Securing India's National Security in the Era of Grey-Zone Conflicts: Case of Cyber Warfare

Ms Poornima Balasubramanium[@]

Abstract

The international security scenario currently faces new and evolving nature of the conflict that teeters between war and peace. Tactics of grey-zone conflict have unfolded to be a major cause of concern that has left the states in limbo. The cyber domain has essentially become a fundamental tool used in such conflicts by virtue of the world being closely knit by networks controlled by cyberspace. The article assesses the kind and level of threat posed by cyber-centric grey zone conflicts to Indian national security and international stability.

Introduction

Cyber-attacks, misinformation campaigns and propaganda have

been occurring so rampantly in this era where communication and connectivity have been made digital to a larger extent. Cyber-attacks using tools such as ransomware and spyware have time and again demonstrated the damage they inflict on the target. State infrastructure and entities have of late become targets of these malicious cyber weapons. With cyberspace becoming a realm, cyber warfare will direct the nature of warfare and the characteristics that define it in the 21st century. What makes cyber warfare an issue of concern is that it falls in the grey zone between war and peace. Despite affecting state sovereignty and security (sometimes drastically), cyber warfare is not considered an act of aggression that provokes a war. While the cyber domain

has been used for its multifarious advantages, the flip side of its potential bodes much uncertainty for global and state security.

Grey Zone Conflict: Negative Peace?

Peace can either be seen as positive or negative peace. Positive peace guarantees sustainable stability and security. Negative peace warrants the absence of violence while tension and abuse continue to persist. This perspective avoids the simplistic view of peace that is built on the notion that "peace means the absence of war". Grey-zone conflict is an embodiment of the concept of negative peace. State and non-state actors use instruments such as political warfare, economic warfare, information warfare, cyber warfare among many others, in their conflict against their opponent without the involvement of armed violence. Meddling in the election process of another state to alter the outcome, imposing sanctions and trade curbs, propagating fake news that can be detrimental to a state's public image are some of the means through which conflict in the grey zone has been evolving. Grey-zone conflict can be defined as: "The process of conflict-induced change is known as grey-zone conflict, in which states conduct operations that only occasionally pass the threshold of war."[1] The impact is profound but just not enough to pass *Jus ad bellum,* the criteria to be considered before waging a war. The concept of *Jus ad bellum* was introduced in International Law during an era when only conventional tactics of warfare were mostly practised and posed critical security risks to international security. With the evolution of the nature of warfare, the loopholes in the laws governing warfare have been widening. This very lacunae in international law, which does not address facets of grey-zone conflict, is being exploited by state and non-state actors. Donning a double-edged sword, cyberspace is a capable means of grey-zone conflict. Its dynamic nature needs to be appraised to gain a better perspective of the threats it poses to state security.

The Vagaries of Cyber Warfare

In today's world, technology is power. At the same time, information is also power. Whosoever controls these can effectively exercise power over the international system.

Cyberspace uses technology that disseminates information from one end of the globe to another. Advances in the Industrial Revolution 4.0 such as robotics, artificial intelligence, and cloud computing — with every digital service steered by the Internet of Things — have further opened new avenues to manoeuvre cyberspace, giving it the key to potentially penetrate the structures of society.

Cyber Threats to Critical Infrastructure

The network of Critical Information Infrastructure (CII), which ensures that the functioning of a state is carried forward, is mainly connected through cyberspace. The security of the CII is of paramount importance for the state as its national security hinges on these infrastructures to a greater degree. A disruption caused in the network even for a short period could cause chaos as it can impede services such as transportation, communication, and power. The CII in any state is protected by multiple layers of physical safeguard protocols. However, since these infrastructures are inter-linked in cyberspace to connect to a central command, they are rendered vulnerable to cyberattacks. Several attempts have been made to attack the CII of states. Most of these attacks are identified post execution when considerable disruption has already been caused. Tracing the origin of these attacks is also a task for which not many states are equipped.

Highly sophisticated cyber technologies like malware and spyware can be deployed on any Programmable Logic Controller (PLC) device and once installed, they can reprogram and command the entire system.[2] States have been at the receiving end of threats such as data mining traps, sabotage campaigns, cyber espionage that have been frequently endangering their security. Yet, these kinds of attacks do not attract physical retaliation because of their asymmetry and covert nature. Reports show that states like the US, China, Russia, Israel and Iran have been using the cyber domain, both for their offensive and defensive operations in the grey zone.[3] Miriam Howe, a Cyber Security Consultant at BAE Systems, opines: “A characteristic of the grey zone is the inherent uncertainty and deniability of operations in cyberspace- the ability to remain covert, difficulties in attribution, false flags and deception often means the absence of

a smoking gun".[4] The capability of cyberspace in grey-zone conflicts and of it being unpredictable but crippling has been demonstrated a number of times in the recent past.

