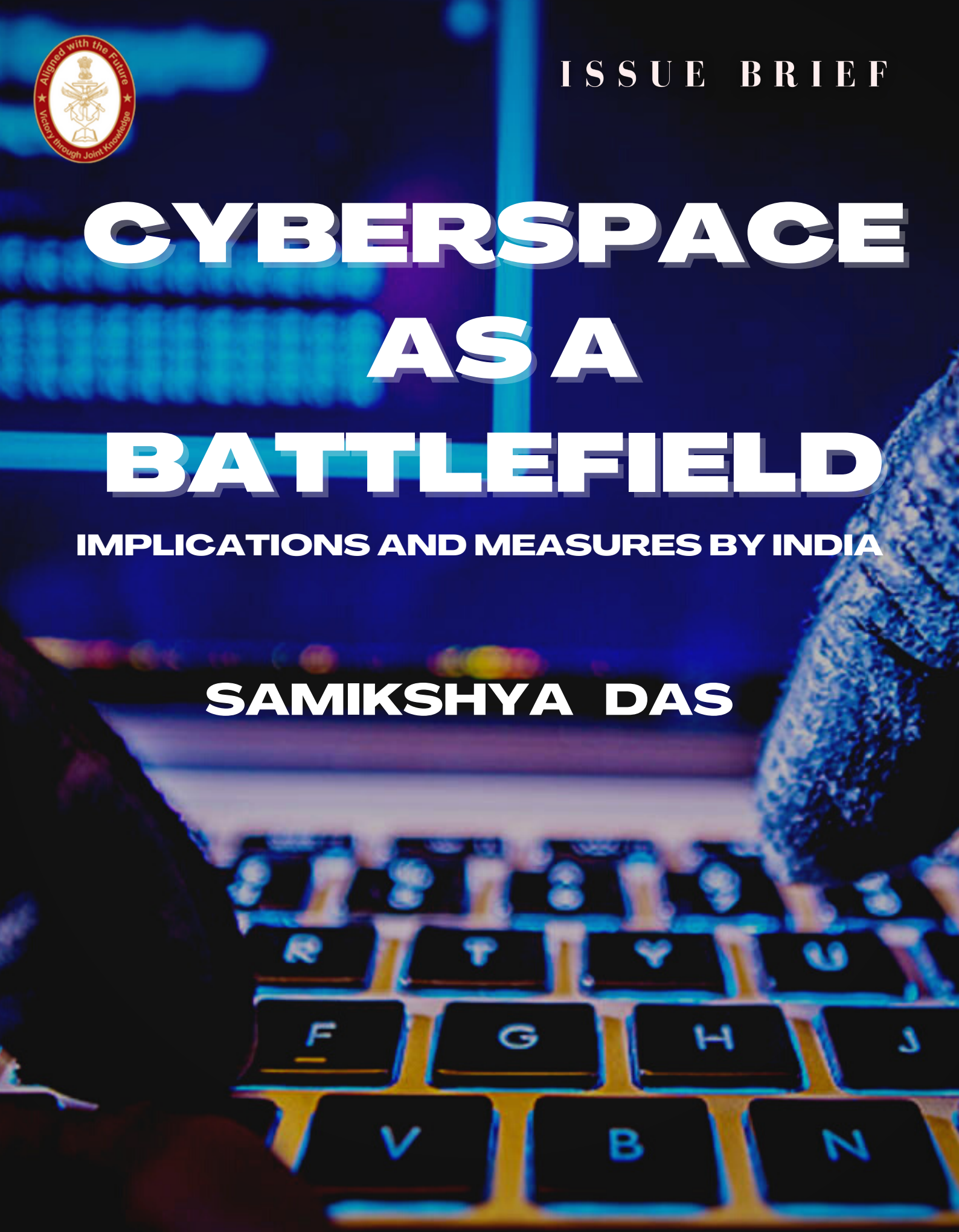
ISSUE BRIEF

# CYBERSPACE AS A BATTLEFIELD

## IMPLICATIONS AND MEASURES BY INDIA

SAMIKSHYA DAS



WWW.CENJOWS.IN

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

# CYBERSPACE AS A BATTLEFIELD: IMPLICATIONS AND MEASURES BY INDIA

**Ms Samikshya Das**, has completed her graduation in law and now pursuing her Master's in International Studies from Symbiosis International University and an Advanced Post-Graduate Diploma in Cyber Security laws from NALSAR University.

**Abstract**

The information age has changed society by enabling digital interaction, but it also makes it possible for certain individuals to employ mass influence to achieve their political goals. Understanding how a disinformation impact might be created is necessary to combat it in the fight against misinformation. Before exploring the issue via the lenses of the planning method, systems thinking, and military strategy, in this paper, we analyse the nature of cyber operations worldwide and their usage in the hybrid warfare environment. Governments and non-state organisations have been striving for dominance in cyberspace for the last twenty years. Political and military figures have made incredible assertions about the potential of these new weapons, and cyber weapons have been used in conflicts. However, we have yet to see a powerful state fully use its cyber capabilities.

Some countries are more prepared and ready than others in terms of cyberspace, cybersecurity, and the creation of national cybersecurity policies. These important countries have recognised the necessity for international cooperation and alliance formation to combat cybercrime, govern the internet, and improve cybersecurity strategy information.

In this paper, we are discussing the role of non-state actors in the cyber warfare scenario. While some people operate alone, others are a member of hierarchical organisations or unofficial networks. Depending on the situation, the positions could potentially shift or overlap. Actors may move between different categories depending on their current goals and intentions. Non-state actors engaged in cyberwarfare have grown, including hacktivists, hackers, spammers, botnet operators, terrorists, radicals, or criminal organisations that employ these players to further their objectives.

Pakistan's cooperation with China deepens its strategic alliance and gives Islamabad's cyber operations the technological edge they would not otherwise have. India has also made strides to fix its cyber vulnerabilities through various institutional and legislative measures in recent years. China is thought to be Asia's most comprehensive and experienced cyberwarfare capability. However, Chinese and Pakistani hackers continue to prey on the average Indian Internet user's lack of cybersecurity awareness and poor cyber security practices, such as failing to confirm the integrity of fake news and clicking on unsolicited web links, to infect vulnerable computer networks and spread their malware.

Due to the global character of cyber threats, countries, even developed countries and intergovernmental organisations, need to be active in the policy-making process for cybersecurity, and it should be a collaborative effort. This paper discusses the cyber risk assessment and level of preparation of India concerning the danger its neighbours pose in the virtual domain.

