RESEARCH PAPERS

Cyber Mercenaries: The Changing Character of Contemporary Warfare

Author: Ashutosh Kumar Singh • **Published:** July 29, 2026 • **Source:** Centre for New Age Warfare Studies



EXECUTIVE BRIEF & KEY FINDINGS

Mercenaries have remained an indispensable part of warfare throughout the history while adapting to shifts in political authority, military organisation and technological innovation. From the hired troops described by Kautilya in Arthashastra to the Condotteri system mercenary companies during European Renaissance and the Private Military Companies (PMCs) that proliferated after the Cold War, the practice of outsourcing military capabilities has gradually evolved alongside the changing character of war. The rise of cyberspace as a strategic domain has boomed cyber mercenary. Contrary to mercenaries selling their military capabilities and PMCs selling security and combat support, the commercialization of offensive capabilities via spyware, cyber espionage, exploitation of vulnerabilities and surveillance is at the heart of the business model of the cyber mercenaries. Cyber Mercenaries provides governments plausible deniability with specialised expertise making them important instruments of grey-zone and hybrid warfare. This article explores the historical evolution of Mercenary into cyberspace, the evolution of cyber mercenary ecosystem and how these actors are transforming contemporary warfare. The commercialisation of offensive cyber capabilities has significantly blurred the boundaries between public and private power, exposing significant challenges for international governance and national security. The article concludes by assessing the strategic implications for India and assessing existing cyber laws, governance and legal issues with Cyber Mercenary.

1. Introduction

War has always evolved alongside technology. The introduction of gunpowder transformed medieval warfare, industrialisation reshaped military organisation in the 19th century, and nuclear weapons redefined deterrence in the 20th. Today, cyberspace is driving another transformation. Cyber operations, digital surveillance, ransomware, influence campaigns and cyber espionage have become integral to interstate competition, enabling states to pursue strategic objectives without crossing the threshold of conventional armed conflict. As a result, the battlefield now extends beyond land, sea, air and space into a domain where information, software and digital infrastructure have become instruments of national power.

This transformation has also altered the actors involved in conflict. The state's monopoly over organised violence and intelligence capabilities is increasingly challenged by private entities with specialised technological expertise. Among the most significant are cyber mercenaries—private firms and individuals that develop, market or deploy offensive cyber capabilities for governments and other clients. By providing services such as spyware, cyber espionage, network intrusion and vulnerability exploitation, they have created a commercial market for offensive cyber power, making sophisticated capabilities accessible beyond state intelligence agencies.

Although cyber mercenaries appear to be products of the digital age, the institution they represent is much older. Throughout history, rulers have outsourced military capabilities to secure political, military and economic advantages, from hired troops in ancient empires to Private Military Companies in the post-Cold War era. Their rise therefore reflects not a new phenomenon but the adaptation of an enduring institution to a new battlespace.

This continuity is best captured by Carl von Clausewitz's observation that while the nature of war remains constant, its character evolves with political, social and technological change.[i] The political purpose of conflict remains unchanged; what has transformed are the means through which states pursue it. In the digital era, offensive cyber capabilities have become strategic assets, with cyber mercenaries emerging as both products of this changing character of warfare and influential actors shaping its future trajectory.

2. Evolution of Mercenaries: From Soldiers of Fortune to Cyber Mercenaries

The history of warfare also reflects the history of mercenaries Long before modern nation-states and regular standing armies, rulers relied on warriors to supplement their forces and overcome manpower shortages. Although its form has evolved, the underlying logic has remained constant: states outsource capabilities whenever doing so offers a strategic advantage.

The earliest mentions of hired military forces appear in Kautilya's Arthashastra in the 4th century BCE. Kautilya identified Bhrita Bala (hired troops) as one of several categories of military forces available to the ruler. While he considered the hereditary army the most reliable, he recognised that mercenaries could be employed when political and military circumstances demanded.[ii] The Carthaginians employed Numidian cavalry and Iberian infantry throughout the Punic Wars, a practice documented extensively in Polybius's histories.[iii] The Byzantine Empire maintained entire regiments of Varangian mercenaries drawn from Scandinavia, whose loyalty was to money rather than to a political cause.[iv]During medieval and Renaissance period 14th –16th centuries in Italy existed condottieri system, a military contracting model where wealthy city-states hired professional mercenary captains to fight their wars.[v] However , Machiavelli criticised mercenary and advocated regular standing army.

