INDIA'S PREPAREDNESS FOR CYBERWARFARE: A LEGAL AND INSTITUTIONAL ANALYSIS

K. Megha Narayana Reddy, Christ (Deemed to be University), Bengaluru[1]

ABSTRACT

As geopolitical disputes increasingly unfold in the digital realm, India's capacity to counter cyber warfare has become a critical national security issue. Rising state-linked cyberattacks targeting Indian infrastructure reveal the inadequacy of existing laws and institutions. This paper examines whether India's fragmented and outdated cyber legal framework can address militarised cyber operations beyond conventional cybercrime or espionage.

Drawing on doctrinal and policy analysis, the study reviews the Information Technology Act 2000, relevant penal codes, and the roles of CERT-IN, NCIIPC, the Defence Cyber Agency, and the National Cyber Coordination Centre. It also compares India's stance with international standards such as the Tallinn Manual and international humanitarian law.

Findings show India's framework is reactive, focused mainly on civilian cybercrime, and hindered by institutional silos and unclear mandates for offensive or defensive cyber warfare. The absence of a comprehensive cybersecurity statute and misalignment with global norms leave India vulnerable to state-sponsored attacks.

The paper argues for a multi-pronged approach: enacting dedicated cybersecurity legislation, clarifying civil–military responsibilities, and aligning domestic practices with evolving international law. It highlights the urgent need for an Indian cyber warfare doctrine, assessment of offensive cyber capabilities, and enhanced international legal cooperation.

Keywords: Cyberwarfare, IT Act, National Security, Sovereignty, Tallinn Manual.

[1] Kavali Megha Narayana Reddy, Christ (Deemed to be University), Bangalore

1. Introduction

Cyberwarfare is no longer a detached concern limited just to fiction or military strategy rooms, but rather a rapidly evolving threat. It is to be considered as a pressing issue that reshapes how modern states secure their sovereignty and digitally protect their borders. The scale and complexity of its exposure to cyber threats have also advanced with time as India tries to move towards a more digitally integrated economy and governance structure.

At its centre, cyberwarfare involves using digital tools to inflict harm or disruption on a nation-state. Definitions vary, but they converge on key ideas. Cybersecurity firm Fortinet states, *"cyberwarfare is a series of strategic cyber attacks against a nation-state, causing it significant harm."*[2] Richard Clarke a former White House counter-terrorism advisor, one of the earliest voices to raise alarm on this issue in his book titled *Cyber War: The Next Threat to National Security and What to Do About It*, described it as *"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."*[3] A more recent and layered interpretation from the book *Cyber Warfare: A Multidisciplinary Analysis* frames it as *"an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."*[4] These definitions reflect how cyberwarfare is not just about isolated incidents but deliberate, strategic actions with potentially serious geopolitical consequences to a nation-state.

India is especially vulnerable in this context. India's digital footprint is humongous, with over 80 crore internet users[5], the world's largest biometric identity database (Aadhaar)[6], and critical infrastructure that is heavily and increasingly reliant on digital systems. However, this connectivity also means potential points of liability. Over the last 10 years, India has witnessed a rise in cyberattacks[7] targeting banks, power grids, healthcare systems, government agencies,

2 Fortinet, Cyber Warfare: The Expanding Battlefield of Nation-State Cyber Threats, The Fortinet (n.d.), https://www.fortinet.com/resources/cyberglossary/cyber-warfare
3 Richard A. Clarke & Robert K. Knake, Cyber War: The Next Threat to National Security and What to do About it, p.6, 2010
4 James A. Green, CyberWarfare: A multidisciplinary analysis, p. 2, James A. Green eds., 2015
5 Kantar & IAMAI, INTERNET IN INDIA 2024, p.4, https://www.iamai.in/sites/default/files/research/Kantar_%20IAMAI%20report_2024.pdf
6 UIDAI, What is Aadhar, https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html
7 MeitY (India), Incidents of cyber attacks across India from 2015 to 2022 (in 1,000s) Statista,

etc[8]. The borderless character of cyberspace only adds to this challenge, as, unlike traditional warfare, cyberwarfare is hard to detect, difficult to attribute to someone, and even more difficult to deter. This research paper poses an urgent question: Is India adequately prepared to respond to and defend against cyberwarfare? To answer this question, the paper examines India's existing legal and institutional frameworks, evaluating how they measure up to the challenges of cyberwarfare, and compares them with best practices across the globe.

As cyberwarfare becomes an increasingly central part of modern conflict, assessing India's readiness is not just a legal or technological issue but a matter of national survival. The methodology involves doctrinal and comparative analysis, relying on statutes, policy documents, international legal instruments, and case studies of various cyber incidents.