## 1.Evolution of Cyberspace

Cyberspace has existed for decades now. Human beings made it to simplify some processes, but lately, the meaning and use of this term has changed a lot. The phrase "cyberspace," which combines the terms "cyber(netics)" and "space," originally appeared in a science fiction work. The recently used version of the word first emerged in a 1948 book by mathematician Norbert Wiener to define the study of command, control and communications in the mechanical world. The word originates from the Greek kybernetes, which means one who steers or governs.[1] In this context, space means an infinite-dimensional expanse in which incidents

occur and is inherently different from the physical world. Cyberspace is made up of all computerised networks in existence as well as all endpoints that are linked to them and subject to orders that go via them.

The cyberspace is digital as well as physical. There are four layers of cyberspace- first, the physical layer that includes the infrastructure meaning the computer or the devices; second, the logical layer that includes the internet, software packages etc.; the third is the information layer which includes the web content, tweets etc. and last is the user layer which includes the human beings who participate in the cyber activities.[2] When we talk about controlling cyberspace, it means influencing or manipulating these layers in certain ways. For instance, the physical layer can be controlled by acquiring control over the infrastructure through physical or digital access. The Information layer can be controlled by manipulation of information or circulating fake news. Control of the logical layer means reconfiguring the rules of the system's operation, and control of the user layer means convincing the user of an alternate reality.[3]

The term 'Cyber' has led to the use of many new phrases, like cyber warfare, cyber conflict, cyber attacks, cyber-attacks, etc. A nation-state or international organisation may engage in cyber warfare by attacking and attempting to harm another country's computers or information networks using methods like computer viruses or denial-of-service attacks. Cybersecurity is the defence against harmful assaults by hackers, spammers, and cybercriminals against internet-connected devices and services. Cyber power is a society's organised capacity to use digital technology for snooping, exploitation, subversion, and coercion in international warfare. Cyberattacks are efforts to compromise computer systems, steal data, or start new attacks by disabling machines.[4] It is a malicious and intentional attempt by a person, group, or State-sponsored organisation to access the information system of another person, group, or State. Cyberattacks are not only expanding geometrically but also taking on increasingly deadly dimensions. If emerging technologies like artificial intelligence (AI), cloud computing, or 5G are helping everyday people, then the risks are rising in direct proportion to the advancements in convenience.[5] It is important to pay attention to the evolving patterns of cybercrimes and threats, which are not simply the activity of lone hackers or groups of hackers, but also of adversarial States.

The number of phishing cases has significantly grown since the start of the pandemic. Cybercriminals are using the epidemic narrative to spread panic and dupe people into giving them access to private data. The adoption of cloud infrastructure has given hackers various chances.[6] The corporate world has altered its system due to increased workers working from home on their own devices and the rapid uptake of cloud computing to assist the workforce, which gives these cyber criminals convenient chances. Significantly, cybercriminals use cloud infrastructure flaws that let them attack several targets using a single vulnerability at once.[7]

Cyber espionage tools such as the Pegasus spyware have become more potent and hazardous due to the rise in mobile device usage. Additionally, it is possible to utilise tools to break into mobile devices to secretly record audio or take photographs without the owners' knowledge. Some smartphones include built-in backdoor mechanisms as well. Trojans and viruses for mobile devices include the Trida, MasterFred, and FlyTrap. These mobile Trojans use similar methods to access target devices and obtain the required rights, such as social media, lax app store security measures, etc. It is also apparent that supply chain assaults have increased. These can happen when hackers identify a weak point or many weaknesses in an organisation's ecosystem, particularly through third-party systems.[8] The quick increase in digitisation, the development of remote labour, and the increasing number of linked gadgets are the main drivers of this.

Since around two decades ago, governments and non-state organisations have been competing in cyber domains. Political and military leaders have made astounding claims about the potential of these new weapons, and cyber weapons have been used in small-scale wars. However, we have yet to witness a large state use its cyber capabilities fully. A large-scale nuclear assault would be significantly more damaging than a cyberattack on key infrastructure. Additionally, the attacker's confidence in the capability of a cyber strike to cause catastrophic damage is probably far lower than that of an attacker using a huge number of nuclear weapons.[9]

## 2. Cyber Strategies of Different Countries

Some nations are more streamlined and prepared than others regarding cyberspace, cybersecurity, and the development of national cybersecurity strategies. These key nations have acknowledged the need for

international collaboration and alliance development to combat cybercrime, rule cyberspace, and knowledge transfer regarding cybersecurity strategy issues.[10] The United States is the only nation in the top tier since it is thought to have advantages across all metrics. The W. J. Clinton administration only prioritised cyber risks towards the end of the 1990s. Much later, in an effort to combat online threats, the Obama administration tried to put deterrence measures into place. The new CYBERCOM, established as a component of STRATCOM, served as the overall organisation to thwart cyber attacks.[11] The US took a two-tier approach to the cyber security issue. The first prioritised information exchange while forging ties with the public sector and forming international alliances. The second tier prioritised defending and protecting its system and American interests. The US stands out due to its digital industrial base, cryptographic know-how, and capacity to launch sophisticated and precise cyberattacks against adversaries.[12] The US government has also been investing a lot in the human resources of this cyber field.

Australia, Canada, China, France, Israel, Russia, and the United Kingdom are among the nations in the second tier due to their global leadership in certain areas. India is in the third tier, which indicates that the nation has some major shortcomings in certain areas but has potential strengths. Japan, Iran, Indonesia, Vietnam, Malaysia, and North Korea make up the other tier 3 nations. It should be noted that nations like Israel and Australia have developed cutting-edge cyber capabilities, while historically strong nations like Japan and India have fallen behind. States with a history of offensive cyber activities, such as online espionage, intellectual property theft, and defamation campaigns, including China and Russia, have lagged behind the US. According to The International Institute of Strategic Studies (IISS), China's cyber intelligence analysis was relatively less developed than the US, UK, Canada, Australia, and New Zealand. According to the study, this was mostly related to its lax security and inadequate intelligence analysis. The majority of evaluations in this regard are based on seven criteria: offensive cyber capabilities, global leadership in cyberspace affairs, Strategy and doctrine, governance, command and control, core cyber-intelligence capability, cyber empowerment and dependency, and cyber security and resilience.[13]

Israel has a well-known cyber defence and is the world's second-largest exporter of products and services after the United States. It has become

one of the top cyber security powers in the world.[14] Geographically, Israel is a small country, and nations surround it with complicated bilateral relations, so it developed its cyber creativity to compensate for its lack of resources. According to Israel, it is a country that needs constant surveillance of its neighbours as it is under constant threat. Unit 8200 is an elite cyber and intelligence division of Israel's defence.[15] Israel, along with the National Security Agency (NSA) of the US, is rumoured to be responsible for the most aggressive cyber-attack in history, Stuxnet. This attack sabotaged the Iranian nuclear program by destroying centrifuges at the Natanz nuclear facility in Iran.[16] By adopting the National Cyber Initiative and protecting the country from cyberattacks, Israel became the hub for information technology. Moreover, by enhancing collaboration between the government, academia, industry, private sector, and security community, Israel's cybersecurity policy was established to place Israel among the top five global superpower nations.[17]

