CENJOWS

ISSUE BRIEF
IB/37/26

THE CHANGING CHARACTER OF WARFARE IN THE CYBER ERA: IMPLICATIONS FOR INDIA

COL VIVEK NAUTIYAL (RETD)

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

The Changing Character of Warfare in the Cyber Era: Implications for India

Col Vivek Nautiyal (Retd) is a senior fellow at CENJOWS

Abstract

The character of warfare is undergoing a structural transformation driven by the integration of cyberspace into the functioning of modern states, economies, and military establishments. This article examines how three interconnected aspects of this transformation affect India's national security. First, it traces the evolution of cyber-enabled conflict from 1970s information warfare debates to landmark incidents like Estonia (2007), Georgia (2008) and Stuxnet (2010), demonstrating how cyberspace has become a critical domain of strategic competition. Second, it analyses the strategic, operational and force modernisation implications of this domain for India, including the cyber-nuclear stability challenge in South Asia, the exploitation of India's expanding digital attack surface by state-sponsored adversaries such as China's RedEcho group and Pakistan's Transparent Tribe (APT36) and the cyber vulnerabilities introduced by India's ongoing military modernisation. Third, it makes the case for integrated cyber defence (covering inter-service, civil-military and industry-academic integrations) as a strategic necessity, arguing that India's current institutional architecture, centred on the Defence Cyber Agency established in 2019, falls short of the unified command structure that the threat environment demands. The article concludes that

India’s cyber challenge is fundamentally one of integration: translating significant but fragmented technical and institutional capacity into a coherent, resilient, and responsive national cyber defence framework.

Keywords: Cyberspace, Cyber Warfare, National Security, Cyber Domain, Integrated Cyber Defence, Defence Cyber Agency, Cyber Security, Inter-Service Integration

Introduction: Warfare in the Age of Invisible Contestation

Warfare is undergoing a profound and enduring transformation. The decisive contests of the twenty-first century are no longer confined to physical battlefields defined by geography, terrain, and visible force. Increasingly, they unfold within an invisible yet pervasive domain, across networks, systems and data flows that support the functioning of modern states and societies. This shift marks not simply the emergence of a new set of tools but redefines how power is exercised and contested.[1]

At its core, this transformation is structural rather than merely technological. The integration of digital technologies into governance, economic systems, critical infrastructure and military capabilities has created an environment in which national power is deeply dependent on cyberspace. Financial systems operate on digital networks; energy grids are managed through industrial control systems; military command and control rely on secure data links; and governmental authority increasingly depends on the integrity of information systems. In such an environment, vulnerabilities in cyberspace translate directly into vulnerabilities in national security.

This growing dependence has altered the very character of conflict. Unlike traditional warfare, which is limited to finite periods of kinetic action and often geographically bounded, cyber conflict is persistent. It unfolds continuously, frequently below the threshold of armed conflict and without boundaries. States are now able to impose costs, gather intelligence, shape perceptions and signal intent without resorting to overt military action. The result is a condition of enduring strategic competition that is constant, multidimensional and only partially visible to policymakers and the public alike.

A defining feature of this environment is ambiguity. Attribution in cyberspace remains technically complex and politically contested, allowing actors to operate with a degree of

plausible deniability. This, in turn, complicates traditional deterrence models, which rely on the ability to identify an adversary and respond credibly. The ambiguity inherent in cyber operations lowers the threshold for action, enabling states and non-state actors alike to engage in activities that would be considered escalatory in the kinetic domain.

For India, this transformation is not an abstract or future concern rather it is an immediate strategic reality. Over the past decade, India has undergone rapid digitalisation across multiple sectors. Government initiatives aimed at expanding digital governance, financial inclusion and technological innovation have significantly increased connectivity and efficiency.[2] At the same time, these developments have expanded the country's attack surface. Critical infrastructure systems, financial networks, and defence capabilities are now increasingly reliant on interconnected digital platforms.[3]

This duality of enhanced capability coupled with increased vulnerability lies at the heart of India's cyber challenge. Cyber intrusions, espionage campaigns and probing attacks against critical systems are no longer hypothetical risks; they are active elements of the strategic environment. Adversaries are able to exploit these vulnerabilities not only for intelligence collection but also for coercive signalling and strategic influence.

