphones on the battlefield. Additionally, Kyiv and its supporters utilised open-source information to shape narratives against Moscow. Consequently, it is crucial to emphasise the controlled use of open-source data.

- **Exploiting the Primitive Yet Powerful Psyops.** India is the second most populous country in the world. With the advent of the IT revolution and YouTube shows the huge pool of talent that India holds. YouTube CEO mentioned that creators should be recognised as 'next-generation studios' for the way they are refining entertainment and India is the fastest-growing market for video-sharing platforms and is leading in many global trends in terms of the creator economy all over the world. From fitness to entertainment to education to vlogs to webinars to gaming, in every sphere of India Youtubers are ruling. This can be a major tool for India while exercising PSYOPs as part of cyberwarfare. Indian Government should work in close coordination with these next-generation studios and shape public opinions as per the interest of the nation. PSYOPs have been the most powerful tool for ages. All the freedom fighters exercised this form of warfare. With the advent of the cyber dimension, the outreach has increased manifolds.

- **Strengthening the Narrative Warfare.** The battle for narrative dominance is a psychological effort to influence public sentiment domestically and internationally. Skillfully constructed narratives can garner support for military actions, justify policies, and persuade undecided groups. In the current digital landscape, managing information flow is crucial. Countries must proactively shape their narratives to thwart adversaries' attempts to manipulate public perception. A cohesive messaging strategy strengthens a country's narrative and undermines opposing viewpoints, necessitating a dedicated psychological operations structure across various command levels. India could establish a psychological operations unit at the theatre command level to effectively handle narrative warfare. Probably Command Cyber

Operations and Support Wings (CCOSW) can be tasked with the same. The unit can initially give exposure to the military lifestyle to journalists and media houses and in turn, get the soldiers trained on media management and narrative warfare. Israel and the US are perfect examples of the same. "Hasbara," a term in Hebrew meaning "explanation," describes Israel's efforts in public diplomacy.[43] These initiatives aim to influence global perceptions and narratives about the nation, especially its policies and actions. Israel's narrative warfare includes the distribution of government-approved military narratives and Search Engine Optimisation which boosts favorable content and diminishes negative information. Another example to quote is the 77th Brigade of the U.S. Army which concentrates on combating misinformation and conducting information operations within conventional military activities. The best way to emerge as a leader in narrative warfare is to play a game on two fronts. To shape the narrative of the world towards India it is essential to checkmate major social media platforms like Meta, Twitter, and YouTube which are all US-based and India has hardly any control over their information optimisation algorithms. Filtering the narration through the psychological operations unit could be significant in this aspect. To shape the narrative within India and India towards the world, lessons from China could be learnt which has banned Western social networking sites and has achieved self-reliance in narrative warfare as well. WeChat is a substitute for Meta, Sina Weibo is a substitute for Twitter and Youku is a substitute for YouTube. New Delhi too could develop its very own narrative warfare DCs and launch apps that will ensure control of information flow, rapid dissemination of state narratives, monitoring of real public sentiment, and counteracting foreign narratives.

- **Dedicated Task Force for Strengthening HUMINT Around Indian Borders.** Sashastra Seema Bal (SSB), post-1962 Chinese invasion was actively involved in strengthening national unity among border populations and nurturing loyalty to India,

especially in remote areas that felt disconnected from the central government.[44] The paramilitary force exercised the HUMINT potential of local villagers thus bolstering intelligence and early warning systems for military units.[45] A similar concept can be revived and a dedicated task force functioning under Command Cyber Operations and Support Wings (CCOSW) under each command can be formulated that will work in close liaison with IB and R&AW, thus further strengthening inter-agency ties.