In foreign and security policy, the European Union has been extending its responsibilities to encompass cybersecurity, where it plays a crucial role. The EU wants to standardise cyberspace operating laws and foster closer ties among its member states, NATO, and other international organisations. In 2020, the EU unveiled a new European Union Cybersecurity Strategy. The Strategy addresses the security of critical infrastructure, including railways, hospitals, energy grids, homes, and offices. In order to maintain global security and stability in cyberspace, it also emphasises the collective capacity to respond to major cyber attacks. It describes how a Joint Cyber Unit may respond best to cyber-attacks by pooling the resources and knowledge that the EU and the Member States offer and working together with all other entities.[18]

In contrast to the Western Strategy, Russia has embraced strategic deterrence as a doctrinal approach that uses a broad range of weapons and tools. The Russian conception of strategic deterrence is significantly more comprehensive, incorporating both offensive and defensive postures, spanning both nuclear and non-nuclear dimensions, and utilising a variety of non-military deterrent instruments. Since 2014, the Russian Federation's military policy has strongly emphasised the use of information technology and information security for military, political, diplomatic, military-technical, and economic purposes.[19] Russian cyber warfare has included hacking assaults, denial-of-service attacks, the spread of

propaganda and misinformation, the involvement of state-sponsored teams in political blogs, internet surveillance using System for Operative Investigative Activities (SORM) technology, the repression of online dissidents, and other active measures. As part of their cyber warfare against other nations, the Russian security services are alleged to have organised several denial-of-service attacks, including the cyberattacks on Estonia in 2007 and the cyberattacks on South Ossetia, Georgia, and Azerbaijan in 2008.[20]

The current Russia-Ukraine crisis can be discussed in this regard. It was anticipated that Russia would utilise cyberattacks as part of its campaign, since the beginning of the Russian invasion of Ukraine in late February 2022, with infrastructure destabilisation as a desirable target. Several infrastructure components of the assault target were decommissioned as a result of the attack. During the early hours of the invasion, hackers disabled tens of thousands of satellite internet modems across Ukraine and around the eastern European region. It continues to rank among the largest publicly acknowledged cyberattacks during the conflict.[21] Following the invasion, Russian hackers violated the security of several crucial Ukrainian enterprises, including nuclear power plants, media outlets, and governmental bodies. During the conflict, Ukraine turned to its hacktivists for assistance in defending itself against Russia. Since then, a continuous stream of unidentified, anonymous hacktivists from both sides has gone to social media, claiming to have successfully penetrated either Russian or Ukrainian targets. The hacktivists have occasionally shared images or caches of documents to support their accusations, but it has been impossible to confirm or quantify their behaviour.[22]

Although many countries have already implemented or are planning to implement a national cybersecurity strategy, very little effort is focused on the contribution of international cybersecurity standardisation, defining jurisdiction in international cyberspace, or the contribution from developed countries to help developing countries establish a uniform cybersecurity programme, policy, or strategy.

### 3. Role of Non-State Actors

Virtually everyone with access to a computer and an internet connection, a smartphone, or any other uplinked multimedia device has access to the global world of cyberspace. In this area, several distinct players coexist,

each with their wants, objectives, and intents. Some people work alone, while others participate in informal networks or hierarchical institutions. The positions might also change or overlap depending on the circumstance. According to their present objectives and purposes, actors may transition between several categories throughout time. There has been an increased number of non-state actors involved in cyber warfare, such as hacktivists, hackers, spammers, botnet herders and terrorists, radicals or criminal organisations hiring these players to execute their goals. For example, the defacement of a Kosovo-Albanian website and the threat to attack NATO's military computers by a gang of Serbian-based nationalist hackers known as 'Black Hand', named after the Serbian military organisation from before World War I, was referred to as "the first Internet war."[23]

The term hacktivism can be explained as the exploitation of online resources, either legally or illegally, to further a political or ideological cause, an ideology, or just for general protest. Hacktivism may also be employed covertly to further covert political, military, or economic objectives. Some hacktivists utilise website defacements, internet resource redirection, denial-of-service assaults, information theft, website parodies, virtual sit-ins, and other types of cyber sabotage. Hackers are those who have a profound understanding of computer technology, including how networking, software, and hardware function together. They frequently worry about operating systems, algorithms, and system setups. They could be driven by a wide range of motives, including curiosity, financial gain, political objectives, a desire for intellectual challenge, or just plain boredom. The malicious forms of hackers known as "crackers" are known as "black-hat hackers." White-hat hackers, often known as "ethical hackers," are cybercriminals who uphold high moral standards compared to accepted social norms. Gray-hat hackers are the ones in between both the categories mentioned above.[24]

Patriot hackers take out various disruptive activities in cyberspace targeted against the State's adversary to promote or assist their nation-state in an ongoing real-world battle or war. Patriotic hacking has historically been a particular strength of Chinese hackers.[25] An active hacking community of Russian nationals has also been noticed during the denial-of-service attacks launched against Estonia in 2007, following the controversy surrounding the relocation of a Soviet-era war memorial, and once more in

2008, when Georgia was the target of similar attacks in conjunction with a conventional military conflict with Russian forces.[26]

Moreover, extremists that utilise heinous acts of violence against the defenceless or massive destruction of public property to advance their political or ideological objectives are known as terrorists. Cyberterrorists are the ones who carry out their assaults and instil fear in public by using a computer and network technology. In some ways, organised crime in cyberspace may be considered the virtual equivalent of its counterpart in the real world. However, the borderless and anonymous character of cyberspace enables previously unconnected people in many regions of the world to unite and create criminal networks with a common objective or interest.[27] Then, some agents engage in cyber espionage. They exploit the internet resources of an adversary nation to gather intelligence for their country. By employing hacking and infiltration tactics, software and hardware surveillance tools, or other similar methods, they intercept information that travels through or is stored in computer networks or computer systems of particular interest. The information obtained is examined and used to create intelligence reports for the commissioning organisation. Cyber espionage may also involve gathering and analysing publicly accessible open-source data from websites or social media platforms like Facebook, Twitter, blogs, discussion boards, and forums.[28] A distinction that can be drawn between cyber espionage agents and other actors, such as cybercriminals, is that the former act lawfully or with the tacit approval of a sponsoring nation-state, at least in relation to that State's laws. This distinction can be made regardless of whether the purpose of cyber espionage is military, political, or economic. According to certain perspectives, monitoring an adversary's cyber capabilities is crucial for maintaining national security, and cyber espionage is seen as an integral component of the global economic battle. Cyber espionage agents can work independently, as rogue entities, despite being frequently linked to national intelligence agencies, military units, or other groups connected to nation-states.[29] Operation Shady RAT is undoubtedly one of the largest cyber espionage instances in history, as it has impacted more than 70 businesses and organisations since 2006. The International Olympic Committee, which was compromised in the months leading up to the Olympic Games in Beijing in 2008, was one of the victims. The United Nations and the World Anti-Doping Agency were also targeted. Cyber terrorists gained authorised access to legal agreements, state secrets, and

other private information. It was alleged that Chinese hackers orchestrated the operation since all of the Southeast Asian nations except China were hit by these attacks.[30]