- **The Stuxnet:** The Stuxnet worm was a product of the US-Israel collaboration to develop a weapon to disrupt Iran's nuclear program without the use of conventional forces. The idea developed in the early 2000s and "Operation Out of Box" was executed in 2010 on the Iranian nuclear enrichment facility in the Natanz region.[5] Cyberweapons work with a similar concept as a conventional missile. They consist of two parts: the delivery system and the payload. In a cyber weapon, the delivery system delivers and distributes the code or the cyber payload to the target system. The code (payload) then infiltrates the system and reprograms it, steals, and transfers data and also destructs the system.[6] The Stuxnet worm is deduced to have probably infected the computer system through an "infected USB" (the delivery system). After getting inside the system, the worm (cyber payload) got access to the control system of the centrifuges of the nuclear reactors. After gaining control, the worm re-programmed the centrifuges. It executed two different patterns of attacks for several months together. One, it drastically increased the speed of the centrifuges for 15 minutes and set it back to the normal speed. After a month or so, it reduced the speed of the centrifuges down to 50 minutes. The erratic speed patterns caused the centrifuges to disintegrate, and it brought the need for 20% of the reactors to be decommissioned. Within months, the Stuxnet could infiltrate into a "supposedly" air-gapped control system of a nuclear plant and delayed the progress of the program.[7] Stuxnet is the first known worm to "target and infiltrate industrial Supervisory Control And Data Acquisition (SCADA), a software that is used to run chemical plants as well as electric power plants and transmission systems."[8] Owing to its covert and uncertain nature, it took almost a few years for Iran to identify the malware and its place of origin. The ambiguity in the character of the attack failed to testify whether the attack tantamounted to an act of aggression

under *Jus ad bellum,* although it violated Iran's sovereignty and revealed the vulnerability of the state.

- **BlackEnergy 3:** In 2015, the Ukrainian Power Grid came under a cyber-attack. The outage plugged the eyes of nearly 30 substations and left 2,30,000 citizens in darkness and cold as the electricity that powered the lights and heaters was cut off through a few mouse clicks. Hackers sitting elsewhere were able to control the cursor in an operating system in the main station that allowed a program to be activated in the system, eventually shutting down the electricity. Further, they were able to sever the backup power supply of two power distribution centres. In few weeks, the hackers had managed to trap the systems through spear-phishing and gained backdoor entry into them. The control systems of the power grid were supposed to be much more secured than the systems in the US but unfortunately, they fell short of securing the system enough to have a resistant SCADA network, which was remotely penetrated with ease.[9] The attack was reported to be orchestrated by Russia with the support of criminal networks against Ukraine as part of the long-drawn conflict between both states. The infamous Russian hybrid warfare strategies also incorporate grey-zone cyber warfare tactics.

Cyber-Information Warfare

Cyberspace has been proficient enough to propel misinformation campaigns that could influence the thoughts and opinions of people. Misdirecting narratives can impact the political and social stability of the states. Fake news and propaganda are being circulated on social media platforms and unfortunately sometimes, even in mainstream media. The erroneous generation and promotion of uncontrolled and unvetted news have affected society's thought process making them susceptible to the cons of the post-truth era.

Information warfare is indeed a threat to the interests of states as domestic and international opinion matters much for states' impression and stature in the international community. Nevertheless, states have been unable to confront cyber-information warfare in its entirety because of the ubiquitous nature

of cyberspace. This issue demands to be tackled by the erudite employment of public diplomacy, awareness campaigns and other defensive methods and not by violent retaliation. Such is the nature of the grey-zone conflicts.

A Bird's Eye View into the Indian Scenario

As emphasised before, grey-zone conflicts have changed the notion of warfare and have now become an indispensable aspect of the conflict between and among state and non-state actors. India, like any other fast-developing state, encounters this threat. This is partly due to the dicey geopolitical environment it is a part of. India has been facing thrice the average number of cyberattacks that are affecting the world. A lot of these have been found to have their source in Pakistan and China.