Following the Peace of Westphalia (1648), the rise of standing national armies reduced the role of traditional mercenaries throughout the 19th and 20th centuries. This changed during the Cold War. Nations found it easier to use proxy militias and Private Military Companies to achieve objectives with deniability in era of nuclear deterrence without direct involvement. Unlike traditional mercenaries, PMCs operated as corporate entities providing training, logistics, intelligence, infrastructure protection and security services. Companies like Executive Outcomes in Angola (1993), Sandline International in Sierra Leone (1995) and more recently, the Wagner Group in Ukraine and Africa demonstrates the use of PMCs by states.

As the internet blossomed in the late 1990s, so did opportunities for illicit activities. Hackers began offering their skills for hire, marking the dawn of a new age in digital warfare-The Cyber Mercenary. The post-9/11 wars increased 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 operated with extraordinary latitude.[vi] Post Covid-19 surge in Internet usage and mass layoffs of IT professionals by companies have inadvertently strengthened the cyber mercenary ecosystem by providing lucrative opportunities to highly skilled unemployed youths.

This transformation reshaped mercenarism itself. The commodity being outsourced now is not only military labour but also cyber power. Their emergence reflects the changing character of warfare. As strategic competition increasingly occurs below the threshold of conventional armed conflict, states require capabilities for persistent intelligence collection, disruption and influence without direct military escalation. Cyber mercenaries provide rapid access to such capabilities while allowing governments varying degrees of operational distance and plausible deniability.

3. Cyber Mercenary and it’s Emerging Ecosystem

The traditional state monopoly over advanced cyber espionage and offensive cyber operations has steadily eroded with the rise of a global market of Private Sector Offensive Actors (PSOAs) and Commercial Surveillance Vendors (CSVs), commonly known as cyber mercenaries. Estimated to be worth over $12 billion, this industry develops and supplies sophisticated cyber intrusion capabilities to governments. This expanding access to state-grade cyber weapons is reshaping geopolitical competition, allowing middle-tier and authoritarian regimes to project asymmetric power and shaping the broader digital security landscape.[vii]

There is no universal definition of what constitutes a cyber mercenary. In 2018, Tim Maurer, a senior fellow in Carnegie's Technology and International Affairs programme, defined Cyber Mercenary as “an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect.”[viii] In 2021, the Working Group on Mercenaries under the United Nations Human Rights Council (UNHRC) defines mercenaries as “corporate entities providing, on a compensatory basis, military and/or security services by physical persons and/or legal entities” and added that activities in cyberspace can “rise to the level of mercenarism”.[ix]

At the centre of this ecosystem lies growing state demand. Governments increasingly require specialised cyber capabilities for intelligence collection, counterterrorism, law enforcement and national security. Developing such capabilities internally demands substantial investment, technical expertise and sustained research. For developing and underdeveloped states, cyber mercenaries provide a convenient option to hire for cyber warfare and surveillance operations.[x]

The term "cyber mercenaries" gained prominence around 2016 following revelations that governments across the world had used Pegasus. It is a sophisticated spyware developed by the Israeli firm NSO Group, highlighting the growing commercial market for offensive cyber capabilities. Despite being marketed for counterterrorism and law enforcement, Pegasus was allegedly used to monitor journalists, activists, political opponents and government officials in several

countries.[xi]

Beneath the commercially visible tier lies a vast grey market driven by exploit brokers and ransomware operators. Exploit brokers such as Zerodium publish public price lists for zero-day vulnerabilities in widely used software with remote code execution exploits for iOS reportedly fetching over US$2 million.[xii] Schneier argues that this market creates a structural conflict between governments' interest in stockpiling zero-days for offensive operations and their responsibility to protect national digital infrastructure. [xiii]

Likewise, the ransomware-as-a-service (RaaS) ecosystem has emerged as one of the most profitable segments of the cyber mercenary market. Groups such as Lock Bit and Black Cat/ALPHV operate with near-corporate efficiency, providing affiliates with attack tools, negotiation infrastructure and data-leak capabilities in return for a share of ransom payments.[xiv]

Alongside spyware vendors are hack-for-hire operators providing services such as network intrusion, credential theft, cyber espionage and data exfiltration. Investigations into Dark Basin, allegedly linked to BellTroX InfoTech Services, revealed campaigns targeting journalists, activists, legal professionals and businesses across multiple countries. This illustrates how offensive cyber expertise has become increasingly accessible through commercial markets.[xv][xvi]

4. Cyber Mercenaries Reshaping Contemporary Warfare

From a strategic perspective, cyber mercenaries are reshaping warfare in three important ways.