Understanding the changing character of warfare in the cyber era is, therefore, not merely an academic exercise but a necessity from a national security point of view. This article examines the evolution of warfare into the cyber domain, traces the emergence of cyberspace as a distinct operational environment and analyses the implications of these developments for national security and military operations, with particular emphasis on India.

The Evolution of Warfare into the Cyber Domain

The history of warfare is, in a fundamental sense, a history of information. From the ancient beacon fires to the telegraph networks that coordinated industrial-age Armies, the ability to communicate faster and more securely than an adversary has always given a decisive advantage. What distinguishes the cyber age is not merely speed but the degree to which information infrastructure has become both the backbone of modern society and the primary target of strategic warfare.

The transition to cyber-enabled conflict did not arrive suddenly. Its intellectual antecedents lie in the information warfare debates of the 1970s and 1980s, when theorists at institutions such as the RAND Corporation began systematically examining how computer networks could be exploited or disrupted to gain strategic advantage. Thomas Rona's 1976 study for Boeing, 'Weapon Systems and Information War,'[4] is widely credited as among the first serious treatments of information as a weapon system in its own right. By the 1990s, the United States Department of Defence had formalised the concept of Information Operations,[5] and the Gulf War of 1990–91, which is sometimes called the 'first information war', demonstrated in operational terms how the integration of electronic warfare, precision targeting and command-and-control disruption could achieve a decisive, asymmetric outcome.[6]

The emergence of the internet as a global common in the 1990s, however, introduced something qualitatively different from earlier information warfare. It created a vast, interconnected and largely ungoverned space in which state and non-state actors could operate with unprecedented reach, anonymity and deniability. Critical infrastructure, including power grids, financial systems, telecommunications networks and water treatment facilities, migrated to internet-connected systems, thereby expanding the attack surface available to hostile actors. What had been a domain of military communication became a domain of national vulnerability.

The first widely documented instance of cyber operations being used in a manner directly analogous to an act of war occurred in Estonia in April and May 2007.[7] Following the Tallinn government's decision to relocate a Soviet-era war memorial, a sustained campaign of Distributed Denial of Service (DDoS) attacks targeted Estonian government ministries, banks, newspapers and broadcasters. The attacks, widely attributed to the Russian state or state-affiliated actors despite Moscow’s denials, paralysed the digital infrastructure of a highly connected nation for nearly three weeks. This demonstrated that a state could be strategically coerced through cyber means without a single shot being fired.

The following year, during the Russo-Georgian War of August 2008, cyber operations were employed in direct coordination with conventional military action for the first time in a documented conflict.[8] Russian cyber operations preceded and accompanied the military advance into South Ossetia, degrading Georgian government communications, disabling

the websites of key state institutions and disorienting the information environment. This was not cyber warfare as a substitute for conventional force; it was cyber warfare as a force multiplier and enabler, a model that has since become doctrinal for several major militaries.

The Stuxnet operation, discovered in 2010 and widely attributed to the United States–Israeli collaboration targeting Iran's Natanz uranium enrichment facility, represented a watershed in the evolution of cyber as an instrument of statecraft.[9] For the first time, a cyber weapon had caused verifiable physical damage, destroying a number of Iran's centrifuges, without any kinetic military action. Stuxnet demonstrated that cyber operations could achieve strategic effects previously reserved for air strikes or special operations and it did so covertly, below the threshold of armed conflict. The implications for deterrence theory, arms control, and the laws of armed conflict were, and remain, profound.

Since Stuxnet, the operational use of cyber capabilities has expanded dramatically in scale, sophistication and ambition. The 2014 destructive attack on Sony Pictures Entertainment[10] by North Korean actors, the 2015–16 intrusions into the Democratic National Committee[11] attributed to the Russian intelligence services, the 2017 NotPetya[12] malware campaign (initially targeted at Ukraine but caused an estimated ten billion US dollars in global damages) and the 2020 SolarWinds[13] supply-chain compromise affecting dozens of United States federal agencies and hundreds of private sector organisations collectively illustrate the breadth of the cyber threat landscape. These were not isolated incidents; they were episodes in an ongoing, low-intensity, permanent campaign that major powers now conduct against one another as a matter of routine.