- **Raising Cyber Territorial Army.** In the realm of Information Technology (IT) and cybersecurity, India has established itself as a global leader, demonstrating the exceptional skills of its workforce. The IT industry accounts for roughly 7.5% of India's GDP, with projected revenues of $254 billion for FY 2024. India is home to more than 70,000 recognised startups and approximately 107 unicorns.[46] The nation has also made considerable progress in cybersecurity, implementing measures to strengthen digital security frameworks and address cyber threats. The government should create a platform for these passionate techies to serve the nation. The PSYOPs unit proposed above can collaborate with Internshala or LinkedIn and recruit individuals fit to serve the nation as part of the Cyber Territorial Army, which can be separate to that of the Territorial Army's existing initiatives like that with the CyberPeace Foundation, in organising hackathon. This will motivate non-uniformed civilians from leading private and other sectors to join the armed forces and the output will surely be better post donning the uniform.

- **Nurturing a Strong Cyber Wing.** Ukraine followed a very reactive approach when it came to cyberwarfare. Following the Russian invasion, Mykhailo Fedorov, who serves as both the Minister of Digital Transformation and First Vice Prime Minister of Ukraine, declared the establishment of the IT Army of Ukraine on February 26, 2022. Since 2014, Ukraine has been under constant cyber-attack. A proactive decision could have saved Ukraine from such attacks well in advance. The recent initiative by Union Government

on training 5000 Cyber commandos in the next 5 years is a commendable step towards securing information and cyberspace.

- **Revisiting Past Memorandums and Treaties.** Various memorandums and treaties are signed over time, however, with changing governments the practical execution of the agreements becomes questionable. As was the case with Ukraine which gave up nuclear arms in the 1994 Budapest Memorandum in exchange for favourable commitments from various nations including Russia. India needs to visit past memorandums and thoroughly evaluate the trustworthiness guaranteed. Even the UN Security Council didn't take any major step towards the Russia-Ukraine conflict highlighting the inability of international bodies when superpowers are involved. On paper, many agreements have been signed like General Security of Military Information Agreement (GSOMIA), Logistics Exchange Memorandum of Agreement (LEMOA), Communications Compatibility and Security Agreement (COMCASA), Basic Exchange and Cooperation Agreement (BECA) and Bilateral Defence Cooperation Agreements.[47] New Delhi needs to ensure that these agreements are exercised once in 6 months and thoroughly discussed in joint exercises and lessons learned are incorporated and necessary changes are made in the agreement, or else every time new government comes, new agreements will keep getting piled up without making any sense.

- **High Adaptability.** A paper published in the 'Carnegie Endowment for International Peace' mentions that cyber-attacks do not serve as decisive strategic tools. Instead, they function in an auxiliary capacity, complementing broader warfare efforts in primary combat zones. Offensive cyber operations during an armed conflict are not strategically decisive but rather play a supporting role in major theatre wars. Although it was evident that Russia had far more cyber op capabilities than Ukraine and Ukraine saw a lot of such attacks since 2014, however still as of today, Ukraine is standing strong against the mighty Russians and this teaches the biggest lesson of 'High Adaptability'. Ukraine always

dealt with such attacks with an open mind and embraced evolving technical solutions despite the conventional battlefield marches. One such example is requesting Elon Musk for Starlink services in Ukraine overnight on X.

- **Placements, Hackathons, and Internships (Israel's Elite Secret Cyber Unit 8200).** A cybersecurity council comprising both government and private sector representatives should be established in India. This body should be empowered to conduct investigations, convene meetings, and propose specific cybersecurity measures. India also needs to expand international cooperation and engage further with international organisations like the US, Interpol, and the Global Forum on Cyber Expertise. India is home to the brightest minds in the world studying in top tech institutions like IIT. Indian Government should engage in Campus Placements attracting the top minds to work with CERT-In rather than Google, Facebook, or other Tech Giants. Also, Cyber Wing should keep track of Hackathon champions and motivate them to work for the nation by giving internships. Internships are the best means to introduce young sharp minds to this way of life where money takes a backseat and something higher drives them to work for the nation. Israel's elite secret cyber unit 8200 is the mastermind behind the recent pager attack which consists of mostly Gen Z. Now it's India's turn to channel the massive potential of the Indian Generation Zoomers.

