CENJOWS

ISSUE BRIEF
IB/35/26

FROM BATTLEFIELDS TO BYTES: THE EVOLUTION OF DIGITAL MERCENARIES

DR MONOJIT DAS

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

From battlefields to Bytes: The Evolution of Digital Mercenaries

Dr Monojit Das is a senior fellow at CENJOWS

Abstract

For centuries, mercenaries have been the hired instruments of state and non-state power. Their tools changed from spears to rifles to private military contracts but their role did not: do the dangerous work that sovereigns prefer to outsource. Today, such outsourcing roles have migrated to a new domain. Cyberspace is now the arena where a new breed of digital mercenary operates, and the implications for global security, sovereignty, and strategic competition are profound. This article examines the historical arc of mercenary employment, the current crisis unfolding across conflict zones including server farms alike, and the trajectory of stateless cyber actors rewriting the rules of warfare itself. The article concludes with ten policy recommendations for India's national security architecture in the context of its Digital India programme.

Keywords: Mercenary, digital India, cyber security

The Long History of Hired Swords

The concept of a mercenary, or an individual who may be a professional soldier taking part in an armed conflict for personal financial gain and not for patriotism, is not a modern concept. Long before any standing army existed, rulers relied on warriors for hire to fill gaps in their military capacity. The Carthaginians employed Numidian cavalry and Iberian infantry throughout the Punic Wars, a practice documented extensively in Polybius's histories.[1] The Byzantine Empire maintained entire regiments of Varangian mercenaries drawn from Scandinavia, whose loyalty was to money rather than to a political cause.[2] Italian city-states of the Renaissance paid condottieri professional soldiers with their own retinues to fight wars that were too costly or politically inconvenient for their citizens to wage directly. Machiavelli devoted substantial sections of what made these arrangements attractive, is exactly what makes their digital descendants attractive today: deniability, flexibility, and cost-efficiency[3]. A mercenary could be dismissed, blamed, or disowned when the political winds shifted. The historian Anthony Mockler, in his comprehensive survey of mercenary history, notes that the relationship between the hiring sovereign and the hired sword was always defined by mutual convenience rather than mutual loyalty.[4]

The modern era of private military force began in earnest during the Cold War, when superpowers found it convenient to launder their interventions through proxy forces and private contractors. Executive outcomes in Angola and Sandline International in Sierra Leone operated in the grey space between state violence and corporate enterprise.[56] Singer's foundational work on the corporate warriors of the post-Cold War era documented how these firms' offered logistics, combat capability, and crucially provided a layer to cover the sponsoring government's official posture.[7]

The post-9/11 wars accelerated this trend dramatically. By the mid-2000s, private military contractors outnumbered regular US troops in Iraq. Companies like DynCorp, MPRI, and the now-infamous Blackwater or Academi operated with extraordinary latitude.[8] When Blackwater contractors killed seventeen Iraqi civilians at Nisour Square in September 2007, the legal and diplomatic fallout that led to criminal convictions that were subsequently overturned and re-litigated for over a decade significantly highlighted how ungoverned this space had become.[9] These episodes did not end the private military industry. They

transformed it. The industry became more sophisticated, more legally structured, and crucially, more interested in domains where physical accountability was harder to establish, where the most logical extension was cyberspace.

The Ongoing Crisis: A Hybrid Battlefield

We are currently living through a period that military strategists are still struggling to name properly. Terms like 'hybrid warfare,' 'grey zone conflict,' and 'multi-domain operations' point at the same uncomfortable reality: the boundaries between war and peace, between state action and criminal enterprise and between espionage and sabotage have dissolved. Hoffman's early conceptualisation of hybrid warfare anticipated precisely this blurring of conventional, irregular, and criminal activity within a single conflict.[10]

The Russia-Ukraine conflict, which escalated to full-scale invasion in February 2022 and has continued at devastating cost into 2026, is the defining case study of this era. Before a single tank crossed the border, Ukrainian infrastructure was hit by destructive wiper malware, WhisperGate and HermeticWiper, largely deployed with surgical precision to create confusion and paralysis.[11] Microsoft's threat intelligence team documented these attacks in real time, establishing that the malwares were designed not for financial gain but for maximum disruption.[12]