2.Conceptual Framework: Cyberwarfare and National Security

The term "Cyberwarfare" is often used as a broad term for any hostile activity online, but this generalisation can dilute the issue. Hence, before examining policy gaps or legal frameworks, it is essential to know what cyberwarfare is, how it compares to other cyber threats, and recognise why it poses a severe national security concern.

Differentiating Cyberwarfare, Cybercrime, and Cyberterrorism

Cybercrime, at its core, is criminal activity that uses digital networks to break the law. Think of credit card fraud, ransomware attacks, or identity theft. These are usually profit-driven and handled through national and international criminal law[9]. Cyberterrorism looks different. It involves using the internet or digital tools to create fear or disrupt public systems, with political or ideological motives. Non-state actors usually carry it out, often targeting civilians or critical services, like healthcare, transport, or public databases[10]. Cyberwarfare stands apart. It involves state-sponsored or state-directed operations that aim to disrupt, spy on, or damage another country's digital systems, sometimes with real-world consequences. The intention is not just criminal gain or fear but strategic disruption. Moreover, it often falls into a legal grey zone. A

https://www-statista-com-christuniversity.knimbus.com/statistics/1201177/india-number-of-cyber-attacks/ (last visited July 30, 2025)

[8] Indian Computer Emergency Response Team annual report 2024, page 7 https://www.cert-in.org.in/ (last visited July 30, 2025)

[9] Cisco, What is Cybercrime, Cisco Web (n.d.), https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html (last visited July 30, 2025)

[10] Amaresh Pujari. CYBER TERRORISM: World Wide Weaponisation, Confederate of Indian Industry, p.2 https://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf

cyber operation only stops short of being a conventional "armed attack," but still hit essential systems or undermine public trust, which threatens the innate nature of sovereignty of a state.

The Tallinn Manual 2.0, though not legally binding, carries weight in international law circles and helps draw these lines. It discusses how cyber operations can count as a "use of force" under the UN Charter if the effects are severe enough[11]. That is where cyberwarfare blurs the boundary between peace and conflict, but it often happens outside formal declarations of war, with very real consequences. It adds law, ethics, and strategy to the picture. Scholars like Thomas Rid have pointed out that cyberwarfare does not usually involve physical violence, yet it still disrupts on a national scale[12].

Each of these views tells us something important, and taken together, they show how cyberwarfare is not just a tech issue. It is a political, legal, and strategic problem all at once.

Why Cyber Power Now Shapes National Power

Historically, a country's strength was mostly measured in military and economic terms. That is still true, but now, digital capability is part of the equation too. Most of a modern state's infrastructure is digital: power grids, communication systems, banks, transport, and even election processes. This makes the process faster and more efficient, but potentially leaves them vulnerable. Additionally, given that cyberattacks can be subtle and difficult to trace, they have emerged as an attractive strategy for nations seeking to apply pressure on others without entering into outright conflict. Unlike conventional weaponry such as bombs or tanks, these attacks can incapacitate a city or compromise state secrets, often leaving no trace behind.

Modern cyber strategy includes both deterrence and pre-emptive action. For instance, the U.S. Cyber Command advocates a strategy of "defending forward," which focuses on disrupting threats before they target American systems[13]. This approach represents a change from a passive stance of waiting for attacks to actively engaging with enemy networks, reflecting the evolving character of cyber defence. For India, the threat of cyberwarfare is not theoretical, as

[11] Schmitt, M.N. (2017) 'The use of force', in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, pp. 328–356. https://doi.org/10.1017/9781316822524.020 (last visited July 30, 2025)

[12] Rid, T. (2011) 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35(1), pp. 5–32. https://doi.org/10.1080/01402390.2011.608939. (last visited July 30, 2025)

[13] Jonathan Reed, Taking the fight to the enemy: Cyber persistence strategy gains momentum, IBM Think,(Jan. 23, 2025) https://www.ibm.com/think/insights/taking-fight-to-enemy-cyber-persistence-strategy-gains-momentum (last visited July 30, 2025)

tensions with neighbouring countries are not confined to the ground or the border but can also transcend online. There have been reports of Chinese malware probing India's power infrastructure and phishing campaigns linked to foreign intelligence units[14]. These incidents serve as clear reminders that cyberwarfare is an immediate and pressing reality for India.

3. Changing Landscape of Cyber Threats in India

India's journey into cyberspace has been swift and transformative. From expanding digital infrastructure under schemes like Digital India, which has positioned India as one of the world's largest internet user bases[15], the country's digital footprint has expanded rapidly. However, that growth has brought with it an equally growing cyber threats. Cyber threats in India extend beyond mere personal data breaches and online scams they evolved into strategic, coordinated attacks that impact national security, economic stability, and public confidence of the country.