Apart from this, there have been many individual attacks on nations and citizens by these non-state actors. The NotPetya assault, which caused more than $10 billion in damage in 2016, affected targets worldwide in waves that lasted for more than a year. The WannaCry ransomware outbreak impacted more than 300,000 systems in 150 countries in 2017, which cost billions of dollars in damages. Following a prior assault that revealed the personal information in 500 million user accounts, Yahoo's data breach event jeopardised the accounts of 1 billion users. In July 2020, Twitter was breached by a group of attackers who seized control of well-known Twitter accounts. They employed social engineering tactics to acquire employee passwords and access the business' internal management systems, which were ultimately labelled as vishing attempts by Twitter, which means phone phishing.[31]

Although most of these online wars involve non-state actors, they are attracting the attention of those who want to use them to advance their agendas. Cyberconflicts can be considered a reflection of their counterparts in the real world. Now, this new environment has more distinct disagreements, skirmishes, attacks, and even possible acts of war. Even though many non-state actors are typically involved in cyber actions, there is presently no legal definition of cyberwarfare or consensus on what constitutes an "act of war" in cyberspace; the overlap between these actor categories and authorised state-backed cyberwarriors is a real cause for worry.[32] Additionally, it is doubtful that such norms will appear anytime soon, opening a window of opportunity for actors with minimal resources who cannot win on a violent battlefield.

### 4. Cyber Warfare by China and Pakistan

China is considered to be Asia's most comprehensive and experienced cyberwarfare capability. Since 1997, China has performed a number of exercises in which computer viruses have been deployed to disrupt military communications and public broadcasting systems. China started implementing information warfare (IW) plan in 1995. In order to "wage battle using computer networks to influence enemy information systems

spanning spare parts delivery to fire control and guidance systems," China developed a strategic IW unit in 2000. On July 20, 2010, the People's Liberation Army (PLA) declared that the General Staff Department now houses an "Information Protection Base."[33] It is most likely a computer network defence or computer security operation. The PLA IW units have created extensive procedures for Internet warfare, including malware, information-paralysing software, information-blocking software, information-deception software, and other malware, as well as software for enacting countermeasures. Since around the 2000s, these processes have been put to the test in real-world scenarios. China is responsible for the majority of cyberattacks and is largely driven by a desire to obtain access to secrets and use such assaults to further its political goals. According to reports, the PLA engaged in hacking activities to acquire government secrets, destroy public utilities and services, and gain access to business secrets, particularly in developing technologies.[33]

China adopts an integrated strategy for information warfare operations encompassing electronic warfare (EW), computer network warfare, and psychological operations as Integrated Network Electronic Warfare (NEW). By 2025, China wants to be a worldwide internet giant with unbreakable cyber security. By including cyberattacks on satellites or space warfare in its offensive operations, China has raised cyberwarfare to a strategic level.[34] It is reasonable to presume that the PLA plans to carry out operations simultaneously in each of the five operational domains—land, sea, air, space, and cyber. China engages in ongoing cyber reconnaissance to find vulnerabilities and gather data that may be used against enemies in conflict by targeting the information infrastructure of vital services, including banking, telecommunications, power, water, and sewage systems.[35] In 2010, Google said that a number of cyber attacks took place, and these threats originated from China. In addition to Google, hackers targeted more than 20 foreign businesses, including Adobe Systems and Yahoo. Google said that both its intellectual property and Gmail accounts were constantly threatened. Then in 2012, the Chinese government hackers reportedly hacked into the American Office of Personnel Management and stole the personal data of 21 million citizens. This cyber espionage gave them access to private information on those who sought or had jobs with the federal government, including military service. The long-term effects of this data breach are yet unknown, despite the assurances of the executives of OPM that nobody was harmed due to

the hacker infiltration. There are many other instances where such cyber attacks took place, and allegedly all of them originated from China.[36]

In 2007, Pakistan passed the Electronic Crime Ordinance to establish tight guidelines for the use of networks. Patriotic programmers and hackers from Pakistan seek to use the internet to target their adversaries, particularly when they are competing with India. Pakistani hackers frequently have targeted the websites of the Indian government.[37] There has been an uptick in these activities after the abrogation of Article 370 of the Indian Constitution and activities in Indian-occupied Kashmir. Pakistan did this by using fake profiles, cyber trolls, journalists, and Pakistani diplomats, focusing on issues like the plight of common Kashmiris, the alleged human rights violations committed by Indian security forces in the Kashmir Valley, and spreading fear about the possibility of an India-Pakistan nuclear conflict, among others. It is unclear if Pakistani hackers are acting alone or in groups for their own benefit. An Indian government officer was the victim of a Pakistan-origin virus named "ReverseRat 2.0" that sent a fake invitation to a United Nations meeting on organised crime along with a Microsoft Teams link. reverse 2.0 can infiltrate the targets' computers, and the virus may remotely use its cameras to take pictures and even download files from USB drives inserted into the infected device.[38] Security researchers from the cybersecurity company Malwarebytes Labs in Ireland discovered attempts in 2020 from the hacking group APT36, a Pakistani state-sponsored malicious actor, to compromise Indian government, diplomatic, and military networks and lure defence personnel into a honey trap to steal confidential information pertaining to Pakistani military and diplomatic interests. Spear phishing emails containing a malicious link, supposedly from the Indian government, were its method of operation. The fact that the gang has been operating since 2016 shows the length of its cyberespionage effort.[39] The first time the Pakistan Cyber Army (PCA) participated in the destruction of the Indian Oil and Natural Gas Company was in November 2008. In 2021, hackers from Pakistan used a new virus to attack crucial power sector facilities and one Indian government organisation. A new variety of Remote Access Trojan (RAT), a malware that permits covert monitoring and unauthorised access to victims' computers, was installed by the attackers, and they hacked the domain URLs with a presence in India.[40]