- Firstly, they have commercialised cyber power. This allows offensive capabilities to be acquired as market commodities rather than developed solely through state institutions.
- Second, they have blurred the boundaries between state and non-state actors. Thus, making attribution and accountability increasingly difficult.
- Thirdly, they have expanded the battlespace beyond physical domains. The Persistent cyber operations conducted during peacetime can produce strategic effects comparable to conventional military action.

Cyber Mercenaries are not replacing armed forces; rather, they are redefining how states compete, deter and project power. Today, Conflict is no longer waged solely with boots, bullets or drones. It is now engineered in code, outsourced via contracts and monetised by private actors rendering digital force as a service. Cyber Mercenaries have emerged as a parallel force layer.[xvii]

Tech firms are underwriting autonomy. PMSCs are bundling force with data and battlefield telemetry is transforming into a commodity. Cyber mercenaries have become force multipliers in grey-zone and hybrid warfare. They enable states to achieve political and military objectives without triggering conventional armed conflict.[xviii]

Cyber mercenaries provide governments specialised expertise while maintaining a degree of plausible deniability, complicating attribution and reducing diplomatic or legal costs. Their operations remain below the threshold of war[xix] but collectively shape the strategic environment in favour of the sponsoring state.

The rise of cyber mercenaries reflects a broader transformation in the character of warfare. Strategic advantage increasingly depends not only on military force but also on controlling information, exploiting digital systems and operating persistently within an adversary's networks.

5.Notable Examples of Cyber Mercenaries

As per Carnegie Endowment for International Peace 2023 data, at least 74 countries deployed spyware or digital forensics technology procured from commercial firms and applied them on more than 190 counts.[xx]

The 2016 Bangladesh Bank heist, attributed to North Korea's Lazarus Group, resulted in the theft of US$81 million through the compromise of the SWIFT banking network. The incident illustrated how cyber operations could target the financial domain and produce strategic effects beyond the battlefield[xxi]. Lazarus is also associated with 2014 Sony Pictures hack, WannaCry ransomware spread in 2017— affected more than 300,000 computers in 150 countries and made financial gain through theft, extortion and cryptocurrency-related operations.[xxii] BellTroX InfoTech Services gained international attention after 2020 investigations by Citizen Lab and Reuters. It ran hack-for-hire campaigns targeting journalists, activists, lawyers and businesses across several countries. The case demonstrated how private firms can commercially provide phishing, digital surveillance and other offensive cyber services, blurring the line between private intelligence, cybercrime and state-sponsored activities.[xxiii]

Recent conflicts demonstrate how cyber capabilities have become integral to modern warfare. The Russia–Ukraine war remains the defining example of cyber-enabled warfare. Before Russia's full-scale invasion in February 2022, destructive malware such as Whisper Gate and Hermetic Wiper targeted Ukrainian networks to disrupt critical systems. Microsoft documented these attacks as being designed for maximum disruption rather than financial gain.[xxiv] At the same time, the IT Army of Ukraine conducted large-scale attacks on Russian government and financial networks, while the cyberattack on Viasat's KA-SAT satellite network disrupted Ukrainian military communications[xxv] and caused collateral disruption across parts of Europe, highlighting the transnational impact of cyber operations.