A Timeline of Growing Complexity

Early cyber incidents in India were relatively unsophisticated. The primary threats in the late 1990s and early 2000s came from website defacements and amateur hacking groups[16]. Many of these attacks were symbolic nationalistic hackers targeting each other's country websites in the India-Pakistan cyber rivalry. These "cyber skirmishes" made headlines but did not go far beyond surface-level damage. Things changed significantly post-2010. As India digitised its key sectors like banking, energy, and governance systems, attackers shifted focus towards real disruption and data theft. The 2012 breach of DRDO (Defence Research and Development Organisation) email servers is considered an alarm, exposing how vulnerable sensitive government communication can be to advanced espionage[17].

In 2016, the *Union Bank of India* suffered a loss of nearly $170 million in a phishing-based SWIFT attack. The attackers tricked a bank employee into opening a malware email, which compromised internal systems and allowed them to send fake SWIFT messages to transfer

[14] Sameera Patil, Expanding Chinese cyber-espionage threat against India, ORF Foundation, (Apr. 18, 2022) https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india (last visited July 30, 2025)
[15] PIB Delhi, Achievements Made under Digital India Programme, PIB, (Dec. 23, 2022) https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1885962 (last visited July 30, 2025)
[16]Prichard Janet & Laurie E. MacDonald, Cyber Terrorism: A Study of the Extent of coverage in Computer Security Textbooks, Vol. 3, JITE, 279 – 289 (2004) https://doi.org/10.28945/302 (last visited July 30, 2025)
[17] Haris Zargar, India must wake up to cyber-terrorism, Indo-Asian News Service, (2 Apr. 2013) https://www.gadgets360.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274 (last visited July 30, 2025)

funds to offshore accounts. Though most of the amount was recovered, it indicated how attackers were directly targeting financial institutions[18]. The following year, i.e, 2017, the *WannaCry ransomware* outbreak disrupted systems across several Indian states, including computers at police stations and state electricity boards. While India was not the hardest hit country[19], it exposed a profound lack of preparedness in public IT infrastructure, especially around patching and basic cyber hygiene in the country. Here, Cyber hygiene refers to the methods and actions that individuals and institutions can take to safeguard their systems and data against cyber threats[20].

Critical Infrastructure in the Crosshairs

A significant turning point came in October 2020 when it was reported that Chinese-sponsored actors had targeted India's power grid infrastructure in Mumbai. The sudden blackout affected different parts of the city, media outlets and experts raised concerns about a potential cyberattack. Though the government did not confirm a direct link, reports from reputed cybersecurity firms like Recorded Future[21] strongly urged that malware had been planted in power control systems of Mumbai. This incident stands out not for its scale but for what it targeted: the critical infrastructure of the nation. Unlike previous attacks, which focused on websites or financial data with clear individual benefits, this incident implied a strategic goal to send a message, assess vulnerabilities, and possibly set the stage for future coercive action against India. It reiterated the ongoing global trend of cyberattacks becoming geopolitical tools, especially during tensions, in this case, following the Galwan Valley clashes. This trend shows that state-sponsored cyberattacks are being used to exercise influence or pressure in international relations.

Learning from Global experiences

India is not the first to face such threats. The 2007 cyberattack on Estonia is widely considered to be one of the first instances of the world's first cyberwar. It paralysed Estonian government

[18] Hardev Kaur, Cyber Crime in Banking Sector a Study Related to Indian Perspective, Vol. 11 Issue 8, IJIRT, p. 45-53 (Jan. 2025) https://ijirt.org/publishedpaper/IJIRT171471_PAPER.pdf (last visited July 30, 2025)
[19] Pushkar Baviskar & Manikant Roy, Wanna cry ransomware: A case study in Indian perspective, Vol. 6 Issue 2 IJCRT, p. 811-814 (Apr. 2018) http://www.ijcrt.org/papers/IJPUB1802133.pdf (last visited July 30, 2025)
[20] Scott Dawson, Cyber Hygiene Practices for Every User, Core Business Solutions, (1 Dec. 2023) https://www.thecoresolution.com/cyber-hygiene-practices-for-every-user (last visited July 30, 2025)
[21] Insikt Group, Threat Analysis – China, Recorded Future Report, (Apr. 6, 2022) https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf (last visited July 30, 2025)

systems, banks, and media outlets, sending shockwaves across the country[22]. This experience made Estonia one of the most cyber-resilient countries today, and it even hosted NATO's Cooperative Cyber Defence Centre. In a similar fashion, the *Stuxnet* worm, which is alleged to have been created by the US and Israel, can self-destruct a computer without leaving any trace. This attack aimed to disrupt Iran's nuclear programme, showing us that cyber tools could now be used to damage real-world infrastructure without using any conventional weaponry[23]. These cases matter for India because they highlight two things: the need for proactive defence, and the difficulty of attribution, which is the process of identifying the source of a cyberattack. Unlike conventional attacks, where the source is often apparent, cyberattacks leave behind indefinite trails. That leaves response strategies oblivious and calls for better technical capabilities, legal tools, and most importantly, international cooperation.