For India, the evolution of this domain holds urgent and strategic relevance. The April 2021 attempted cyberattack on the Mumbai power grid, attributed by investigators as to a Chinese state-sponsored threat group designated RedEcho,[14] occurred in the weeks following the military standoff at Galwan. Whether or not the attack was directly linked to the Galwan crisis, its timing underscored a strategic logic that Indian planners cannot afford to ignore: that adversaries will use cyber operations as instruments of coercion, signalling and escalation management in support of, as well as in parallel with, conventional military pressure.

Cyber as the Fifth Domain of Warfare

The formal recognition of cyberspace as a distinct domain of military operations is a development of the twenty-first century, though its conceptual foundations were laid in the preceding decades. The United States Department of Defence formally designated cyberspace as an operational domain in 2011, joining land, sea, air and space.[15] The North Atlantic Treaty Organisation (NATO) followed in 2016, formally recognising cyber as a domain of operations at the Warsaw Summit,[16] with member States affirming that a cyberattack could trigger the collective defence provisions of Article 5.[17] The United Kingdom, Australia, China, Russia, India and numerous other states have subsequently articulated doctrinal positions that treat cyberspace as a contested operational environment requiring dedicated military capability.[18]

The domain construct is more than taxonomic convenience. It carries significant doctrinal, organisational and resource implications. Designating cyberspace as a domain implies the need for dedicated forces trained and equipped to operate within it; a command structure with authority over cyber operations; a doctrine that governs the employment of those forces; and an acquisition system capable of developing and sustaining the relevant capabilities. It also implies parity of strategic consideration, meaning that cyber operations must be planned, resourced and integrated with operations in other domains with the same rigour applied to land, maritime, or air operations.

Cyberspace, however, is a domain with characteristics that distinguish it fundamentally from the physical domains of warfare. Four features are especially significant from a strategic and military perspective.

Ubiquity and Borderlessness

Unlike land, sea, air or even space, cyberspace has no natural boundaries corresponding to sovereign territory. An attacker in Beijing can reach a target in New Delhi in milliseconds, traversing multiple third-country networks in the process. The attribution of attacks is technically difficult and often politically contentious. This creates an environment wherein conventional concepts of sovereignty, self-defence, and proportionate responses are the foundation of the laws of armed conflict that are deeply strained.

Asymmetry of Offence and Defence

One of the most strategically consequential features of cyberspace is the inherent advantage it confers on the offence. With millions of lines of code, vast supply chains, and countless human operators, the sheer complexity of modern information systems means that attackers need to find and exploit only a single vulnerability to succeed, while defenders must protect against all possible attack vectors simultaneously. This asymmetry has profound implications for deterrence, and it becomes far harder to deter cyber aggression than to deter a conventional or nuclear attack.

Dual-Use Infrastructure

In cyberspace, the same infrastructure that enables civilian commerce, communication and governance, also supports military operations. Few examples are given as under:

- Military logistics systems rely on civilian telecommunications networks (e.g. BSNL).
- Intelligence collection leverages civilian social media and internet infrastructure.

This dual-use character means that cyberattacks on civilian infrastructure often may have military implications and vice versa. The distinction between civilian and military targets is fundamental to international humanitarian law and is extraordinarily difficult to maintain in the cyber domain.

The Speed of Operations

Cyber operations can be planned, launched, and executed in timeframes that leave human decision-makers with little time to respond. The 2017 NotPetya malware, for example, spread globally within hours of its initial release, disrupting operations at shipping giant Maersk, pharmaceutical company Merck and logistics provider FedEx before any of these organisations had fully understood what was happening. In a military context, this speed compresses decision cycles in ways that challenge established command and control architectures and create pressure for automated or autonomous defensive responses, along with attendant risks of escalation.