CONCLUSION

The world only respects the one, who is powerful and independent. There is no place for the weak. The crux of the paper boils down to just one word: Atmanirbharata. The word is the key to Global dominance and becoming a world leader. The Government of India has taken various initiatives to ensure an armoured cyberspace. Some of the key milestones in this direction have been the introduction of the National Cyber Security Policy 2013, the formation of the National Critical Information Infrastructure Protection Centre (NCIIPC) under section 70A

of the IT Act 2000 (amended in 2008), the formation of Indian Computer Response Team and in turn introduction of Cyber Swachhta Kendra by Cert In in 2017. Personal Data Protection Bill was introduced in the year 2023 which focused on concurrence-based Data Collection by businesses. Ministry of Home Affairs introduced The Cyber Coordination Centre to ensure coordination between various law enforcement and cyber security agencies. In 2018, the Defence Cyber Agency (DCyA) was established. In June 2024, India introduced its Joint Doctrine for Cyberspace Operations, under the leadership of the Chief of Defence Staff. Although this doctrine marks a significant advancement in bolstering India's cyber capabilities and fostering inter-service cooperation, the issue of a disjointed governance framework remains unresolved. Additionally, the doctrine requires the inclusion of appropriate legal guidelines for initiating offensive cyber attacks. The government has largely invested in developing indigenous Software Defined Radios (SDRs) bringing together the Defence Electronics Applications Laboratory (DEAL), IIT Kanpur and DRDO.[48] This process needs to be expedited, and concurrent research should be initiated on software development for real-time analysis of adversary communications, taking into account the Software Development Institute (SDI). Israel follows an aggressive approach and eliminates targets in advance to maintain regional supremacy. The Stuxnet attack showcases the offensive stance of both the US and Israel. India should work on similar lines but first, decide the rules of engagement for global awareness. India must actively work towards strengthening the narrative warfare. By promoting narratives that distort reality, Russia aims to attract global attention in its favor. As one of the most populous nations, India should actively work towards safeguarding itself from the projection of distorted reality. To boost the cyberculture in the country, basic cyber hygiene should be introduced as an independent subject in schools and young minds should be educated on the potential of the cyber world. Ethical hacking and cyber security can be made an independent engineering discipline with universities working in close coordination with DCyA, CERT-In, TCS, NCCC, etc. towards providing internships and handpicking exceptional talent. Additional Security Operation Centres should be established across

the Nation to ensure real-time threat monitoring and incident response. India could also ponder over incentivising cybersecurity start-ups and providing funding to top research institutions working towards filling gaps in the cyber-ecosystem. Thus, building a ramrod and credible security arm, boosting local tech innovation, identifying nascent talent via hackathons and internships, incentivising cyber startups, fostering public-private partnerships, and educating on correct cyber posture can help sketch a resilient digital future of India.

★★★

Flt Lt Shobhit Mehta is a serving officer in the Indian Air Force and is an Engineering graduate from IIIT Ranchi. He is an alumnus of AFTC Bangalore.

Gp Capt Umang Kumar is a serving officer in the Indian Air Force. He is an alumnus of AFTC Bangalore and did his M Tech in Computer Science from IIT Bombay.