The evolution of cyber threats in India signifies a significant shift from simple cyber attacks to strategic disruption. It is no longer just about private data or corporate loss. This stays especially true, as India continues to digitise everything from military systems to municipal services, the line between a cyberattack and an act of war is becoming increasingly blurred, underscoring the potential seriousness of the situation.

4. Indian Cyberwarfare Governance: Laws, Policies, and Institutions

While reflecting a growing awareness of cybersecurity threats, India's legal and institutional readiness for cyberwarfare remains fragmented, mostly reactive, and very unevenly implemented. The need for a cooperative cyber command and legal reforms is urgent and of utmost importance in this current landscape. Firstly, the Information Technology Act, 2000 (IT Act), which was initially passed to support e-commerce and digital contracts, has gradually expanded its scope through amendments and judicial interpretation. Section 66F of the IT Act, 2000[24], for instance, defines and criminalises cyber terrorism as any act that threatens India's sovereignty, security, or the integrity of its critical information infrastructure (CII) as

[22] Rain Ottis, Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, p. 163-168, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (last visited July 30, 2025)

[23] Josh Fruhlinger, Stuxnet explained: The first known cyberweapon, CSO, (31 Aug. 2022) https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html (last visited July 30, 2025)

[24] The Information Technology Act, 2000, §66F

mentioned in section 70[25] of the same act. However, Section 66F heavily depends on subjective terms like intent and impact, making real-world enforcement difficult, especially where high-stakes situations involving state actors or proxy groups affecting national sovereignty. The act also focuses mainly on personal data protection and cybercrime, with a narrow articulation of state obligations or command structures in a cyberwar scenario.

A recent legislation, the Digital Personal Data Protection Act, 2023, regulates data processing, safeguards personal data, and imposes responsibilities for data fiduciaries and processors. Although the law aligns closely with global data protection frameworks (especially the GDPR), it does not directly address national security concerns[26]. The act grants the central government broad powers to exempt agencies from compliance for reasons linked to sovereignty, public order, or national security. This provision gives flexibility in emergencies but also raises accountability concerns. From a cyberwarfare perspective, this law supports state actors in securing digital infrastructures but does not establish any precise coordination mechanisms between data protection regulators and institutions. It also fails to address vulnerabilities in critical infrastructure sectors or digital supply chains, which are frequent targets during cyber conflicts.

Thirdly, India's regulatory ecosystem also includes domain-specific cybersecurity mandates. Financial institutions, for instance, are regulated through the RBI's Cybersecurity Framework (2016)[27], which requires banks to develop Board-approved strategies for cyber risk management. Likewise, SEBI issued its Cybersecurity and Cyber Resilience Framework for stock exchanges, clearing corporations, and depositories[28]. The Insurance Regulatory and Development Authority of India (IRDAI) has also released guidelines mandating insurers to strengthen their cyber hygiene[29]. However, these sectoral regulations function independently, leaving them without any interoperability. While they enforce compliance and basic incident reporting, they do not form part of a unified architecture that is very much needed to respond

[25] The Information Technology Act, 2000, §70
[26] Latham & Watkins LLP, India's Digital Personal Data Protection Act 2023 vs. The GDPR: A Comparison, (Dec. 2023) https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf (last visited July 30, 2025)
[27] Reserve Bank of India, RBI/2015-16/418 (Notified on 2 Jun. 2016) https://www.rbi.org.in/commonperson/english/scripts/Notification.aspx?Id=1721 (last visited July 30, 2025)
[28] Securities and Exchange Board of India, Circular, SEBI/HO/ ITD-1/ITD_CSC_EXT/P/CIR/2024/113 (Issued on Aug. 20, 2024) https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (last visited July 30, 2025)
[29] Anuj Bahukhandi & P. Singh, Information and Cybersecurity Guidelines, 2023, Tuli & Co, (Jun. 13, 2023), https://www.tuli.co.in/pdf/2023/062023.pdf (last visited July 30, 2025)

to cyberwarfare-like incidents that target multiple critical sectors simultaneously. The lack of such a unified structure could lead to delayed or ineffective responses during complicated cyber events, potentially causing significant damage to the country's critical infrastructure.