Within this domain, military cyber operations span a spectrum from intelligence collection at one end to destructive attack at the other, with a large middle ground occupied by influence operations, coercive signalling and operational preparation of the battlespace. The dominant form of activity for most major powers, most of the time, is persistent engagement i.e. the

maintenance of access to adversary networks for intelligence collection and potential future exploitation, rather than dramatic destructive attacks. This has led the United States Cyber Command to develop a doctrine (US Department of Defence Cyber Strategy 2018) of 'Defend Forward' and 'Persistent Engagement,' which holds effective defence of the American networks that require active operations in adversary networks to identify, track and, where necessary, disrupt hostile cyber actors before they can execute attacks.[19]

India's formal recognition of cyberspace as an operational domain has been evolving. The Defence Cyber Agency (DCyA), established in 2019 under the Integrated Defence Staff, represents a significant step toward dedicated military cyber capability.[20] However, the existing institutional architecture falls short of the unified, well-resourced cyber command that the threat environment demands.

The Impact on National Security and Military Operations

The integration of cyberspace into warfare has altered the character of conflict in ways that cut across all levels of the traditional spectrum like strategic, operational, and tactical. These challenges established frameworks for thinking about security, deterrence and the use of force.

Strategic Implications

At the strategic level, cyber capabilities have created new instruments of coercion that can be employed below the threshold of armed conflict. States can use cyber operations to signal resolve, impose costs, degrade adversary capabilities, or undermine domestic political cohesion without triggering the conventional military response that a kinetic attack would invite. This 'grey zone' of strategic competition, which is persistently contested, rarely acknowledged and difficult to attribute, has become a primary arena of great-power rivalry.

The concept of hybrid warfare is the integrated use of conventional military force, irregular tactics, information operations, economic coercion, and cyber operations, is most clearly illustrated by Russian doctrine and practice. But it is by no means exclusively a Russian phenomenon. China's concept of 'Three Warfares' (psychological warfare, public opinion warfare and legal warfare) explicitly integrates cyber-enabled information operations with conventional military strategy.[21] Pakistan's use of cyber capabilities in support of proxy operations against India, which includes the activities of groups such as the Transparent

Tribe (APT36) threat actor, represents a persistent, low-level cyber campaign that complements its broader strategy of sub-conventional pressure.[22]

Perhaps most significantly, cyber operations have introduced new complexities into nuclear deterrence stability. The same networks that enable nuclear command, control and communications (NC3) are potentially vulnerable to cyber penetration.[23] If a nuclear-armed state cannot be confident of the integrity of its NC3 systems under pressure, the stability assumptions that ensure deterrence are undermined. There is growing evidence that nuclear command, control and communications infrastructure across nuclear-armed states is increasingly exposed to cyber vulnerabilities, with several states known to have experienced intrusions targeting nuclear-related facilities.[24] In South Asia, where nuclear arsenals are relatively small, where the strategic community is less formally institutionalised and where conventional military crises recur with regularity, the cyber-nuclear interface deserves far more analytical attention than it has received.

Operational Implications

At the operational level, the impact of cyber on military operations is already evident and will only deepen as military systems become more digitally dependent. Modern military platforms, including fighter aircrafts, naval vessels, armoured vehicles and artillery systems, are increasingly networked, sensor-fused and software-driven. This creates both enormous operational capability and significant vulnerability. An adversary with access to the software or data links of a weapons system can potentially degrade, manipulate or destroy it without engaging it in conventional combat.

The 2007 Israeli air strike on Syria's Al-Kibar nuclear reactor, designated Operation Orchard, reportedly employed cyber operations to neutralise Syrian air defence radar systems before the strike, allowing Israeli aircraft to penetrate Syrian airspace undetected.[25] Whether or not this specific account is accurate in all its details, the operational concept it illustrates using cyber operations to suppress or blind adversary air defences as a precursor to kinetic action, is now a standard element of advanced military planning. India's own combat aircraft, air defence systems and command networks are potential targets for analogous operations by adversaries with advanced cyber capabilities.