Beijing and Islamabad have intensified their information technology cooperation in recent years. This is also implied by the key component of the Long Term Plan for China-Pakistan Economic Corridor (2017-2030), which includes digital and cyber cooperation. The Strategy emphasises the growth and promotion of e-commerce in Pakistan with the aid of Information and Communications Technology.[41] Beyond this constructive cooperation, however, a reality of China-Pakistan conspiracy has also evolved, with Pakistan acting as a front for China's nefarious intentions. This is especially true when it comes to anti-Indian misinformation spread through social media. Propaganda against India has been distributed on Twitter by accounts located in Pakistan that pretend to be Chinese citizens. A number of such incidents took place during the border standoff between China and India along the Line of Actual Control. These Twitter accounts frequently spread false information concerning the bloody conflict at Galwan Valley in June 2020 and India's military readiness.[42] Pakistan serves as the implementer and disseminator, while China takes the lead in providing the technology and content. Because popular social media sites like Twitter and Facebook are forbidden in China, and a large portion of the Chinese population has very low proficiency in English and Hindi, which is where Pakistan is helpful to China. China can also avoid responsibility by not directly participating and making Pakistan the hub of the anti-Indian effort. Pakistan's cooperation with China deepens its strategic alliance and gives Islamabad's cyber operations the technological advantage they otherwise could not have. This cyber-collusion is probably going to include hostile cyber-activities like APT assaults to gather important geopolitical, commercial, and military data.[43] The role of the China-Pakistan Economic Corridor in improving Pakistan's ICT infrastructure is one piece of evidence, but the real proof comes from the tactics used by cyber actors in both nations, which include influence operations based on false propaganda, espionage using malware and honey traps, and other forms of tactical cyber warfare.

**5. Cyber Warfare- The Indian Experience**

According to recent report from the Russian cybersecurity company Kaspersky, titled "Cyberthreats to Financial Organizations in 2022," India is one of the top five countries in Asia-Pacific region that are targeted by cyberattacks, particularly Advanced Persistent Threat attacks that take advantage of weaknesses in cyberdefenses and go undetected for a long time. Kaspersky predicts an increase in APT attacks over the next few

years. The Kaspersky statistics show that cyber risks to India are growing, with penetration attacks primarily coming from China and Pakistan. A number of highly skilled cybercriminals and international attack organisations continue to have India on their hit list. The Russian company has suggested that funding should be allocated to infrastructure and tools that will enhance cyber intelligence by improving analytical skills.[44] Despite the rising prevalence of cybercrime, cyber espionage, and various other types of malware, India has started the path of digitalisation of the economy and the governing apparatus. India is also at risk for terrorist attacks since terrorist organisations are utilising technology and hiring highly qualified individuals. These threats and attackers may increase their assaults significantly along with the shifting environment of digital India.[45] We must develop a deterrent strategy and use it effectively.

- In March 2021, two of the Indian vaccine manufacturers, Bharat Biotech and the Serum Institute of India (SII), had their information technology systems attacked by a Chinese state-sponsored hacking organisation, according to CyFirma, a Singapore-based corporation. The most important component of India's national immunisation programme and vaccine diplomacy has been the use of vaccines produced by these firms.[46]

- Similarly, large portions of Mumbai saw one of the greatest power disruptions in October 2020, impacting hospitals and suburban train services. Recorded Future claimed months later that "RedEcho," a hacker group with ties to China, had gained access to the Indian power grid and may have been responsible for Mumbai's power outage, a claim that was later refuted by the Maharashtra government's technical audit committee after looking into the incident. However, Recorded Future noted that Chinese hackers also attacked two Indian ports and sections of the railway infrastructure in addition to the power industry. This attack on India's vital infrastructure followed the bloody fight between the Indian and Chinese troops in the Galwan Valley in June 2020, which signalled a mix of intimidation and retaliation.[47]

- Another challenge for India's cybersecurity setup took place in February 2021 when SITA, the Geneva-based air transport data company that services more than 90% of the world's airlines,

informed Air India that hackers had stolen the personal data of 4.5 million passengers. Despite the fact that the incident took place outside of Indian territory, millions of Indians were impacted. While the Indian cyber-warriors made every effort to minimise the harm caused by the breach, they soon realised that it was difficult to conduct an inquiry into assaults that occurred outside of Indian cyberspace due to jurisdictional difficulties.[48]

**Cyber Capabilities- Institutional Evolution**

To offer IT solutions to the government, the National Informatics Center (NIC) was founded as early as 1975. Between 1986 and 1988, Three Networks NWs were established: NICNET (the NIC Network), a nationwide very small aperture terminal (VSAT) NW for public sector organisations as well as to connect the central government with the state governments and district administrations; and the Education and Research Network (ERNET), which served the academic and research communities. INDONET connected the IBM mainframe installations that made up India's computer infrastructure.[49] Under the direction of Lt. General Rajesh Pant, the Data Security Council of India (DSCI) conceptualised the National Cyber Security Strategy in 2020.[50] The Center has not yet taken any concrete steps to put the National Cyber Security Strategy into practice, despite an increase in cyberattacks on India's networks. It is especially crucial in light of the growing sectoral interconnection and abundance of internet access points, both of which might expand further with the implementation of the 5G network. According to data submitted to and maintained by the Indian Computer Emergency Response Team (CERT-In), 6.07 lakh cyber security incidents were reported in the first eight months of 2020, almost equal to the preceding four combined years.[51] The large-scale digitisation of public services, which places a focus on security in the early stages of design in all digitisation initiatives, the development of institutional capacity for assessment, evaluation, certification, and rating of the core devices, as well as the tracking and mapping of the supply chain of Integrated Circuits (ICT) and electronics products, are the main pillars of the cyber security strategy.[52] The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was established to provide free tools for detecting and eradicating dangerous software. The government has concentrated on creating a Crisis Management Plan to

combat cyberattacks and cyberterrorism and issuing warnings and advisories on cyber risks and countermeasures via CERT-In. The Cyber Surakshit Bharat programme was started by the Ministry of Electronics and Information Technology to raise awareness of cybercrime and develop capacity for safety measures across all governmental agencies. The government made plans to establish the Cyber Warrior Police Force (CWPF) in 2018. It is intended to be raised on the model of the Central Armed Police Force (CAPF).[53]

In 2019, the Indian Armed Forces have established a tri-service command called the Defence Cyber Agency (DCyA). The DCA under the current leadership is supposed to perform two tasks; first, to fight virtual conflicts in the cyber domain, and second, to develop a cyberwarfare doctrine. It is anticipated that this will help develop a cybersecurity strategy policy that incorporates cyberwarfare with traditional military operations. While simultaneously developing capabilities for full spectrum information warfare with cyber power as one of its major constituents, the formation of the Defence Cyber Agency should be seen as an intermediate step toward the formation of a full-fledged Cyber Formation or Cyber Command in the future.