Fourthly, the National Critical Information Infrastructure Protection Centre (NCIIPC), set up under Section 70A of the IT Act[30], is meant to act as the nodal agency for safeguarding India's critical information infrastructure. It plays a central role in identifying CII sectors such as energy, banking, telecom, and defence and issuing cybersecurity guidelines to their operators. However, the classification of critical systems remains opaque, and CII protection guidelines are not always legally binding. Moreover, NCIIPC's advisory role lacks operational teeth during real-time incidents, especially in the absence of a legally mandated crisis response framework that cuts across military and civilian domains.

Furthermore, the CERT-In, the Indian Computer Emergency Response Team, is the national nodal agency that coordinates responses to cybersecurity incidents. It monitors threats, issues alerts and advisories, conducts incident analysis, and supports recovery efforts. Recent amendments to the CERT-In guidelines (2022)[31] have expanded reporting obligations and introduced a six-hour breach notification rule for service providers and data centres. While this marks progress in responsiveness, CERT-In still lacks statutory powers to enforce its directives beyond the IT Act's administrative reach. This lack of enforcement powers could hinder CERT-In's ability to ensure compliance with its directives, especially in cases where the IT Act does not apply. Importantly, it does not have jurisdiction over military systems or classified networks, where cyberwarfare concerns are most acute.

Finally, India's Ministry of Home Affairs (MHA) has also become increasingly active. The MHA's Cyber and Information Security (CIS) Division oversees multiple branches, including the Indian Cyber Crime Coordination Centre (I4C), which focuses on cybercrime prevention, investigation tools, and capacity building[32]. However, its primary mandate is civilian law enforcement, not strategic cyber defence or deterrence. The military's cyber units, such as the Defence Cyber Agency (DCyA), established in 2019, operate more discreetly under the

[30] The Information Technology Act, 2000, §70A
[31] Indian Computer Emergency Response Team, No. 20(3)/2022-CERT-In, (Issued on Apr. 28, 2022) https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited July 30, 2025)
[32] Ministry of Home Affairs, Cyber and Information Security (C&IS) Division, MHA https://www.mha.gov.in/en/divisionofmha/cyber-and-information-security-cis-division (last visited July 30, 2025)

Integrated Defence Staff and focus on both defensive and offensive cyber capabilities[33]. However, they do not operate under any public statute or clearly defined legal mandate, which makes institutional accountability and democratic oversight challenging.

What becomes clear here is that the legal and institutional framework lacks a central, integrative structure. Most agencies operate in parallel, with narrow interoperability. This fragmented architecture raises concerns about coordination during complex cyber events, such as simultaneous attacks on a private telecom provider, a public sector bank, and a military communications node. While individual agencies like NCIIPC or CERT-In may respond to sector-specific breaches, a broader national cyber command structure with clearly defined legal powers still remains missing.

Now, turning to broader policy instruments, the National Cyber Security Policy (NCSP) of 2013 was India's first official attempt at laying down a vision for cybersecurity. It set out goals like creating a secure cyberspace, developing a skilled workforce of 500,000 professionals, and establishing a national cyber coordination centre[34]. However, the policy was aspirational and lacked reasonable timelines or accountability mechanisms. It is also founded on a narrow basis without anticipating the military and geopolitical dimensions of cyberwarfare. Efforts to update this policy have been ongoing for years, with several draft versions leaked but never formally adopted. The gap between policy articulation and implementation continues to be wide. There have been some newer strategic initiatives. The National Cyber Coordination Centre (NCCC), operated by the Ministry of Electronics and Information Technology (MeitY), is intended to function as a real-time internet traffic monitoring platform to detect and mitigate threats. Critics, however, argue that the NCCC's legal framework is weak, its mandate is unclear, and its oversight is limited as well. There is concern over how surveillance powers may be exercised without adequate transparency or checks[35]. The potential misuse of these surveillance powers could lead to privacy and civil liberties violations, undermining public trust in the NCCC's operations.

On the defence side, the 2020 Defence Cyber Agency[36] is part of India's shift towards

[33] Drishti Gupta, Digital Defence: India's Cybersecurity Landscape, Defence Research and Studies, (Aug. 27, 2024) https://dras.in/digital-defence-indias-cybersecurity-landscape/ (last visited July 30, 2024)
[34] MeitY, National Cybersecurity Policy, Issued on 2013
[35] Zachary Keck, India Sets up Domestic PRISM – Like Cyber Surveillance ?, The Diplomat (Jun. 14, 2013) https://thediplomat.com/2013/06/india-sets-up-domestic-prism-like-cyber-surveillance/ (last visited Jul. 30)
[36] Arindrajit Basu, India's International Cyber Operations, pg. 2, UNIDIR, (Issued on 2022) https://unidir.org/wp-content/uploads/2023/05/UNIDIR_India_International_Cyber_Operations.pdf (last visited