In the Indo-Pacific, Chinese state-linked groups such as APT40—also known as Leviathan, Bronze Mohawk and Gingham Typhoon—illustrate the growing use of contractor-based cyber operations. Assessed by several Western intelligence agencies as operating under the direction of China's Ministry of State Security, these groups reportedly combine state guidance with private technical expertise to conduct cyber espionage against foreign networks.[xxvi][xxvii]

The Middle East presents another evolving model. Alongside Iranian-linked groups, cyber units affiliated with Hamas and Hezbollah, and other state-sponsored actors, cyber operations have become closely integrated with conventional military campaigns. During the US–Israel strikes on Iran under Operation Epic Fury/Roaring Lion on 28 February 2026, cyber activities accompanied kinetic operations, ranging from the abuse of legitimate IT tools and intelligence-gathering by China-linked Mustang Panda to disruptive campaigns by groups such as Handala and the Iran-linked Dust Specter, underscoring the increasingly interconnected nature of cyber and conventional warfare.[xxviii]

6. Governance, Accountability and Legal Challenges

The rapid expansion of the cyber mercenary industry has outpaced the evolution of international legal and regulatory frameworks. Existing international law, developed primarily for conventional armed conflict and traditional mercenaries. They offer limited guidance for private actors that develop, market or deploy offensive cyber capabilities. As a result, cyber mercenaries operate in a legal grey area marked by unresolved questions of jurisdiction, attribution and accountability. There isn’t any specific binding regulatory international law for Cyber Mercenaries.

The 1989 United Nations International Convention against the Recruitment, Use, Financing and Training of Mercenaries provides only limited applicability. Its definition focuses on direct participation in armed conflict and barely on cyber mercenary.[xxix]

The 2008 Montreux Document established non-binding norms for private military and security companies but remains largely irrelevant to cyber operations.[xxx] Similarly, the 2021 UN Group of Governmental Experts report outlined norms for responsible state behaviour in cyberspace but lacks enforcement mechanisms and excludes non-state actors. Some progress has emerged at the operational level. In January 2024, a coordinated law enforcement operation led by Europol and the US Department of Justice temporarily disrupted the Lock Bit ransomware infrastructure across ten countries. While the Tallinn Manual 2.0 offers an influential interpretation of international law in cyberspace, it remains a non-binding academic framework. It provides limited clarity on the responsibility of private cyber contractors.[xxxi]

Efforts to regulate offensive cyber tools have also yielded mixed results. The Wassenaar Arrangement introduced export controls on intrusion software and dual-use cyber technologies[xxxii]. However, inconsistent implementation and the transnational nature of cyberspace allow firms to exploit jurisdictional differences and continue operating across borders.

Attribution remains another major challenge. Layers of intermediaries, subcontractors and digital obfuscation often make it difficult to determine whether a cyber operation was conducted by a state, a private contractor or a criminal group. This weakens deterrence, complicates legal responses and raises concerns over the misuse of offensive cyber capabilities.

Addressing these challenges requires more than legal regulation. It demands international norms that balance national security needs with accountability, transparency and responsible state behaviour. Until such norms emerge, cyber mercenaries are likely to continue operating within the regulatory ambiguities that increasingly characterise contemporary conflict.

7. Implications for India

For India, the rise of cyber mercenaries represents a strategic challenge that extends beyond cybersecurity. As one of the world's largest digital economies, India's expanding digital public infrastructure, financial networks and critical information infrastructure have strengthened governance while also increasing vulnerability to sophisticated cyber operations by both state and non-state actors.

This challenge is particularly significant given India's security environment. Recorded Future reported in 2020 that the Chinese state-linked group Red Echo had compromised at least 12 Indian power sector entities. This highlights the risk of cyberattacks on critical infrastructure during military crises. Likewise, the 2022 ransomware attack on AIIMS Delhi by Chamel Gang disrupting hospital systems for nearly a month, demonstrated the real-world impact of cyber threats against civilian infrastructure.[xxxiii]

Post Operation Sindoor, several Pakistan based hackers like APT 36, Team Insane PK, Cyber Group HOAX 1337 etc. collectively launched 1.5 million attacks on Indian Infrastructure. The methods used by hackers included malware campaigns, Distributed Denial-of-Service (DDoS) attacks and GPS spoofing. The defacement of Indian websites like AVNL, Defence Nursing College in Jalandhar was also reported.[xxxiv]

Consequently, India must prepare for cyber operations conducted both by hostile states and private intermediaries operating across jurisdictions. Addressing this challenge requires a comprehensive strategy. India should explicitly recognise cyber mercenaries in its national security and cyber strategy to strengthen coordination among the Defence Cyber Agency, CERT-In, NCIIPC and intelligence agencies. Thus, deepening collaboration with the domestic cybersecurity industry and research institutions.[xxxv] India should develop legal framework against Private Offensive Cyber Operations.