The IT Army of Ukraine, a volunteer hacker group that grew to include thousands of participants globally, conducted distributed denial-of-service attacks against Russian state websites, financial infrastructure, and media outlets.[13] Cyber conflict researcher, Thomas Rid has argued that this kind of mass cyber mobilisation represents a genuinely new form of political violence that existing international humanitarian law is poorly equipped to regulate.[14]

Russian-linked groups hit European energy infrastructure, satellite communications networks, and Western defence contractors. The attack on Viasat's KA-SAT network in the opening hours of the invasion caused large scale disruption in Ukrainian military communications and, as part of collateral damage, knocked out wind turbines across central Europe which further establishes that cyber operations in a major conflict would have effects far beyond the theatre of war.[15]

The Wagner Group, before its June 2023 mutiny and subsequent restructuring following Prigozhin's death, operated not just in kinetic domains across Africa and the Middle East but also maintained information warfare capabilities that blurred the line between paramilitary group and state proxy.[16]

Researchers at the Stanford Internet Observatory documented Wagner-linked influence operations across African social media platforms, involving coordinated inauthentic behaviour and locally tailored disinformation.[17]

In the Indo-Pacific region, groups like APT40, which is referred to by different entities with different names, like Leviathan, which is used by CrowdStrike; Bronze Mohawk by Secureworks, Gingham Typhoon used by Microsoft, etc, assessed by multiple Western intelligence agencies as operating under the direction of China's Ministry of State Security, functioning with a contractor model where skilled hackers were given operational guidance and resources in exchange for targeting particular networks.[18] A July 2021 joint advisory issued by the United States, the European Union, NATO (North Atlantic Treaty Organization), and allied partners formally attributed APT40 activity to the MSS, marking a significant moment of collective attribution.[19]

The Middle East presents yet another variant. Iranian-linked groups, cyber units affiliated with Hamas and Hezbollah, and various state-sponsored actors have created a layered digital conflict ecosystem that runs parallel to conventional military options.[20] The ClearSky research firm's documentation of Iranian cyber operations targeting Israeli critical infrastructure in the period following October 2023 illustrates how non-state cyber capacity feeds into broader regional confrontation without being directly controlled by any single sovereign.[21]

The Emerging Digital Mercenary Economy

The commercial architecture supporting this world is sophisticated and largely legal at the face of it. The global market for cyber capabilities includes offensive tools, intelligence services, and access brokers, including both individuals and organisations who specialise in gaining initial network access and then selling that access to the highest bidder.

Companies like NSO Group, the Israeli firm behind the Pegasus spyware platform, represent the most commercially visible end of this spectrum. Pegasus was marketed to governments as a counterterrorism and law enforcement tool. In practice, it was used to target journalists, opposition politicians, and human rights lawyers across dozens of countries.[22] The 2021 Pegasus Project, a consortium investigation coordinated by Forbidden Stories involving seventeen media organisations, documented surveillance of over fifty thousand phone numbers globally.[23]

Below the commercially visible tier sits a vast grey market. Exploit brokers like Zerodium publish public price lists for zero-day vulnerabilities in widely used software, comprising a remote code execution exploit for iOS with no user interaction required can fetch over two million US dollars.[24] Schneier has argued that this commercial market for vulnerabilities creates a structural conflict between governments' interest in stockpiling zero-days for offensive use and their obligation to protect their citizens' digital infrastructure.[25]

The ransomware-as-a-service ecosystem represents perhaps the most economically significant dimension of the digital mercenary market. Groups like LockBit, BlackCat/ALPHV, and their successors operate with near-corporate efficiency, providing affiliates with attack tools, negotiation infrastructure, and data leak capabilities in exchange for a percentage of ransom proceeds.[26] The FBI's 2024 Internet Crime Report estimated ransomware losses in the United States alone at over 59 billion dollars, though researchers believe this substantially understates actual economic impact due to under-reporting.[27] The most dangerous development is not that states are sponsoring cyber-attacks. It is that the market for offensive cyber capability has become sufficiently liquid that any sufficiently motivated actors, i.e. state, corporation, cartel, or ideological group, can acquire meaningful capability at commercially accessible price points.