The attempted attack on the control systems of the Kudankulam Nuclear Power Plant in the state of Tamil Nadu in 2019 is a classic example. The DTRACK malware penetrated the administrative computer of the plant and had taken information stored in the system. Although in this case only the administrative system was targeted, there were possibilities of a control system being attacked like in the case of Stuxnet. The ramification would have been detrimental as a nuclear leak could have harmed the people and the environment. The psychological impact of the Kudankulam attack had mobilised political parties and activist to call for the shutting down of the Plant, which would have a drastic impact on India's energy needs in the future.[10] Though the attack was attributed to a North Korean company, Lazarus Group, connections to any state actor was not established.

The Cyberthreat World-time Map reports that India is the seventh most attacked state in the cyber realm. According to the Indian National Security Council Secretariat report of 2018, 35% of India's cyberattacks are of Chinese origin. Though high-impact attacks targeting CII have not taken place, there have been constant attempts at espionage and theft of sensitive data from government and private enterprises. One report even accused China of using the Stuxnet worm to disrupt India's communication satellite.[11]

For a major power like India, threats from states, especially its neighbours and the non-state actors they support, are a plethora. More so, Pakistan has been relying on cyber warfare as one of the efficient tools that would, on one hand, disrupt the functioning of the state and on the other, not escalate the conflict. Apart from this, the rounds that fake news and propaganda materials originating from Pakistan have caused a deep dent in Indian politics and society, furthering the divide between people. Many shreds of evidence have been provided that proves the involvement of external sources in funding and proliferating such influence campaigns that work against the state. Social network platforms have been used prevalently for this purpose where different cyber tools enable the circulation of these messages that it reached every corner of social media. Following is a small excerpt of one such incident:-

> "The 2013 riots in Muzaffarnagar (UP) were aggravated by the use of social media networks by suspected terror groups. On 21 November 2013, the then Home Minister Sushil Kumar Shinde had observed, "More recently, the Muzaffarnagar riots were fanned by similar misuse (of social media)." There is mounting evidence that the abuse of the Internet against India is substantially orchestrated under the aegis of Pakistan's external Intelligence agency, the Inter-Services Intelligence (ISI). A classified note of a high-level security review meeting held in New Delhi in September 2012, noted, "The ISI is now working on a bigger game-plan in training terrorists in the use of cyber and computer technology as the Pakistani agency feels India is not fully equipped in dealing with incidents of cyberwar or attack." Importantly, the note observed, the training is given to subversive elements by ISI's cyber experts played a key role in spreading hate campaigns through MMS and SMS, targeting people from the Northeast in the wake of ethnic violence in Assam. The note warned that this trend would only increase in days to come, and this was also the reason why ISI was increasingly stressing the recruitment of more educated youth by Islamist terrorist formations. An unnamed Indian intelligence officer stated, further, "It is almost certain that the Pakistani agency was behind the recent cyberattack

> on India, at least indirectly. Having tasted success, they will try it again in future and on a much bigger scale. So, we must be prepared to deal with this challenge."[12]

After the abrogation of Article 370 from the constitution of India, a surge in the volume of cyberattacks was observed from Pakistan, with several fake accounts that were created to swiftly circulate fake news, videos, and morphed photographs to instigate unrest in Indian society. The cyber domain has been a tool for Pakistan for its psychological operations against India, to shape the opinion of the people in both the states and worldwide. Such information warfare could tarnish India's image and credibility at the domestic as well as international level. Challenges to India's diplomatic manoeuvrability have arisen out of misperceptions and deceptive information that is propagated through social networking platforms. Cyberspace has been immensely used to bolster propaganda by manipulating algorithms and DDoS capabilities.[13] Though India has been largely successful in overcoming the war of narratives with Pakistan, it leaves behind stains that can hamper India's national interests, thanks to the grey-zone nature of cyberspace.

The Way Ahead

The absence of international norms and laws that adequately govern the manifestations of grey-zone conflicts, especially cyber warfare, has the potential to extremely affecting state security. More so, in a complexly interdependent world that makes wars costlier, states will increasingly invest in capabilities that help them in grey-zone conflicts. Cyberspace will be a conducive battlefield towards that end. Irrespective of the defensive capabilities a state possesses, the uncertainty that cyber warfare produces in the grey zone will be a hard challenge to confront in the future. The threat has already started to loom, and it is important that states, including India, need to be aware of the intricacies of conflicts of such kind. States need to come together to be aware of the nature of such threats as well as cooperate to bring about institutions and regimes that bring clarity by removing the greyness of this zone and build confidence among the states. Collective action can bear fruit, apart from securing one's national security, in keeping the threat under control.