integrated theatre commands, and it has reportedly been tasked with developing offensive cyber capabilities. However, these developments remain opaque, and unlike countries such as the US (with its Cyber Command)[37] or the UK (with its National Cyber Force)[38], India lacks an articulated cyberwarfare doctrine. This absence makes it difficult to assess how cyber operations are integrated into broader strategic planning, what legal constraints they are subject to, or how responsibilities are divided between civilian and military spheres. Internationally, India has been cautious[39]. It supports the UN Group of Governmental Experts (GGE) recommendations and has participated in the Open-Ended Working Group (OEWG) on cybersecurity[40]. However, it has yet to set global norms on state behaviour in cyberspace. India has signed limited bilateral cyber cooperation agreements with countries like the US, France, Israel, and Australia. This position, while understandable, limits India's engagement in shaping the international legal order around cyberwarfare.

Despite these gaps, some efforts are being made to draft a National Cybersecurity Strategy. The draft, prepared by the National Security Council Secretariat, reportedly calls for a dedicated cyber command, a national cyber registry, and legal reforms[41]. However, it has been stuck in review stages for years, and until it is adopted, India's cybersecurity posture will continue to rely on fragmented policies and ad hoc responses. To conclude, India's legal, institutional, and policy architecture for dealing with cyber threats is growing but still lags behind the complexity and scale of potential cyberwarfare. While the IT Act, DPDP Act, and sectoral guidelines lay down the basic legal structure, they fall short of addressing interstate cyber conflict, cross-sector coordination, and offensive capabilities. Institutional bodies like CERT-In, NCIIPC, and the DCA play vital roles, but often operate without a unified legal clarity. Moreover, while policies like the NCSP 2013 laid a foundation, their outdated frameworks highlight the urgent need for an integrated and forward-looking strategy. As cyber

July 30)

[37] Cyber Command of US Army, Homepage - https://www.arcyber.army.mil/

[38] UK Govt, The National Cyber Force: Responsible Cyber Power in Practice, p.1 https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf (last visited July 30)

[39] Statement delivered by India at OEWG session, Developments in the field of Information and Telecommunications in the context of International Security' in New York, (Jun. 3, 2019), pmindiaun.gov https://pmindiaun.gov.in/Cdgeneva/statement_content/NDA2 (last visited July 30)

[40] CCDCOE, A surprising turn of events: UN creates two working groups on cyberspace, CCDOE(n.d.) https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/ (last visited July 30)

[41] Data Security Council of India, National Cyber Security Strategy 2020, Issued on 2020 https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf (last visited July 30)

threats evolve rapidly, especially in light of AI, quantum computing, and hybrid warfare, India cannot afford to treat cyberwarfare as an afterthought. What is needed is a clear, enforceable legal mandate that connects policy vision with institutional readiness and operational capability. India can only move from a reactive stance to a truly resilient and strategic cyber power.

5. Global Cyberwarfare Models: Where does India Stand?

India is not alone in facing legal ambiguity and institutional growing pains in Cyberwarfare. However, valuable lessons must be learned from the structures of other major powers, especially the US, China, Russia, and the EU, which have a dedicated mechanism for cyberwarfare. While not perfect, their experiences, provide sound difference to India's current position and offer a promising path for future development.

Firstly, the United States is arguably the most open and structured when it comes to cyber operations. The US Cyber Command (USCYBERCOM), formed in 2009, operates under a clear legal and operational mandate within the Department of Defence of the US. It is responsible for defending military networks and also for carrying out offensive cyber missions. US law also, particularly through Presidential Policy Directives and the National Defence Authorisation Acts, directly lays out how cyberwarfare fits into broader military and strategic goals of the US[42]. What is to be noted here is the level of clarity around roles, rules of engagement, and oversight in the organisation, which India has not come close to.

Secondly, China, on the other hand, takes a far more centralised and ambiguous approach. Its cyber strategy is integrated into its military doctrine. The People's Liberation Army (PLA) has entire divisions focused on "informationised warfare[43]." Their emphasis is on maintaining control, state surveillance, and integration between civilian and military infrastructure. While this model is not one that is suitable for India as it is, given its implications for civil liberties, it definitely offers a case study of how a centralised command structure can rapidly increase capacity and coordination against cyber threats[44]. India's current system, with multiple agencies

[42] Switzer Robert & Catherine Theohary, Defense Primer: U.S. Cyber Command (USCYBERCOM), Congress.gov (25 May, 2025), https://www.congress.gov/crs-product/IF13042 (last visited July 30)
[43] Richard A. Bitzinger, China's love affair with 'informationized warfare' Asia times, (25 Feb. 2018) https://asiatimes.com/2018/02/chinas-love-affair-informatized-warfare/# (last visited July 30)
[44] Eric C. Anderson & Jeffrey G., Capabilities of the Chinese People's Liberation Army to Carry out Military Action in the Event of a Regional Military Conflict, SAIC, (March 2009) https://www.uscc.gov/sites/default/files/Research/CapabilitiesoftheChinesePeople%27sLiberationArmytoCarry

operating in parallel, lacks the same.