At the same time, investing in indigenous capabilities such as vulnerability research, malware analysis, digital forensics and cyber threat intelligence will enhance strategic autonomy. Internationally, India should continue to shape cyber governance through forums such as the United Nations Open-Ended Working Group (OEWG), the Quad and other multilateral platforms to promote norms on responsible state behaviour, commercial spyware regulation and accountability for private offensive cyber actors.

The rapid expansion of Digital India especially the UPI, Fastag, Adhar linked services etc. brings with it potential cyber vulnerability. So, Govt. should mandate Critical Infrastructure Cyber Resilience Standards with mandatory incident reporting to CERT-In, regular third-party audits and financial penalties for non-compliance.

The challenge for India is therefore not merely technological but strategic. As cyber mercenaries become increasingly embedded in interstate competition, the ability to anticipate, attribute and respond to their activities will be essential to national security.

8.Conclusion

The evolution of cyber mercenaries demonstrates that while the nature of war remains constant, its character continues to evolve with technological change. From Kautilya's Bhrita Bala to post-Cold War PMCs, the outsourcing of military capabilities has continually adapted to changing strategic realities. Today, that logic has entered cyberspace where offensive cyber capabilities are increasingly commercialised through private actors.

Cyber Mercenaries have become important enablers of grey-zone competition. They provide states specialised capabilities, operational flexibility and plausible deniability. At the same time, they blur the boundaries between state and non-state actors, exposing critical gaps in international law, attribution and cyber governance. As AI, offensive cyber tools and commercial surveillance technologies continue to advance, their strategic relevance is likely to grow further.

For India, the challenge extends beyond strengthening cyber defences. It requires a long-term strategy that combines institutional coordination, indigenous cyber capabilities, robust legal frameworks and active participation in shaping international cyber norms.

Understanding cyber mercenaries as both a product and an enabler of the changing character of warfare is therefore essential for anticipating the future trajectory of conflict. In an era where strategic advantage increasingly depends on control over digital networks rather than physical territory alone, cyber mercenaries are likely to remain enduring actors in the evolving landscape of contemporary warfare.

Footnotes:

[i] Echevarria, Antulio J., “War's Changing Character and Varying Nature: A Closer Look at Clausewitz's Trinity,” *Infinity Journal*, Volume 5, Issue 4, Summer 2017, pages 15-20. https://doi.org/10.64148/msm.v5i4.3

[ii] 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."

[iii] 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.

[iv] 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)

[v] Condottieri di Ventura. (n.d.) “The Condottieri System: The Role of Geography and Social Class in the Lives of Italian Condottieri” https://condottieridiventura.it/the-condottieri-system-the-role-of-geography-and-social-class-in-the-lives-of-italian-condottieri/

[vi] Christian Miller, "Contractors Outnumber Troops in Iraq," New York Times, July 4, 2007. https://www.latimes.com/archives/la-xpm-2007-jul-04-na-private4-story.html

[vii]Falconfeeds.io. ‘The Rise of Cyber Mercenaries: How Private Threat Actors Are Reshaping Global Conflict’.2026. Blog https://falconfeeds.io/blogs/rise-of-cyber-mercenaries-private-offensive-cyber-actors/

[viii] Tim Maurer, Cyber mercenaries: the state, hackers, and power, (Cambridge, Cambridge University Press, 2018): p. 31.

[ix] The human rights impacts of mercenaries, mercenary-related actors and private military and security companies engaging in cyber activities - Report of the Working Group on the use of mercenaries

[x] Pablo Rice. ‘Cyber Mercenaries Decoded’. Issue Brief.2024. Paris Peace Forum https://parispeaceforum.org/app/uploads/2024/07/issue-brief-cyber-mercenaries-decoded-1.pdf

[xi] Ibid.