India has taken strides to fix its cyber vulnerabilities in recent years through a variety of institutional and legislative measures. However, hackers from China and Pakistan, continue to take advantage of the lack of cybersecurity awareness and poor cyber hygiene habits of average Indian Internet users. Habits such as not verifying the accuracy of fake news and clicking on unsolicited web links to infect sensitive computer networks and spread their malware, are common among Indians. India must thus take two measures even as it improves its cyber defences by addressing its weaknesses.[54]

- One, India should broaden its measures to promote cyber hygiene and improve its citizens' resistance to new cyber threats. The majority of public and private organisations are hesitant to report incidences of hacking out of concern for negative publicity and client loss, which is the main weakness in India's cyber preparation.

- Two, it has to strengthen its offensive cyber posture on a larger scale in order to make its intentions plain to its enemies and discourage

them. The national security establishment has resisted presenting technical proof linking these assaults to Chinese state-sponsored hackers, despite the fact that the technology community in India and elsewhere has done so. As a result, it is necessary to start doing so.

## 6. Cyber Risk Assessment in The Indian Context

Cybersecurity is essential for daily economic operations, the smooth running of social and economic infrastructure systems, as well as for internal and external national security in the era of exponential growth in data, information, and knowledge. Modern warfare's defensive component, which is closely related to the vicious and on-the-ground military operations, also includes cyber warfare. Therefore, it is important to comprehend the risks to privacy and national security posed by data loss, leakage, or corruption due to ignorance, error, or cyberattack. Cyberattacks, for instance, could occasionally be essential against cyber terrorists for which cyber defence security have to be improved.[55] Cyber weapons can and should be used by India in order to weaken its enemies' capabilities and respond to harmful behaviour. There should be an inclusion of the concept of cyber warfare into the whole definition and gambit of modern warfare and national security.

The cyber risk assessment includes assessing the type and level of the threat, the probability and the effect of the same on every aspect of the security infrastructure. Cyberspace has the capacity to seriously compromise national security while eluding conventional national defence systems and striking vital domestic targets directly. Thus, a deliberate shift in the area of national security is being brought about by the emerging phenomena of cyberspace. Cyber Operations are at the early stages of development today. However, several publicly accessible strategy documents requesting international collaboration proclaim deterrents, proportionate responses, and self-defence measures.[56]

It is evident that no matter the agency behind the cyberattack, be it China, Pakistan, or any other country, the first and the main objective is to safeguard the network by limiting the access of unauthorised users to the network at the physical level. India is not an exception to this since the Chinese have enhanced capabilities to attack the adversary's network, endangering the national and other network-dependent functions of any

nation. Although the public networks cannot be completely protected against cyberattacks, the exposure can be reduced to some extent. Defence agencies should independently design, acquire and operate the cyber network. Media interference should be restricted in addition to complete network security. Although the government of India has mostly developed preventive cyber security measures, it has also developed the potential for proactive actions. There are proven tactics for both preemptive and preventive cyber responses.[57]

Because networks may be attacked from anywhere in the globe and for a variety of reasons, including political inclination, fraud, criminality, or an extension of state conflict, it is difficult to ensure cyber and IT security. Digital traces are very simple to conceal. Global cooperation can ensure that the internet thrives without having to live in continual dread of information being misused. India has also participated in a number of cyber diplomacy initiatives that are expected to grow in scope. The sharing of information on cyberattacks, security measures, and cyber law enforcement has been at the centre of several bilateral cyber accords. Notably, agreements with Israel, the US, Japan, the UK, Australia, and other countries are robust and renewed to grow. With the Quad shifting its emphasis to essential and emerging technologies, including cyber security, India will play a significant role in this domain. India will also be a prominent player as the international community steps up to agree on legally enforceable cyber security standards and introduce some kind of legislation, which has previously been discussed by the Group of Governmental Experts (GGE) based at the UN. Partnering governments may anticipate an updated and concise Indian Cyber Security Policy that complies with its suggestions for further cooperation.[58]

The majority of the hardware and software used by the Indian government and commercial businesses for cyber operations is imported. The potential of adding new malware or having malware that has already been installed steal data while upgrading its current capabilities is quite high. Public-private collaborations are required to address these issues and develop India's key infrastructure. One particularly significant concern is the Advanced Persistent Threat, in which a hacker or a group of hackers get access to the system and harvest data for a prolonged period of time while going unnoticed. Since it can often be difficult to distinguish between State and non-state actors, this presents a significant problem for any nation.

The ignorance of a common man about the risk of data leak is one of the biggest issues with cyber-attacks. They frequently become both targets and unintentional assault tools; thus, knowledge and awareness of such attacks among the public is essential.[59] Furthermore, because social media is a massive repository of data and important information can be extracted from it, it poses a major risk to the security of a nation. Since in India, there are a lot of new people using the Internet, it is easy to target them and steal their data and money. All of these arguments imply that the government faces a formidable problem in educating the general public about cyber threats. India is still dedicated to acting as a responsible global citizen and a willing participant in initiatives to spur action on this problem. India can coordinate its efforts across a number of areas, such as standard-setting, protecting digital intellectual property rights, exchanging best practises, building developing nations' capacities, providing crucial intelligence data, and establishing pertinent security parameters.

## 7. Conclusion

At the tactical level, soldiers are becoming more and more reliant on cyberspace, and at the strategic level, the State's capabilities and vulnerabilities in cyberspace are being used to influence and impede the strategic balance of power. With this, cyberspace's Future is likely to see the deep integration of Internet and PC technology into many commonplace items, including not only technological ones like computers, telephones, radios, and televisions but also non-cyberspace-related ones like home appliances, consumer goods, clothing, and more. This networked grid of things will be crucial to the economy of industrialised countries. Unfortunately, the grid is based on technologies that were not intentionally created to manage information of this scope and significance. Attackers will be able to create extensive networks of infected things through security holes that they may then use to influence target companies, take advantage of other objects, and perhaps even destroy entire nations and economies.