Thirdly, Russia follows a hybrid model somewhere in between. It has strong offensive cyber capabilities, usually operating through Non-state actors and groups. Unlike other countries, much of Russia's cyber activity exists in the murky zone, so it is disruptive but deniable[45]. Their legal frameworks are either unclear or integrated within military secrecy this is done deliberately as, this policy allows for flexibility but it blurs the line between cybercrime and state actions.

Fourthly, the European Union, has exercised unified cybercommand mainly through countries like Estonia and Germany, it placed significant emphasis on establishing legal clarity and promoting international cooperation. The General Data Protection Regulation (GDPR) by EU sets high standards for data privacy. Furthermore, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Estonia, has put up to the development of *Tallinn Manual*. Though this manual is not legally binding, it provides explicit guidelines on how international law applies to cyberwarfare. It defines what qualifies as an 'armed attack' or 'use of force' in cyberspace, or when a state can respond with force in the context of cyberspace. India, while supportive of the United Nations GGE operation, is yet to completely engage with frameworks like the Tallinn Manual.

It is crucial, then, to assess where India stands within this evolving global landscape. At the moment, India appears cautious. There is no official cyberwarfare doctrine. Offensive capabilities are being developed, but with very little legal or parliamentary oversight. Inter-agency coordination remains patchy. However, this cautious approach also ensures that India does not rush into a cyberwarfare model that might not be suitable for its unique geopolitical and socio-economic conditions. Compared to the US, India lacks a well-defined command structure. Compared to China, it lacks integration. Compared to the EU, it lacks legal clarity and international alignment. That said, India does not need to mimic any one model. Instead, it can build a hybrid system, rooted in democratic accountability like the EU, with strategic clarity like the US, and capacity-building focus like China. However, to do that, it first needs to acknowledge that cyberwarfare is no longer an emerging threat. It is already here. What

OutMilitaryActionintheEventofaRegionalConflict.pdf (Last visited July 30)

[45] Janne Hakala & Jazlyn Melnychuk, Russia's strategy in Cyberspace, NATO CCDCOE, (June, 2021) https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf (Last visited July 30)

matters now is how quickly and thoughtfully India adapts to this new reality.

6. Recommendations: Getting India Ready for Cyberwarfare

India has made progress in recognising the threat of cyberwarfare, but lacks a coordinated strategy. Ineffective legal provisions, segregated agencies, and no dedicated doctrine leaves the country vulnerable.

To begin with, the IT Act, 2000, was not built for war. It is helpful in dealing with cybercrime, fraud, and data breaches, but it does not cover things like state-sponsored attacks, military cyber operations, or rules for retaliation. We currently use a law designed for cyber hygiene to fight cyber battles. This inadequacy could lead to ineffective responses and potential escalation of cyber conflicts. That is not enough. India needs a specific law that defines what cyberwarfare is, outlines what the state can and cannot do, and sets out clear legal boundaries for both defensive and offensive operations. It should also tackle complex questions like what counts as a cyber "armed attack," how and when retaliation is allowed, and who gets to decide. Most importantly, this law should include oversight mechanisms, whether through parliamentary review, judicial checks, or independent audits, to prevent misuse.

Secondly, India has a number of agencies involved in cyber issues: CERT-In, NCIIPC, the Ministry of Home Affairs' cyber division, defence cyber units, and more. They all do important work, but there is too much overlap and not enough coordination. Information sharing is slow. Response times are patchy. Moreover, during a real cyber conflict, confusion can cost us dearly. India should establish a unified, centralised cyber command ideally under the National Security Council that brings together defence, intelligence, civilian, and private-sector stakeholders. This would streamline operations, improve response times, and enhance coordination during cyber incidents. It does not mean striking current policy and institutions, but rather integrating them all under a single strategic command structure with well-defined roles and responsibilities. This body should be equipped to lead both defensive and offensive cyber operations and coordinate with local governments and private players when needed.

Thirdly, India's present laws do not clearly define things like state attribution, private sector responsibilities during cyber incidents, or how international law applies to cyberattacks. For instance, if a foreign state targets Indian banks or power grids, how does India respond? Who investigates? What counts as enough evidence? These things need to be clarified. A practical

first step would be to issue a set of official rules of engagement akin to the Tallinn Manual, but tailored to India's legal and strategic needs. The manual does not need to be legally binding at first. It can start as a doctrine or white paper that outlines when India considers a cyber operation an act of war, how proportional responses work, and how attribution is handled.