NOTES

1 *D. Goodin, "After Ukraine recruits an "IT Army," dozens of Russian sites go dark," 1 March 2022. [Online]. Available: https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/. [Accessed 26 September 2024].*

2 *B. Prince, "'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Lookingglass," Security Week, 28 April 2015. [Online]. Available: https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass/. [Accessed 26 September 2024].*

3 *L. Ciolacu, "'Game-Changing' Snake Malware Used in Espionage on Ukraine," 2014 March 11. [Online]. Available: https://www.bitdefender.com/en-us/blog/hotforsecurity/game-changing-snake-malware-used-in-espionage-on-ukraine. [Accessed 01 Jan 2025].*

4 *S. Jones, "Russia-linked cyber attack on Ukraine PM's office," CNBC, 08 August 2014. [Online]. Available: https://www.cnbc.com/2014/08/08/russia-linked-cyber-attack-on-ukraine-pms-office.html. [Accessed 21 September 2024].*

5 *M. Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," The Christian Science Monitor, 18 June 2014. [Online]. Available: https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers. [Accessed 29 September 2024].*

[6] *Ibid*

[7] *"Cyber-Attack Against Ukrainian Critical Infrastructure," 20 July 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [Accessed 01 Jan 2025].*

[8] *Ibid*

[9] *Ibid*

[10] *A. Luhn, "Ukrainian military intelligence officer killed by car bomb in Kiev," The Guardian, 27 June 2017. [Online]. Available: https://www.theguardian.com/world/2017/jun/27/ukraine-colonel-maksim-shapoval-killed-car-bomb-kiev. [Accessed 23 September 2024].*

[11] *Ibid*

[12] *J. Wolff, "How the NotPetya attack is reshaping cyber insurance," 01 Dec 2021. [Online]. Available: https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/. [Accessed 01 Jan 2025]*

[13] *Ibid*

[14] *D. Jones, "Viasat network cyberattack linked to newly discovered Russian wiper," Cyber Security Dive, 2022 April 2022. [Online]. Available: https://www.cybersecuritydive.com/news/viasat-network-cyberattack-linked-to-newly-discovered-russian-wiper/621421/. [Accessed 24 September 2024].*

[15] *Ibid*

[16] *Ibid*

[17] *"Cyberattacks on Ukraine Increase Tenfold," 28 Mar 2022. [Online]. Available: https://evgenverzun.com/cyberattacks-on-ukraine-increase-tenfold/. [Accessed 01 Jan 2025].*

[18] *Ibid*

[19] *M. Burgess, "The Hacking of Starlink Terminals Has Begun," Wired, 10 August 2022. [Online]. Available: https://www.wired.com/story/starlink-internet-dish-hack/. [Accessed 22 September 2024].*

[20] *Ibid*

[21] *Ibid*

[22] *B. Toulas, "Ukraine: Hack wiped 2 petabytes of data from Russian research center," 26 Jan 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/ukraine-hack-wiped-2-petabytes-of-data-from-russian-research-center/. [Accessed 01 January 2025].*

[23] *Ibid*

[24] *Kyiv Post, (2024), "HUR Hacks Russian Defense Ministry, Gets Access to Classified Documents", URL: https://www.kyivpost.com/post/28979*

[25] *The New Voice of Ukraine, (2024), "Ukrainian cyber specialists disrupt Russia's drone control system in successful operation", URL: https://english.nv.ua/nation/cyber-specialists-of-the-hur-attacked-the-russian-drone-control-system-50391154.html*

[26] *"Ukrainian Hackers Launch Cyberattacks on Subsidiary of Major Russian Telecom," 28 April 2024. [Online]. Available: https://www.kyivpost.com/post/31798. [Accessed 01 Jan 2025]*

[27] *M. Fornusek, "Ukrainian cyberattack 'paralyzed' work of Russian ministries, companies, source said," 05 June 2024. [Online]. Available: https://kyivindependent.com/ukrainian-cyberattack-paralyzes-work-of-russian-ministries-companies-source-said/. [Accessed 01 Jan 2025].*

[28] *Ibid*

[29] *P. Paganini, "Ukraine's cyber operation shut down the ATM services of major Russian banks," 27 July 2024. [Online]. Available: https://securityaffairs.com/166214/cyber-warfare-2/atm-services-russian-banks-hacked.html. [Accessed 01 Jan 2025]*