This assessment, reflected across multiple intelligence community open-source publications, points to the core structural problem: the cyber mercenary economy has lowered barriers to entry for serious offensive capability to a degree that has no analogue in conventional military affairs.[28]

Looking Forward: Cyber Mercenaries and Global Instability

The trajectory of cyber mercenary proliferation is concerning, and worth attention. The proliferation of this capacity is not simply a technical problem; it is a structural challenge to the international order. Healey's work on conflict in cyberspace identifies the attribution problem as the central driver of escalation risk, i.e. when states cannot quickly and confidently identify the source of an attack, the risk of miscalculation increases dramatically.[29]

The 2016 Bangladesh Bank heist, where attackers linked to North Korea's Lazarus Group stole eighty-one million US dollars by compromising SWIFT (Society for Worldwide Interbank Financial Telecommunication) banking infrastructure, demonstrated that cyber-enabled financial warfare was not only possible but had already happened at scale.[30] The incident prefigures the kind of cross-domain escalation that could emerge from a genuine great-power crisis, ranging from a military confrontation that triggers financial cyber-attacks that cascade into the banking systems of uninvolved third parties. Artificial intelligence is accelerating every dimension of this problem. The cost of conducting sophisticated cyber operations is falling as AI-assisted tools makes attack automation cheaper and faster. Brundage and colleagues' foundational 2018 report on the malicious uses of artificial intelligence, which has proven remarkably prescient, identified automated attack tools, AI-enhanced social engineering, and AI-generated synthetic media as the three primary vectors of concern.[31] Each of these have now matured into operational reality.

The growing role of non-state actors makes this worse. Patriotic hacker collectives, ideologically motivated hacktivist groups, criminal organisations with political agendas, and privately funded information warfare shops, operating in the same space as state-sponsored groups. Lindsay and Gartzke's research on cross-domain coercion suggests that the introduction of cyber operations into conventional military crises tends to lower the threshold for escalation rather than providing stable deterrence, contrary to some earlier optimistic assessments.[32]

For India specifically, the strategic environment is particularly complex. Leading AI threat research firm Recorded Future in their 2020 research documented that Chinese state-linked actors designated RedEcho had pre-positioned themselves in at least twelve Indian power sector entities, raising the prospect of destructive attacks on civilian infrastructure as

leverage in a military confrontation.[33] The 2022 ransomware attack on AIIMS Delhi, which paralysed the hospital's systems for nearly a month, has already shown the lethal potential and the operational reality of these threats against critical civilian infrastructure.[34]

Governance, Accountability, and the Mercenary Problem

The international community has been slow to respond. The 2008 Montreux Document attempted to establish norms for the conduct of private military and security companies in armed conflict, but it is non-binding and largely irrelevant to cyber operations.[35] The UN Group of Governmental Experts process has produced some agreed norms for responsible state behaviour in cyberspace, the most recent being the 2021 GGE report, but enforcement mechanisms are absent, and non-state actors are entirely outside its scope.[36]

Some progress is being made at the tactical level. The January 2024 law enforcement operation against LockBit infrastructure, coordinated across ten countries and led by Europol and the US Department of Justice, temporarily disrupted one of the world's most prolific ransomware franchises.[37] But these operations are slow, resource-intensive, and ultimately reactive. LockBit resumed operations within weeks of the disruption. Eichensehr's analysis of the international law applicable to cyber operations identifies the core governance gap: existing frameworks were designed for state actors and physical domain conflicts and apply to cyber mercenaries only through contested doctrinal extension.[38] The Tallinn Manual process, while valuable as a scholarly exercise, represents expert opinion rather than binding law, and its applicability to non-state cyber actors remains disputed.[39]

For India, which faces an extraordinarily complex cyber threat environment from both state and non-state groups, the governance question is not abstract. India's IT Act of 2000, amended in 2008, and the subsequent frameworks developed under CERT-In (Indian Computer Emergency Response Team CERT-In), were not designed for the current threat landscape. The 2023 Digital Personal Data Protection Act represents a step forward on data governance but does not address offensive cyber operations or the mercenary economy.[40]

Recommendation

India, remains under constant threat not just from its belligerent countries but also from non-state actor groups, the existing acts or policies which are in place often fall short to address the evolving challenges. While developing or implementing of a legislation might take time, a few steps can be initiated under the PMO (Prime Minister's Office) to address the evolving nature of threats to India's cyber architecture.