Logistics and sustainment, which is often the decisive factor in extended conventional operations, is deeply cyber-dependent in modern militaries. Supply chain management systems, fuel and ammunition tracking, maintenance scheduling, medical records and personnel systems all rely on networked digital infrastructure. The disruption of these systems through cyberattack can degrade combat power without engaging frontline forces. The NotPetya attack's impact on Maersk, which forced the company to manually reinstall software on 45,000 computers and 4,000 servers to restore shipping operations, provide a vivid civilian illustration of the military logistics vulnerability.[26]

Impact on India's Military Modernisation

India's ongoing military modernisation programme, encompassing the induction of advanced platforms such as the Rafale fighter and the S-400 air defence system, as well as the expansion of the Indian Navy's carrier-based aviation, is increasing the country's military capability while simultaneously increasing its cyberattack surface. Advanced platforms are sophisticated cyber targets. The networks that link them to command centres, logistics systems and intelligence feeds are potential vectors for adversary exploitation.

The Indian Army's ongoing transition toward network-centric warfare through initiatives such as the Tactical Communication System (TCS) and the Battle Management System (BMS) will create a significantly more capable, but also more cyber-vulnerable, force. Ensuring the cybersecurity of these programmes, from acquisition through to operational deployment, requires a level of integration between the military, the defence industrial base and civilian cybersecurity authorities that has yet to be achieved. The risks of supply chain compromise i.e. the insertion of malicious hardware or software components into military systems by adversarial actors, are particularly acute for a country that remains heavily dependent on imported defence equipment.

The Need for Integrated Cyber Defence

The foregoing analysis establishes a clear strategic logic. First, cyber threats to India's national security are real, present and growing. These threats span the full spectrum from strategic coercion to tactical disruption. Furthermore, they are pursued by state adversaries with significant resources and sophistication. Finally, they cannot be adequately addressed by any single institution, ministry, or service operating in isolation.

The case for integrated cyber defence follows directly from these realities. This approach requires the coherent, coordinated and synergised deployment of military, civil and industry cyber capabilities under a unified strategic framework.

The concept of integration in this context has several distinct dimensions that are worth examining carefully because each captures a different dimension of the problem.

Inter-Service Integration

India's three-armed services, namely Army, Navy and Air Force, each have their own cyber establishments, priorities and operational requirements. The Defence Cyber Agency, created under the Integrated Defence Staff, was intended to provide a measure of tri-service coordination, but it remains under-resourced and without the authority or organisational reach to function as a genuine joint cyber command. Operations in the cyber domain are inherently joint, meaning a cyberattack on a naval base's logistics network will have implications for Army force sustainment and Air Force operational tempo. Effective defence requires a joint command architecture with the authority to plan, direct, and conduct integrated cyber operations across service boundaries.

Civil-Military Integration

The cyber domain does not respect the boundary between military and civilian infrastructure. India's critical national infrastructure, including the power grid, financial sector, telecommunications networks, oil and gas pipelines and water treatment systems, is almost entirely operated by civilian entities, whether government-owned or private. Yet its disruption would have immediate and severe military consequences. A sustained attack on India's power grid in the days preceding a conventional military operation, for example, could significantly degrade the mobilisation and sustainment of military forces. Protecting military capability therefore requires defending civilian infrastructure, which in turn requires deep and institutionalised civil-military coordination of a kind that does not presently exist in India.

CERT-In, the primary civilian national cybersecurity agency, and NCIIPC, responsible for protecting critical information infrastructure, operate largely in separate silos from the Defence Cyber Agency and the service cyber establishments. Information sharing between these bodies is intermittent and informal. Standard operating procedures for responding to

major cyberattacks include the escalation protocols that would determine when a cyberattack constitutes an act of war, requiring a military response, are either absent or inadequate. This civil-military disconnect is arguably the single most important structural vulnerability in India's cyber defence architecture.

Industry and Academic Integration

India's vibrant technology sector that is home to world-class software engineering talent, a growing start-up ecosystem and internationally competitive information security firms, represent a national asset that is almost entirely uncoupled from the country's defence cyber architecture. Major democracies have developed institutionalised mechanisms, like the US Cyber Command's collaboration with NSA and CISA, the UK's National Cyber Security Centre's engagement with private industry, and Israel's Unit 8200 alumni network's relationship with the defence technology start-up ecosystem that harness private sector cyber capability for national security purposes.[27] India has not yet developed comparable mechanisms, and the talent, innovation and capacity that could significantly strengthen the country's cyber defence remain largely disconnected from it.