[30] *Ibid*

[31] *OCCRP, "A Most Reliable Ally: How Corruption in the Russian Military Could Save Ukraine," 13 April 2022. [Online]. Available: https://www.occrp.org/en/feature/a-most-reliable-ally-how-corruption-in-the-russian-military-could-save-ukraine. [Accessed 05 December 2024].*

[32] *Ibid*

[33] *K. Denisova, "The Kyiv Independent," 04 March 2024. [Online]. Available: https://kyivindependent.com/military-intelligence-claims-cyberattack-on-russian-defense-ministry-gave-access-to-classified-documents/. [Accessed 05 December 2024].*

[34] *S. Magnuson, "Daily Fight for Ukraine Spectrum Superiority Puts Electronic Warfare Front, Center," 03 August 2024. [Online]. Available: https://www.nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center. [Accessed 01 December 2024].*

[35] *"Global Corporate Security," [Online]. Available: https://rgsscareers.ril.com/. [Accessed 02 December 2024].*

[36] *S. Yu, "Cognitive Warfare: A Psychological Strategy to Manipulate Public Opinion," [Online]. Available: https://www.igi-global.com/chapter/cognitive-warfare/332283. [Accessed 03 December 2024].*

[37] *"Software Testing: Trends Shaping the Industry-May 2022," [Online]. Available: https://www.nasscom.in/knowledge-center/publications/software-testing-trends-shaping-industry-may-2022. [Accessed 29 November 2024].*

[38] *"Russia's War Machine Runs on Western Parts," 22 February 2024. [Online]. Available: https://foreignpolicy.com/2024/02/22/russia-sanctions-weapons-ukraine-war-military-semiconductors/. [Accessed 02 December 2024].*

[39] *G. s. Ananya Raj Kakoti, "The new cyberspace doctrine's impact on India's security," 09 July 2024. [Online]. Available: https://www.hindustantimes.com/ht-insight/future-tech/the-new-cyberspace-doctrine-s-impact-on-indias-security-101720517961470.html. [Accessed 03 December 2024].*

[40] *"Sovereignty," [Online]. Available: https://cyberlaw.ccdcoe.org/wiki/Sovereignty. [Accessed 04 December 2024].*

[41] *Ibid*

[42] *Z. H. Z. K. Wang Peiwen, "Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security," [Online]. Available: https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security/. [Accessed 04 December 2024].*

[43] *"The art of deception: How Israel uses 'hasbara' to whitewash its crimes," [Online]. Available: https://www.trtworld.com/magazine/the-art-of-deception-how-israel-uses-hasbara-to-whitewash-its-crimes-12766404. [Accessed 01 December 2024].*

[44] *A. Chakravorty, "Explained: Why was the Sashastra Seema Bal force created?," 17 Feb 2016. [Online]. Available: https://indianexpress.com/article/explained/sashastra-seema-bal-ssb-news/. [Accessed 01 Jan 2025].*

[45] *A. Sharma, "Know Your Paramilitary | Part 5: SSB — India's Watchful Protectors at The Nepal And Bhutan Borders," 15 April 2022. [Online]. Available: https://www.news18.com/news/india/know-your-paramilitary-part-5-ssb-indias-watchful-protectors-at-the-nepal-and-bhutan-borders-4986169.html. [Accessed 28 November 2024].*

[46] *S. Sun, "IT industry in India - statistics & facts," 12 June 2024. [Online]. Available: https://www.statista.com/topics/2256/it-industry-in-india/#topicOverview. [Accessed 05 December 2024].*

[47] *"Indo-US Military Agreements," [Online]. Available: https://byjus.com/free-ias-prep/militaries-us-india-share-facilities/. [Accessed 01 December 2024].*

[48] *"Application of Software Defined Radio (SDR) in the Indian Defence Sector," 21 December 2023. [Online]. Available: https://www.hsc.com/resources/blog/software-defined-radio-applications-defense/. [Accessed 04 December 2024].*