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

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

[xiv] 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-asa-service

[xv]Cyber Warfare Asia. “Cyber Guns for Hire: Unmasking the Indian Subcontinent’s Shadowy Hacking Empire’’.2025. Medium https://mahdiabbastech.medium.com/cyber-guns-for-hire-unmasking-the-indian-subcontinents-shadowy-hacking-empire-566bc768929b

[xvi] John Scott-Railton, Adam Hulcoop, Bahr Abdul Razzak, Bill Marczak, Siena Anstis, and Ron Deibert. “Dark Basin: Uncovering a Massive Hack-For-Hire Operation,” The Citizen Lab Research Report No. 128, University of Toronto, June 2020.

[xvii] Joana de Deus Pereira. “From Drones to Data: Private Contractors and Cyber Mercenaries”.2025. Commentary. RUSI https://www.rusi.org/explore-our-research/publications/commentary/drones-data-private-contractors-and-cyber-mercenaries

[xviii] Ibid.

[xix] Fitri Bintang Timur. “Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration”. Monograph. 2023. ORF https://www.orfonline.org/research/cyber-mercenaries

[xx] Steven Feldstein and Brian Kot, Global Inventory of Commercial Spyware & Digital Forensics in the Mendeley Data, March 2023, https://data.mendeley.com/datasets/csvhpkt8tm/10

[xxi] Fitri Bintang Timur. “Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration”. Monograph. 2023. ORF https://www.orfonline.org/research/cyber-mercenaries

[xxii] Ibid.

[xxiii] Cyber Warfare Asia. “Cyber Guns for Hire: Unmasking the Indian Subcontinent’s Shadowy Hacking Empire’’.2025. Medium https://mahdiabbastech.medium.com/cyber-guns-for-hire-unmasking-the-indian-subcontinents-shadowy-hacking-empire-566bc768929b

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

[xxv] Joana de Deus Pereira. “From Drones to Data: Private Contractors and Cyber Mercenaries”.2025. Commentary. RUSI https://www.rusi.org/explore-our-research/publications/commentary/drones-data-private-contractors-and-cyber-mercenaries

[xxvi] B?çakc? S, Gücüyener Evren A and Maail AG (2026) Cyber coercion in the indo-pacific: a comparative analysis of India’s and Australia’s responses. Front. Polit. Sci. 8:1748496. doi: 10.3389/fpos.2026.1748496

[xxvii]Timur. ‘Cyber Mercenaries: The Failures of Current Responses and the Imperative of International Collaboration’.2023. ORF

[xxviii]Seqrite. ‘Advisory: Middle East Conflict & Cyber Escalation Overview’.2026 https://www.seqrite.com/blog/iran-us-israel-cyberwar-2026-analysis/

[xxix]UNHR. ‘International Convention against the Recruitment, Use, Financing and Training of Mercenaries’.1989

https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-against-recruitment-use-financing-and

[xxx] 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) https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies

[xxxi] Monojit Das. “From battlefields to Bytes: The Evolution of Digital Mercenaries From Guns to Code: The Evolution of Mercenary Power”2026. CENJOWS https://cenjows.in/wp-content/uploads/2026/05/Dr-Dass-IB.pdf

[xxxii] Kojla Brockmann, Lauriane Héau. ‘Spyware as a service: Challenges in applying export controls to cloud-based cyber-surveillance software’.2025. SIPRI https://www.sipri.org/commentary/topical-backgrounder/2025/spyware-service-challenges-applying-export-controls-cloud-based-cyber-surveillance-software

[xxxiii] Ravie Lakshmanan. ‘**Chinese and N. Korean Hackers Target Global Infrastructure with Ransomware**’.2024. The Hacker News

[xxxiv]TOI Tech Desk. ‘Pakistani Hacker attacked 1.5 million Indian websites after Operation Sindoor: Failure rate, names…’2025.Times of India

http://timesofindia.indiatimes.com/articleshow/121128592.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=c

[xxxv]Monojit Das. “From battlefields to Bytes: The Evolution of Digital Mercenaries From Guns to Code: The Evolution of Mercenary Power”2026. CENJOWS https://cenjows.in/wp-content/uploads/2026/05/Dr-Dass-IB.pdf

The views expressed are those of the authors and do not represent the views of CNAWS.

Image Source: ChatGPT