Academic institutions, particularly the Indian Institutes of Technology, the National Institutes of Technology and specialised cybersecurity institutions such as C-DAC, represent a further resource that is inadequately integrated into the national cybersecurity architecture. The development of indigenous cyber capabilities (both defensive tools and, where appropriate, offensive capabilities) requires a sustained research and development investment that can only be achieved through deep and sustained collaboration between military establishments, government research agencies and academic institutions.

Doctrinal and Conceptual Integration

Integration is not merely organisational, but also doctrinal and conceptual. Effective integrated cyber defence requires a coherent national cybersecurity strategy that articulates objectives, assigns responsibilities, establishes priorities, and provides a framework for decision-making under pressure. It requires cyber doctrine that governs how military cyber forces will be employed and in what circumstances, under whose authority, within what legal constraints and in pursuit of what strategic objectives. It requires rules of engagement for cyber operations that are consistent with India's international legal obligations and that are clearly communicated, at least in general terms, to both domestic actors and adversaries.

And it requires an information-sharing architecture that allows threat intelligence to flow rapidly and securely among all relevant actors i.e. military services, civilian agencies, critical infrastructure operators and private sector partners.

The United States offers one model for integrated cyber defence, shaped by its unique political and resource landscape. This approach involved the establishment of US Cyber Command in 2010, its elevation to a Unified Combatant Command in 2018, and the concurrent evolution of the Cybersecurity and Infrastructure Security Agency (CISA) in the civilian domain. Israel provides a different model, defined by close integration between Unit 8200, the Shin Bet's National Cyber Bureau, and the nation's civilian technology ecosystem.

India's strategic environment, which is defined by its unique threats, institutional landscape, and constitutional framework, differs significantly from both the American and Israeli models. Consequently, any framework for integrated cyber defence must be tailored to these specificities. What is clearly established is the strategic imperative that makes such a framework not merely desirable, but essential. As the cyber domain becomes central to modern warfare, India's current institutional arrangements are increasingly inadequate to address the sophisticated threats it faces.

Conclusion: Integration as a Strategic Imperative

The character of warfare in the cyber era is defined by connectivity, complexity and continuous competition. The boundaries between domains, between civilian and military systems as also between war and peace are increasingly getting blurred. In this environment, traditional approaches to security are no longer sufficient. Cyber capabilities are now central to national power, shaping outcomes across the spectrum of conflict.

For India, the challenge is not merely to develop cyber capabilities but to integrate them effectively across the national security architecture. The country possesses significant strengths in technical expertise, institutional capacity, and strategic awareness, but these remain fragmented. India's cyber defence challenge is therefore fundamentally one of integration: bringing together disparate capabilities into a coherent, resilient and adaptive framework.

Achieving this will require more than incremental reform. It will demand institutional innovation, doctrinal clarity, sustained investment, and a shift in perspective from viewing cybersecurity as a technical issue to recognising it as a core element of national strategy. In the coming decades, India's ability to secure its digital infrastructure, protect its military capabilities and respond effectively to cyber threats will play a decisive role in shaping its strategic trajectory. The contest for advantage in cyberspace is already underway. The question is not whether India will engage in this contest, but how effectively it will do so.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

[1] Martin C. Libicki, What Is Information Warfare? (Washington, DC: National Defence University Press, 1995); John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!' Comparative Strategy 12, no. 2 (1993): 141–165.

[2] Ministry of Electronics and Information Technology (MeitY), India's Trillion Dollar Digital Opportunity (New Delhi: MeitY, 2019), https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[3] Government of India, Ministry of Electronics and Information Technology, National Cyber Security Policy, 2013 (New Delhi: MeitY, 2013); CERT-In, Annual Report 2022–23 (New Delhi: CERT-In, 2023), https://www.cert-in.org.in.

[4] Thomas P. Rona, Weapon Systems and Information War (Seattle, WA: Boeing Aerospace Company for the Office of the Secretary of Defence, 1976).

[5] US Department of Defence, Joint Publication 3-13: Information Operations (Washington, DC: DoD, 1998).