Fourthly, A lot of the focus in cyber policy tends to be on tools and firewalls. However, the truth is, India's biggest challenge is not a lack of technology; it is a lack of trained people. There are just not enough cybersecurity experts, forensic analysts, and military cyber specialists. The government should invest in creating cyberwarfare academies or centres of excellence within existing institutions like the National Defence Academy or IITs. Training should also extend to state police forces, civil servants, and legal professionals, so that capacity exists across the system, not just in elite pockets. More importantly, there needs to be a pipeline to attract and retain talent. Presently, the majority of skilled professionals are in the private sector or overseas. Offering competitive salaries, incentives, and opportunities for research within government roles would help keep talent within the government.

Furthermore, many of the systems that are most vulnerable to cyberwarfare, banking networks, power grids, and telecom infrastructure, are run by private entities. However, during a national cyber incident, these companies often do not know who to talk to or what to do. There is no transparent chain of command, and no formal mechanism for cooperation. This needs to change. India should create standing cyber coordination units at both the central and state levels, with designated contact points from essential sectors. These units should run joint simulations, create protocols for sharing information, and even draft sector-specific guidelines. The private sector is not just a stakeholder; it is part of the battlefield and a crucial ally in defending our national cyber infrastructure. Bringing it into the national cyber strategy is long overdue.

Additionally, India has been cautious about joining international frameworks like the Budapest Convention or fully endorsing the Tallinn Manual. Part of this is understandable, as many of these frameworks were created without Global South participation. However, staying on the sidelines has its downsides, too. It limits India's ability to shape the global rules of the road for cyberwarfare. India should play a more proactive role in platforms like the UN Open-Ended Working Group (OEWG) and take leadership in suggesting norms that harmonise national security, digital sovereignty, and civil liberties. Bilateral and regional cooperation, especially

with Quad partners and neighbouring countries, should also be a priority. Cyber threats do not respect borders, and our response mechanisms should not either.

Besides, cyberwarfare is not going away. If anything, it is going to get messier, faster, and more sophisticated. That is why India needs to treat cyber preparedness not as a one-time project, but as a constantly evolving mission. Regular policy reviews, updated threat assessments, scenario-based planning, and independent audits should all be built into the system. Laws need to evolve with technology. Institutions need to adapt with time. And above all, cyberwarfare should become a mainstream concern, not something buried in technical committees or left to IT departments.

7. India's Cyberwarfare Preparedness: A Way Forward

India's rapid digital advancement has not only brought progress but also heightened the risk of cyberwarfare. While India acknowledges this growing risk, its present laws and institutions are inadequate to cope with the same. The focus primarily remains on cybercrime, overlooking the more significant and intricate issue of state-sponsored attacks or digital warfare.

The Information Technology Act, 2000, laid some important groundwork but does not go far enough. It was not built to deal with military-grade cyber threats. Moreover, while helpful for privacy, the newer Digital Personal Data Protection Act, 2023, does not touch the national security side of things. That leaves us with a legal gap, especially in situations that call for clear rules on responding when another country targets our digital infrastructure. On the institutional front, we do have important players like CERT-In, NCIIPC, and the Defence Cyber Agency. They are doing valuable work but often work in separate lanes. There is no single place where everything comes together. That disconnection makes it harder to respond quickly and effectively when a serious cyber threat hits. India needs to shift its perspective on cyberwarfare from a secondary issue to a primary focus. A dedicated law that clearly outlines roles, responsibilities, attack identification, attribution, and defensive and offensive responses and strategies is essential. A unified cyber command, ideally under the National Security Council, can foster a sense of unity and ensure that everyone is working towards a shared goal. This ensures that coordination should be the standard and not a special case.

It would also help if India aligned more with global legal thinking around cyberwarfare. Building a stronger talent pool of cyber experts and working closely with the private sector

should be a priority, too. For instance, the private sector can provide expertise in developing and implementing cybersecurity solutions, as well as in training and capacity building. After all, the government does not run many critical systems, and they need to be part of the conversation. This all adds up to a simple point: India cannot afford to wait. Cyberwarfare is no longer a distant or future problem; it is already here and will only grow more complex. If India wants to protect its national security, digital infrastructure, and global standing, it must treat this as a serious, strategic issue. The tools and institutions are there. What is needed now is clarity, coordination, and commitment.

So the question is: What should come first? A new law? A unified command? Better training? Probably all of it is in the correct order. However, what matters most is that we stop hesitating and start building the system we need.

.