- **Establish a National Cyber Command with Unified Authority**

  India's cyber defence remains fragmented across CERT-In under MeitY (Ministry of Electronics and Information Technology), the National Critical Information Infrastructure Protection Centre (NCIIPC) under NTRO (National Technical Research Organisation), tri-service cyber commands under each branch of the armed forces, and state police cybercrime units. The 2013 National Cyber Security Policy acknowledged this compartmentalisation but did not resolve it.[41] A single National Cyber Command with clear authority over both defensive and offensive capabilities is operationally necessary. Comparative analysis of US Cyber Command, the UK's National Cyber Force, and Israel's Unit 8200 suggests that unified command structures produce better outcomes in crisis response.[42]

- **Build a Sovereign AI-Powered Threat Intelligence Platform**

  India currently relies substantially on foreign commercial threat intelligence providers like Recorded Future, CrowdStrike, and Mandiant for intelligence about threats to its own critical infrastructure. This creates a strategic dependency that is incompatible with great-power status. The 2020 RedEcho report, produced by an American private firm, revealed Chinese pre-positioning in India's power sector before Indian government agencies had made a public assessment.[43]

  A domestically developed, AI-enabled threat intelligence platform, drawing on India's considerable software engineering talent base and anchored in the proposed National Cyber Command, would reduce this dependency.

- **Legislation Against Private Offensive Cyber Operations**

  India has no specific legal framework governing the purchase or deployment of offensive cyber tools by private actors. The IT Act does not explicitly criminalise the acquisition of spyware for use against Indian citizens by domestic entities.[44] Amnesty International's Security Lab documented Pegasus infections on Indian devices belonging to journalists and activists, including those associated with the Bhima Koregaon case.[45] Legislation modelled on the EU's proposed Cyber Solidarity Act, adapted to India's constitutional framework, should establish clear liability for the deployment of commercial spyware against Indian nationals regardless of who deploys it.

- **Mandate Critical Infrastructure Cyber Resilience Standards**

  The rapid expansion of Digital India especially the Unified Payments Interface (UPI), enabling the undertaking of instant payment system developed by the National Payments Corporation of India (NPCI), allows registered users to link multiple bank accounts into a single mobile application to facilitate immediate money transfers via a Virtual Payment Address (VPA) for over fourteen billion transactions monthly[46]. Interestingly the UPI accounts also hold the Aadhaar linked to individuals each of the accounts, government cloud services expanding rapidly are unintentionally creating a vulnerable target that is growing faster than defences are being built, leaving space for attacks. The 2022 AIIMS Delhi ransomware attack exposed the consequences of inadequate baseline security standards.[47] Binding minimum security standards, with mandatory incident reporting to CERT-In within six hours (already required but inconsistently enforced), regular third-party audits, and financial penalties for non-compliance, must replace the current voluntary approach.

- **Develop a Tri-Service Cyber Reserve and Force**

  India's active cyber security personnel across government are vastly outnumbered by the threat environment. The United Kingdom's Joint Cyber Reserve, which recruits from the private sector technology industry, provides a relevant model.[48] A structured Indian cyber reserve, drawing on the country's largest-in-the-world IT services workforce through a formal reserve commission programme, would create surge

capacity during crises without the fiscal cost of full-time equivalents. Clear rules of engagement for offensive cyber response in grey-zone scenarios stand analogous to the nuclear doctrine's no-first-use framework in conceptual terms that must accompany this capability.

- **Counter Information Warfare and Influence Operations**

  Pakistan and China originated information operations targeting Indian democratic processes, communal tensions and strategic narratives are extensively documented, with multiple instances when it is observed that accounts are linked to Pakistani state interests.[49] India needs a dedicated counter-influence capability housed within the proposed National Cyber Command with the authority to label, disrupt, and where legally appropriate, respond to foreign information warfare, efforts including synthetic media operations targeting Indian elections and communal relations.