[6] Alan D. Campen (ed.), The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War (Fairfax, VA: AFCEA International Press, 1992); Fred Kaplan, Dark Territory: The Secret History of Cyber War (New York: Simon & Schuster, 2016), pp. 8–12.

[7] NATO Strategic Communications Centre of Excellence, Hybrid Threats: 2007 Cyber Attacks on Estonia (Riga: NATO StratCom COE, 2019), https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

[8] Stephen Korns and Joshua Kastenberg, 'Georgia's Cyber Left Hook,' Parameters 38, no. 4 (Winter 2008–09): 60–76.

[99] Institute for Science and International Security, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?' (Washington, DC: ISIS, 22 December 2010), https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant

[10] Federal Bureau of Investigation, Update on Sony Investigation, Press Release (Washington, DC: FBI, 19 December 2014), https://www.fbi.gov/news/press-releases/update-on-sony-investigation.

[11] Federal Bureau of Investigation and Department of Homeland Security, Joint Analysis Report: GRIZZLY STEPPE — Russian Malicious Cyber Activity, JAR-16-20296A (Washington, DC: FBI/DHS, 29 December 2016), https://www.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf

[12] Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (New York: Doubleday, 2019); Brookings Institution, 'How the NotPetya Attack Is Reshaping Cyber Insurance,' December 2021, https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

[13] US Government Accountability Office, 'SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response,' GAO Blog, 22 April 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[14] Insikt Group, Recorded Future, 'China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions,' 28 February 2021, https://www.recordedfuture.com/redecho-targeting-indian-power-sector/.

[15] U.S. Department of Defence, Department of Defence Strategy for Operating in Cyberspace (Washington, DC: DoD, July 2011).

[16] North Atlantic Treaty Organization, Warsaw Summit Communiqué, 9 July 2016, para. 70; NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'NATO Recognises Cyberspace as a Domain of Operations at Warsaw Summit,' https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

[17] North Atlantic Treaty Organization, Warsaw Summit Communiqué, 9 July 2016, para. 72.

[18] Ministry of Defence, Government of India, Joint Doctrine India 2017 (New Delhi: Headquarters Integrated Defence Staff, 2017), pp. 52–55.

[19] U.S. Cyber Command Public Affairs Office, 'Cyber 101: Defend Forward and Persistent Engagement,' U.S. Cyber Command, 17 August 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

[20] International Institute for Strategic Studies (IISS), Cyber Capabilities and National Power: A Net Assessment (London: IISS, June 2021), https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---india.pdf.

[21] Stefan Halper, China: The Three Warfares (Washington, DC: Office of Net Assessment, US Department of Defence, May 2013); Timothy A. Thomas, China's Evolving Military Strategy (Washington, DC: Potomac Books, 2017), pp. 134–158.

[22] CYFIRMA, 'APT Profile: Transparent Tribe aka APT36,' CYFIRMA Research, May 2025, https://www.cyfirma.com/research/apt-profile-transparent-tribe-aka-apt36/.

[23] Page Stoutland and Samantha Pitts-Kiefer, Nuclear Weapons in the New Cyber Age: Report of the Cyber-Nuclear Weapons Study Group (Washington, DC: Nuclear Threat Initiative, September 2018), https://media.nti.org/documents/Cyber_report_finalsmall.pdf.

[24] Beyza Unal and Patricia Lewis, Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences (London: Chatham House, January 2018), https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

[25] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Cyber Law Toolkit, 'Operation Orchard/Outside the Box (2007)', https://cyberlaw.ccdcoe.org/wiki/Operation_Orchard/Outside_the_Box_(2007).

[26] Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (New York: Doubleday, 2019), p. 204; see also Catalin Cimpanu, 'Maersk

Reinstalled 45,000 PCs and 4,000 Servers to Recover from NotPetya Attack,' Bleeping Computer, 25 January 2018, https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.

[27] Shmuel Even and David Siman-Tov, Cyber Warfare: Concepts and Strategic Trends (Tel Aviv: Institute for National Security Studies, May 2012), https://www.inss.org.il/publication/cyber-warfare-concepts-and-strategic-trends/.