India is at the crossroads, which is why we need to include cybersecurity in our national agenda and major projects on the strategic and socioeconomic fronts. India needs a strong cybersecurity policy that protects citizens and the economic environment in order to do this. This

will assist in defending individuals against cyber threats and increase investor faith in the economy. Additionally, it will open up job opportunities in this industry. By 2025, there will be roughly 1.5 million open positions in the cybersecurity industry, according to the most recent statistics. There is a need for a single nodal body to enforce stringent regulations and penalise organisations that do not increase their spending on cybersecurity. There are several government organisations at both the state and federal levels now, and it is imperative to bring all of these separate task forces together to generate synergy. A national cybercrime unit is required so that we can use resources to combat threats and breaches. India may concentrate on creating and producing the essential infrastructures domestically, which is in line with the country's "Atmanirbhar" goal. Research & development investments must be made in order to accomplish this. Public-private partnerships should be supported since the business sector has a significant stake. We may also use these partnerships to devise a plan to combat China's developing cyber capabilities. The correct application of conventional and cyber weapons on the battlefield should be investigated, along with collaboration among the three services. Due to the rapidly growing user base, it is imperative to raise awareness of cybercrimes among the general population and encourage digital literacy. A minimal set of cyber security measures must be included in the baseline security criteria for each industry. Due to the global character of cyber threats, countries, even developed countries and intergovernmental organisations, need to be active in the policy-making process for cybersecurity. To combat and prosecute cybercrime, India must create current laws and regulations. It has also become crucial to develop cyber law capability in all areas, including the police, corporate sector, judicial, and legislative departments.

In order to preserve economic and informational interests that are essential to national security, political and military involvement is required. Cyberspace has arisen as a significant new arena for political and military rivalry. The military has particular problems in the age of online connection and information flow that call for intense international cooperation. Even though the concept of cyber diplomacy is catching up, immediate steps need to be taken. The difficulties increase as a result of the extent to which civilian operations are included in cyberspace, which does not properly belong to the military. A cooperative civilian defence collaboration,

including public-private partnership, is necessary to protect cyberspace in the interests of national security and international stability. Political rules and moral principles should govern and restrain cyberspace.

**Disclaimer:** Views expressed are of the author and do not necessarily reflect the views of CENJOWS.

---

**Endnotes**

[1] Lior Tabansky, 'Basic Concepts of Cyber Warfare', *Military and Strategic Affairs*, (May,2011), https://www.inss.org.il/wp-content/uploads/2017/02/FILE1308129610-1.pdf

[2] Jason Andress, Steve Winterfeld, *Cyber Warfare*, (Elsevier, 2014), 4-10

[3] Jitender K. Malik & Dr. Sanjaya Choudhary, 'Cyberspace-Evolution & Growth', *East African Scholars Journal for Education, Humanities and Literature*' (March, 2019), https://www.easpublisher.com/get-articles/883

[4] Paul J. Springer, '*Enclyclopedia of Cyber Warfare'*, (ABC-CLIO, 2017)

[5] Jason Andress, Steve Winterfeld, *Cyber Warfare*, (Elsevier, 2014), 35-38

[6] Syed Rameem Zahra & Others, 'Detecting COVID-19 Chaos driven Phishing/Malicious URL attacks by a Fuzzy Logic and Data Mining Based Intelligence System', *Egyptian Informatics Journal,* (July, 2022), https://www.sciencedirect.com/science/article/pii/S1110866521000815

[7] '*Cloud Computing Attacks:A New Vector for Cyber Security*', Apriorit, (Ferbuary,2022), https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

[8] David Weissbrodt, 'Cyber-conflict, Cyber-crime and Cyber Espionage'*, University of Minnesota Law School*, (2013), https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

[9] Ryan J. Hayward, 'Evaluating the imminence of a cyber attack for purposes of anticipatory self-defense', *Columbia Law Review,* https://columbialawreview.org/content/evaluating-the-imminence-of-a-cyber-attack-for-purposes-of-anticipatory-self-defense/

[10] *International Cooperation on Cyber Security Matters*, United Nations Office of Drugs and Crimes (UNDOC), https://www.unodc.org/e4j/en/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

[11] Max Smeets, 'A US History of not Conducting Cyber Attacks', Taylor and Francis, (July, 2022), https://www.tandfonline.com/doi/full/10.1080/00963402.2022.2087380

[12] Julian Jang-Jaccard & Surya Nepal, 'A Survey of Emerging Threats in Cybersecurity', *Journal of Computer and System Sciences*, (August,2014), https://www.sciencedirect.com/science/article/pii/S0022000014000178

[13] Cyber Capabilities and National Power: A Net Assessment, *International Institute of Strategic Studies,* (June,2021), https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[14] Isarel's National Cyber Security and Cyber Defense Posture, Cyber Defense Project, Centre for Security Studies, (2020), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf

[15] Mathew Cohen & Charles Freilich, 'Israel and Cyberspace: Unique threat and Response', *International Studies Perspectives,* (2016), https://www.researchgate.net/publication/288823312_Israel_and_Cyberspace_Unique_Threat_and_Response

[16] Jason Andress, Steve Winterfeld, *Cyber Warfare*, (Elsevier, 2014), 279-281

[17] Fabio Cristino, 'Israel: Cyber Defense and Security as National Trademarks', *Routledge,* (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3698972

[18] *'New European Cyber Security Strategy*', European Commission, (December, 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[19] Michael Connell & Sarah Vogler, 'Russia's Approach to Cyber Warfare', *CNA Analysis and Solutions,* (December,2016), https://apps.dtic.mil/sti/pdfs/AD1019062.pdf

[20] Jason Andress, Steve Winterfeld, *Cyber Warfare*, (Elsevier, 2014), 12-18

[21] Kenneth R. Rosen, 'The Man at the Center of the New Cyber World War', *Politico,* (July,2022), https://www.politico.com/news/magazine/2022/07/14/russia-cyberattacks-ukraine-cybersecurity-00045486

[22] James Andrew Lewis, 'Cyber War and Ukraine', *Center for Strategic and International Studies,* (June,2022), https://www.csis.org/analysis/cyber-war-and-ukraine

[23] April Lynch, 'Kosovo being Called the First Internet War', *SFGATE*, (April,1999), https://www.sfgate.com/news/article/Kosovo-Being-Called-First-Internet-War-Web-2936299.php

[24] Johan Sigholm, 'Non-State Actors in Cyberspace Operations', *Journal of Military Studies*, (December,2013), http://dx.doi.org/10.1515/jms-2016-0184

[25] Niccolo Bussolati, 'The Rise of Non-State Actors in Cyber Warfare', (March,2015), https://doi.org/10.1093/acprof:oso/9780198717492.003.0007

[26] Tim Lister, '*Patriot Games-The Murky World of Russian Hacking'*, CNN, (June,2017), https://edition.cnn.com/2017/06/02/politics/vladimir-putin-russian-hacking/index.html