- **Lead Multilateral Cyber Mercenary Norms in Global South Forums**

  India's G20 presidency in 2023 established a New Delhi Leaders' Declaration that referenced cyber security but stopped short of binding commitments on the regulation of offensive cyber tools. India's position in BRICS (Brazil, Russia, India, China, and South Africa), the SCO (Shanghai Cooperation Organization), and the UN GGE (United Nations Group of Governmental Experts) process gives it convening power that it has not fully exploited on cyber governance. Using these forums to advocate for binding norms on the export and use of offensive cyber tools largely analogous in architecture to the Arms Trade Treaty would serve Indian interests while positioning India as a responsible cyber power. Passivity on this agenda cedes agenda-setting to the US-EU bloc or, worse, to China.

- **Secure the Digital India Supply Chain**

  The Digital India programme's hardware and software components have substantial foreign provenance, including from Chinese manufacturers whose products have been flagged by multiple allied intelligence services. The Government of India's 2020 ban of 267 Chinese applications under Section 69A of the IT Act was a reactive measure taken under crisis conditions[50]; calling for a proactive supply chain security programme, which should include mandatory source code escrow and review for

software embedded in critical systems, hardware attestation requirements for government procurement, and active diversification away from single-country component dependencies for 5G infrastructure, surveillance systems, and public cloud services.

- **Establish a Classified National Cyber Attribution Centre**

  Indian government often depends on external agencies for ensuring comprehensive cyber security[51]. This forces dependence on US, UK, and Five Eyes intelligence assessments even thereby leaving doors open for a strategic vulnerability. A classified attribution centre drawing on NTRO signals intelligence, military cyber intelligence, and structured engagement with private sector forensics firms through a cleared contractor framework, can thereby enable India to make independent attribution calls. The ability to publicly attribute attacks is increasingly understood as a deterrence tool in itself.

- **Build a National Cyber Talent Pipeline**

  Sustained cyber power requires a deep talent base, not ad hoc recruitment. India graduates approximately 1.5 million engineers annually from its IIT, NIT, and affiliated institutions, but very few receive structured training in offensive and defensive cyber operations. A nationally funded programme linking IITs, the Indian Defence University (IDU) directorate under HQ IDS, and DRDO's cyber research establishment should create a pipeline of cyber security professionals with structured pathways into government service. The Israeli model of mandatory national service that routes top technical graduates through Unit 8200 and the subsequent creation of a world-leading private sector cyber industry demonstrates the long-term strategic and economic returns on this kind of investment.

Conclusion

The mercenary has always been a mirror held up to the state system being a key reflection of what states are unwilling or unable to do themselves. In the digital age, that mirror shows something genuinely new: a marketplace of violence that operates at the speed of light,

crosses borders without friction, and gives small and mid-sized actors capabilities that were once the exclusive preserve of major powers.

The net balance of the mercenary proliferation in cyberspace is negative for stability. More capable actors, lower barriers to entry, ambiguous attribution, inadequate governance frameworks, and accelerating technological change combine to create a threat environment that is structurally prone to miscalculation and escalation. Nye's concept of cyber power as a diffuse and difficult-to-monopolise resource captures why this problem is so intractable: unlike nuclear weapons, offensive cyber capability cannot be corralled by a small club of states.

Managing that environment and not eliminating it, which is not possible, but managing it is one of the defining security challenges of the coming decade. The condottieri of Renaissance Italy eventually gave way to professional standing armies because states recognised that unregulated hired force was ultimately incompatible with stable political order. Whether the international community can reach a similar conclusion about digital mercenaries and do so before a serious miscalculation triggers a crisis none of the parties wanted remains the open question of our era.

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] Polybius, The Histories, trans. Robin Waterfield (Oxford: Oxford University Press, 2010), Books I–III, on Carthaginian mercenary deployments during the First Punic War and the Mercenary War of 240–238 BC.

[2] John Haldon, The Byzantine Wars (Stroud: The History Press, 2008), 45–67. See also Sigfús Blöndal, The Varangians of Byzantium (Cambridge: Cambridge University Press, 1978).

[3] Niccolò Machiavelli, The Prince, trans. Harvey C. Mansfield (Chicago: University of Chicago Press, 1998), chapters 12–13, "Of Different Kinds of Troops and of Mercenaries."

[4] Anthony Mockler, The Mercenaries (London: Macmillan, 1970), 3–28

[5] Eeben Barlow, Executive Outcomes: Against All Odds (Johannesburg: Galago Publishing, 2010).