Over the years, India has been building its defence against cyber warfare by instituting various laws, organisations, and regulations as part of its digital revolution. India has also been in active collaboration with states like the United States and Israel to share best practices and participate in joint training initiatives to fortify itself in the cyber domain. Despite these measures, cyberattacks have been a grave threat for India. The National Cyber Security Strategy is a good head start. It aims at bolstering India's overall cyber defence capabilities that will equip the state to be resilient in cyberspace. However, effective implementation of the strategy is imperative, which demands the investment of resources including finance as well as human capital. India must also counter the narratives that are mobilized against it, especially during sensitive times such as now, during the pandemic. This can be done mainly through connecting with its people and those abroad and raising awareness about the grey-zone threat. The mainstream media, for instance, can keep people informed about the dangers of fake news and help them build resilience towards such peril. In this conflict, the general public is the first line of battle. A resilient society will eventually show zero porosity for disinformation.

Conclusion

Cyber warfare and cyber-information warfare portend an era where the deniability of such means of warfare can be used by state and non-state actors against their targets while leaving the conflict in the grey zone. The ramifications of such assaults can be irreversible or at the least, extremely hard to recover from as they target high-value national assets including the CII as well as information, the new-age oil. Advancements in technology can lead to mutation and thereby, to the evolution of the nature of the grey-zone conflict. Such advancements can simultaneously be used to develop defensive walls that can preserve the security of a state as well as the international system. The hazards of cyber warfare in the grey zone linger even as the Covid-19 crisis has kept the world reeling. At this crucial juncture, India must not lower its guard and prepare to face the future of warfare in the grey zone as it treads the path in its pursuit of power and progress.

Endnotes

[1] David Carment and Dani Belo, “War’s Future: The Risks and Rewards of Grey-Zone Conflict and Hybrid Warfare”, *Canadian Global Affairs Institute,* Policy Paper (2018).

[2] Robert Mcmillan, “Was Stuxnet Built to Attack Iran’s Nuclear Program?”, *IDG News Service* (Boston), September 21, 2010, https://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html.

[3] Abhijit Ahaskar, “How Cyberattacks Are Being Used by States Against Each Other”, *LiveMint,* June 21, 2019, https://www.livemint.com/technology/tech-news/how-cyberattacks-are-being-used-by-states-against-each-other-1561100711834.html.

[4] “Competition and Conflict in the Grey Zone: Government Insights”, BAE Systems, accessed 15 June, 2021, https://www.baesystems.com/en/cybersecurity/feature/competition-and-conflict-in-the-grey-zone.

[5] Nicole Perlroth, “Researchers Find Clues in Malware”, *The New York Times,* May 30, 2012, https://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

[6] Kartik Bommakanti, “The Impact of Cyber Weapons on Nuclear Deterrence: A Conceptual and Empirical Overview”, *ORF Issue Brief,* n. 266, 2018.

[7] “How Stuxnet Attacked a Nuclear Plant,” BBC, accessed June 15, 2021, https://www.bbc.com/timelines/zc6fbk7.

[8] Mark Clayton, “The Stuxnet Malware Is Weapon Out to Destroy Iran’s Bushehr Nuclear Plant?”, *CS Monitor,* September 21, 2010, see website https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.

[9] Jose A. Bernat, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid”, *Wired,* March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[10] Stephanie Findlay, “India Confirms Cyber Attack on Nuclear Power Plants”, *Financial Times,* October 31, 2019, https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6.

[11] Elizabeth Radziszewski, Brendan Hanson and Salman Khalid, “India’s Response to China’s Cyber Attacks post- Kashmir Decision”, *LiveMint,* August 19, 2019, https://www.livemint.com/news/india/india-sees-dramatic-rise-in-cyber-attacks-post-kashmir-decision-1566217795883.html.

[12] Sanchita Bhattacharya, “Cyber Wars”, *Outlook,* November 20, 2014, https://www.outlookindia.com/website/story/cyber-wars/292633.

[13] Shashank Shekar, “Pakistan Bots Wage Cyber Warfare”, *msn,* August 12, 2019, https://www.msn.com/en-in/news/newsindia/pakistan-bots-wage-cyber-warfa/re/ar-AAFHyyy.

@**Ms Poornima Balasubramanium** is a PhD research scholar at the Department of Geopolitics and International Relations, Manipal Academy of Higher Education, India. Her research interests include Conflict analysis, Indian Foreign Policy and National Security, Geopolitics of West Asia.

Journal of the United Service Institution of India, Vol. CLI, No. 624, April-June 2021.