[27] Jason Andress, Steve Winterfeld, *Cyber Warfare*, (Elsevier, 2014), 213-215

[28] Johan Sigholm, 'Non-State Actors in Cyberspace Operations', *Journal of Military Studies*, (December,2013), http://dx.doi.org/10.1515/jms-2016-0184

[29] Paul J. Springer, '*Enclyclopedia of Cyber Warfare'*, (ABC-CLIO, 2017)

[30] Pierluigi Paganini, '*10 Biggest Cyber Espionage Cases*', Security Affairs, (December, 2013), https://securityaffairs.co/wordpress/66617/hacking/cyber-espionage-cases.html

[31] '*Recent Ransomware attacks and Examples*', Measured, https://measuredinsurance.com/blog/recent-ransomware-attacks-examples/

[32] Michael Robinson, Kevin Jones & Helge Janicke, 'Cyber Warfare: Issues and Challenges' (March,2015), http://dx.doi.org/10.1016/j.cose.2014.11.007

[33] Magnus Hjortdal, 'China's Use of Cyber Warfare: Espionage meets Strategic Deterrence, *Journal of Strategic Security,* (2011) , https://digitalcommons.usf.edu/jss/vol4/iss2/2/

[34] Jason Fritz, 'How China will Use Cyber Warfare to Leapfrog in Military Competitiveness' *The Bulletin of the Centre for East-West Cultural and Economics Studies*, (October, 2008), https://www.researchgate.net/publication/27828264_How_China_Will_Use_Cyber_Warfare_to_Leapfrog_in_Military_Competitiveness

[35] Col. Mandeep Singh,'China's Cyber Warfare Cpabilities', *Indian Defence Review*, (July,2020), http://www.indiandefencereview.com/news/chinas-cyber-warfare-capabilities/

[36] Robert Lai & Shawon S.M. Rahman, 'Analytic of China Cyberattack' *The International Journal of Multimedia and its Applications*, (July, 2012), https://www.researchgate.net/publication/267363551_Analytic_of_China_Cyberattack

[37] Dr Ghulam Mustafa, Zainab Murtaza & Khadija Murtaza, 'Cyber Warfare between Pakistan and India: Implications for the Region', (2020), http://dx.doi.org/10.47205/plhr.2020(4-I)2.5

[38] Sameer Patil & Aditya Bhan, 'Pakistan is India's New Cyber Security Headache', *Gateway House,* (November 2021), https://www.gatewayhouse.in/pakistan-indias-cybersecurity-headache/

[39] '*APT36 jumps on the Coronavirus Bandwagon, Delivers Crimson RAT,* 'MalwareBytes', (March,2020), https://www.malwarebytes.com/blog/news/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat

[40] '*Pakistan-based Hackers target Indian Power Sector, Government, Organisation',* Business Today, (July,2021), https://www.businesstoday.in/technology/news/story/pakistan-based-hackers-target-indian-power-sector-govt-organisation-301224-2021-07-13

[41] Ma Zhong & Others, 'China Pakistan Economic Corridor Digital Transformation', *Frontiers in Psychology*, (May,2022), https://doi.org/10.3389/fpsyg.2022.887848

[42] Aditya Bhan, Sameer Patil, 'Cyber attacks- Pakistan emerges as China's Proxy against India', *Observer Research Foundation*, (Ferbuary, 2012), https://www.orfonline.org/research/pakistan-emerges-as-chinas-proxy-against-india/

[43] '*Why China Desperately Needs Pakistan for its Cyber-Warfare against India?*' The Eurasian Times, (August,2020), https://eurasiantimes.com/why-china-desperately-needs-pakistan-for-its-cyber-warfare-against-india/

[44] *'Kaspersky predicts rise in Cyber Espionage in India in 2022'*, Business Standard, (January,2022), https://www.business-standard.com/article/economy-policy/kaspersky-predicts-rise-in-cyber-espionage-for-india-in-2022-122011401057_1.html

[45] Alik Naha, 'Emerging Cyber Security Threats: India's Concerns and Options', *International Journal of Politics and Security,* (May,2022), https://www.researchgate.net/publication/360297294_Emerging_Cyber_Security_Threats_India's_Concerns_and_Options#read

[46] Sameer Patil & Kishika Mhajan, 'Expanding Cyber Espionage Threat Against India' *Observer Research Foundation,* (April,2022), https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india/

[47] *'Did Chinese Hackers Cause Mumbai Power Failure in October?'*, The Wire, (March, 2021), https://thewire.in/world/india-china-hackers-border-tension-power-grid-malware-recorded-future

[48] '*Air India says Ferbuary's Data Breach Affected 4.5 Million Passengers'*, Reuters, (May,2021), https://www.reuters.com/world/india/air-india-says-februarys-data-breach-affected-45-mln-passengers-2021-05-21/

[49] National Informatics Centre, https://www.nic.in/servicecontents/nicnet/

[50] India's Cybertech Repository, https://www.dsci.in/sites/default/files/TechSagarLaunch.pdf

[51] *'More than 6.07 cyber security incidents occurred'*, The Hindu, (August,2021), https://www.thehindu.com/business/cert-in-observed-more-than-607-lakh-cyber-security-incidents-till-june-2021-government/article35726974.ece

[52] M.K. Sharma, 'Cyber Warfare: Implications for India', *India'a National Security Annual Review,* 2011, (March, 2011), https://www.researchgate.net/publication/339956351_Cyber_Warfare_Implications_for_India

[53] *Press Information Bureau*, Government of India, (July,2019), https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

[54] Lt. General Nitin Kumar Kohli, 'Challenges and Prospects of Cyber Security in the Indian Context, *The United Service Institution of India*, (June, 2012),

https://usiofindia.org/publication/usi-journal/challenges-and-prospects-of-cyber-security-in-the-indian-context/

[55] RA Atrews, 'Cyberwarfare: Threats, Security, Attacks and Impact', *Journal of Information Warfare*, (2020), https://www.jstor.org/stable/27033642

[56] Ana I. Cerezo, Javier & Ahmed Patel, 'International Cooperation to fight Transnational Cybercrime', *Digital Forensics & Incident Analysis* (2007), http://dx.doi.org/10.1109/WDFIA.2007.4299369

[57] Madhu Vanthi, 'India's Cyber Space Security requires Urgent Booster Shot', *Centre for Land Warfare Studies*, (August 2021), https://www.claws.in/indias-cyber-space-security-requires-an-urgent-booster-shot/

[58] Sameer Patil, 'India's Cyber Diplomacy', *India Perspectives,* (2021), https://www.indiaperspectives.gov.in/en_US/indias-cyber-diplomacy/

[59] Sushma Devi, 'Cyber Security in the National Security Discourse', *The Journal of International Issues*, (2019), https://www.jstor.org/stable/48531107