[6] Herbert M. Howe, Ambiguous Order: Military Forces in African States (Boulder: Lynne Rienner, 2001), 215–241.

[7] P.W. Singer, Corporate Warriors: The Rise of the Privatized Military Industry (Ithaca: Cornell University Press, 2001), 8–44.

[8] Christian Miller, "Contractors Outnumber Troops in Iraq," New York Times, July 4, 2007.

[9] David Isenberg, Shadow Force: Private Security Contractors in Iraq (Westport: Praeger, 2009), 88–112. On the Nisour Square legal proceedings, see United States v. Paul Alvin Slough et al., US District Court for the District of Columbia, Case No. 08-cr-00360.

[10] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington: Potomac Institute for Policy Studies, 2007), 14–29.

[11] Microsoft Threat Intelligence Center, "Destructive Malware Targeting Ukrainian Organizations," Microsoft Security Blog, January 15, 2022, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

[12] ESET Research, "HermeticWiper: New Destructive Malware Used in Ukraine," ESET WeLiveSecurity, February 24, 2022, https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

[13] Gavin Wilde and Justin Sherman, "The IT Army of Ukraine: Structure, Tasking, and Targeting," Lawfare, January 27, 2023, https://www.lawfaremedia.org/article/the-lawfare-podcast-gavin-wilde-and-justin-sherman-on-russia-s-information-war-and-regime-security

[14] Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020), 421–438.

[15] US Cybersecurity and Infrastructure Security Agency (CISA), "Advisory on Viasat KA-SAT Network Cyber Attack," AA22-076A, March 17, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a

[16] Jack Watling and Nick Reynolds, "Prigozhin's Gambit and the Future of Wagner," RUSI Commentary, June 27, 2023, https://www.rusi.org/explore-our-research/publications/commentary/prigozhins-gambit-and-future-wagner

[17] Stanford Internet Observatory, "Unheard Voice: Evaluating Five Years of Pro-Western Covert Influence Operations," August 24, 2022, https://fsi.stanford.edu/news/unheard-voice-evaluating-five-years-pro-western-covert-influence-operations. For Wagner-linked Africa operations specifically, see EU DisinfoLab, "Wagner Group's Disinformation Campaign in Africa," 2023

[18] FireEye/Mandiant, "APT40: Examining a China-Nexus Espionage Actor," March 2019, https://www.mandiant.com/resources/reports/apt40

[19] US Department of Justice, "United States and Allies Attribute Malicious Cyber Activity to China's Ministry of State Security," Press Release, July 19, 2021, https://www.justice.gov/opa/pr/united-states-and-allies-attribute-malicious-cyber-activity-china-s-ministry-state-security

[20] Collin Anderson and Karim Sadjadpour, "Iran's Cyber Threat: Espionage, Sabotage, and Revenge," Carnegie Endowment for International Peace, 2018, https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

[21] ClearSky Cyber Security, "Operation Shaheen and Iranian Cyber Offensive Activity Against Israeli Infrastructure," ClearSky Research Report, 2024 (restricted distribution; cited in public summaries).

[22] Claudio Guarnieri et al., "Forensic Methodology Report: How to Catch NSO Group's Pegasus," Amnesty International Security Lab, July 18, 2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/

[23] Forbidden Stories and Amnesty International, "The Pegasus Project," July 18–25, 2021. Published simultaneously across seventeen partner media outlets including Le Monde, The Guardian, and The Wire.

[24] Zerodium, "Our Exploit Acquisition Program," https://zerodium.com/program.html (accessed April 2026). The iOS full chain zero-click RCE price is publicly listed at $2.5 million.

[25] Bruce Schneier, Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World (New York: W.W. Norton, 2018), 83–102.

[26] Allan Liska and Timothy Gallo, Ransomware: Defending Against Digital Extortion (Sebastopol: O'Reilly Media, 2016). For current RaaS models, see Mandiant, "Ransomware-as-a-Service: The Business Model Behind Ransomware," 2023, https://www.mandiant.com/resources/ransomware-as-a-service.

[27] Federal Bureau of Investigation, Internet Crime Report 2023 (Washington, DC: FBI Internet Crime Complaint Center, 2024), 17–22, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[28] Director of National Intelligence, Annual Threat Assessment of the US Intelligence Community (Washington, DC: ODNI, 2024), 22–26, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

[29] Jason Healey, ed., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Vienna: Cyber Conflict Studies Association, 2013), 265–290.

[30] Kaspersky Lab, "Lazarus Under the Hood," April 3, 2017, https://securelist.com/lazarus-under-the-hood/77908/. See also United States v. Park Jin Hyok, US District Court for the Central District of California, Criminal Complaint, September 5, 2018.

[31] Miles Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," Future of Humanity Institute, University of Oxford, February 2018, https://arxiv.org/abs/1802.07228

[32] Jon R. Lindsay and Erik Gartzke, eds., Cross-Domain Deterrence: Strategy in an Era of Complexity (Oxford: Oxford University Press, 2019), 215–244.

[33] Recorded Future, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," February 28, 2021, https://go.recordedfuture.com/hubfs/reports/cta-2021-0228.pdf

[34] Indian Computer Emergency Response Team (CERT-In), "Ransomware Attack on AIIMS Delhi," Advisory CERT-In/C-1539, November 30, 2022.

[35] International Committee of the Red Cross, The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict (Geneva: ICRC, 2009)

[36] United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, Final Report, A/76/135 (New York: United Nations, 2021).

[37] US Department of Justice, "US and UK Disrupt LockBit Ransomware Variant," Press Release, February 20, 2024, https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

[38] Kristen Eichensehr, "The Cyber-Law of Nations," Georgetown Law Journal 103, no. 2 (2015): 317–380.

[39] Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed. (Cambridge: Cambridge University Press, 2017), 1–30.

[40] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Act, 2023 (New Delhi: MeitY, 2023), https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[41] Joseph S. Nye Jr., The Future of Power (New York: PublicAffairs, 2011), 113–151. See also Nye, "Cyber Power," Belfer Center Paper (Cambridge: Harvard Kennedy School, 2010).

[42] National Security Council Secretariat, Government of India, National Cyber Security Policy 2013 (New Delhi: Department of Electronics and Information Technology, 2013).

[43] Jason Healey and Karl Grindal, eds., A Fierce Domain: Conflict in Cyberspace 1986 to 2012 (Vienna: CCSA Press, 2013), 201–230. On UK National Cyber Force, see GCHQ, "A History of the National Cyber Force," 2023, https://www.gchq.gov.uk/information/national-cyber-force

[44] Information Technology Act, 2000 (as amended 2008), No. 21 of 2000, Government of India. Section 66B covers data theft but does not specifically address acquisition of offensive spyware tools. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[45] Amnesty International, "Pegasus Spyware Used to Surveil Activists Around Bhima Koregaon Case," October 2019, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/

[46] Subhojit Sarkar, “From Tea Stalls to 14 Bn Transactions, UPI’s Next Test Is Credit Access, Says Policybazaar’s Harsh Vardhan Masta,” *Fortune India*, April 18, 2026, https://www.fortuneindia.com/india/from-tea-stalls-to-14-billion-transactions-upis-next-test-is-credit-access-says-policybazaars-harsh-vardhan-masta/133073

47 “AIIMS Ransomware Attack: What It Means for Health Data Privacy,” ETCISO, December 27, 2022, https://ciso.economictimes.indiatimes.com/news/aiims-ransomware-attack-what-it-means-for-health-data-privacy/96538957

48 “Reserve Cyber Unit,” *Royal Navy*, accessed May 7, 2026, https://www.royalnavy.mod.uk/careers/roles/reserve-cyber-unit

49 IANS, “Pakistan Running Propaganda against India on Social Media,” Times of India, April 23, 2020, https://timesofindia.indiatimes.com/india/pakistan-running-propaganda-against-india-on-social-media/articleshow/75321469.cms

[50] Pankaj Doval, “43 New Chinese Apps Banned, 267 in All,” The Times of India, November 25, 2020, The Times of India https://timesofindia.indiatimes.com/business/india-business/43-new-chinese-apps-banned-267-in-all/articleshow/79397633.cms

[51] Ministry of External Affairs, Government of India, “The UK-India Technology Security Initiative,” last modified July 24, 2024, https://www.mea.gov.in/bilateral-documents.htm?dtl%2F37995%2FThe_UKIndia_Technology_Security_Initiative