NEXT IAS

DAILY EDITORIAL ANALYSIS

TOPIC

GREY-ZONE WARFARE AND CYBER PRECURSOR TO CONVENTIONAL CONFLICT

www.nextias.com

GREY-ZONE WARFARE AND CYBER PRECURSOR TO CONVENTIONAL CONFLICT

Context

- Grey-zone warfare is reshaping modern conflict by exploiting ambiguity and leveraging cyber operations as a **strategic precursor to conventional military engagement.**

Understanding Grey-Zone Warfare

- It refers to a **spectrum of hostile actions** that are **deliberately ambiguous**, allowing states **to pursue strategic objectives without crossing the threshold.**
    - It includes **cyberattacks, disinformation campaigns, economic coercion, use of proxies and non-state actors, and legal and diplomatic manipulation.**
- It leverages **ambiguity, deniability, and non-kinetic tactics** to achieve strategic effects traditionally associated with conventional warfare.
- **Contemporary conflicts** between State actors are **increasingly fought in the** grey zone and the cyber domain stands at the **pivotal point** in this, which has evolved from a mere **support function into a decisive battlespace** capable of shaping outcomes.

Cyber Operations as the First Strike in Grey-Zone Warfare

- Modern conflicts demonstrate that cyber operations have become the **opening salvo of state-on-state confrontations.**
    - These operations t**arget critical infrastructure** like power grids, telecommunications, transport networks, and command systems to paralyse an adversary's ability to respond effectively.
- Cyber strikes create cascading effects across governance, military readiness, and public morale without triggering immediate political backlash by **disrupting the backbone of modern society.**
- **Malware, dormant implants** and **industrial control systems** can be pre-positioned years before activation, allowing for strategic surprise.
    - The Ukrainian power grid attacks of 2015–16 exemplify this approach, revealing how dormant cyber tools can cripple essential services at a decisive moment.

Logic Behind Cyber Operations in Grey-Zone Warfare

- Cyber operations in the grey zone are designed for **strategic confusion and paralysis**.
    - They erode confidence, delay decisions, and reduce an adversary's capacity to govern or respond.
- The advantage lies in **plausible deniability** as cyber disruptions **can mimic technical faults or accidents,** complicating attribution and accountability.
    - As a result, states can impose substantial strategic costs without overt aggression.

Case Studies: Cyber as a Precursor

- **Recent Operation in Venezuela (2026)**: The coordinated US action that led to the **capture of the Venezuelan President** showcased the **integration of cyber and kinetic operations** like cyber preconditioning, air defence manipulation, communication disruption, and exploitation of surveillance infrastructure.
- **Russia-Ukraine Conflict:** Prior to the 2022 invasion, Ukraine faced a barrage of cyberattacks targeting government websites and infrastructure, softening the ground for kinetic operations.
- **China's South China Sea Strategy:** China has used **cyber espionage and disinformation** to assert dominance and undermine rival claimants without direct confrontation.
- **Iran-Israel Shadow War:** Both nations have engaged in tit-for-tat cyberattacks on infrastructure and private sectors, avoiding open warfare while inflicting strategic damage.

India's Experience: Lessons from the Grey Zone

- **India – China:**
    - **Infrastructure and Psychological Warfare:** China has continued its grey-zone campaign along the LAC by **constructing dual-use infrastructure** (roads, helipads, villages) near disputed areas to assert

territorial claims without direct conflict, and deploying troops and surveillance assets in contested zones under the guise of routine patrols.

- **Galwan Valley Conflict and Beyond:** China's post-incident strategy has focused on cyber intrusions into Indian power grids and telecom networks.
- Narrative manipulation through state media and diplomatic channels to portray India as the aggressor.
- **Mumbai Blackout (2020):** Attributed to Chinese state-sponsored actors, the outage highlighted how civilian infrastructure can serve as leverage during geopolitical crises.

- **India–Pakistan:**
    - **Cyber Warfare Surge (2025):** Pakistan launched a series of cyberattacks targeting government portals, financial institutions, and media outlets. These included:
        - **Distributed Denial of Service (DDoS) attacks** on Indian banking systems.
        - **Defacement of official websites** with anti-India propaganda.
        - **Phishing campaigns** aimed at military personnel and critical infrastructure operators.
- However, these **incidents exposed gaps** in India's cyber deterrence posture, particularly in **attribution, coordination, and doctrinal clarity.**

Structural Gaps in India's Cyber Preparedness

- **Fragmented Institutional Framework:** Cybersecurity responsibilities remain divided among c**ivilian, military, and sectoral agencies.**
    - **Coordination** between the National Critical Information Infrastructure Protection Centre (NCIIPC), state authorities, and private operators is **inconsistent**.
- **Civil-Military Disconnect: Most critical infrastructure** like power grids, ports, telecommunications are **civilian-run**, **but directly linked to national security.**
    - The **absence of integrated cyber-military exercises** leaves India ill-prepared for combined cyber-kinetic scenarios.
- **Supply-Chain Vulnerabilities:** India's reliance on foreign hardware and software, often from adversarial regions, introduces hidden risks.
    - Compromised components may remain dormant until strategically activated.
- **Human Capital Deficit:** There is a **shortage of specialists** capable of bridging information technology (IT) and operational technology systems.
    - It limits India's capacity to defend industrial control systems effectively.
- **Ambiguous Deterrence Posture:** India **lacks clear declaratory policies on cyber retaliation.**
    - Without explicit signalling of red lines or proportional response mechanisms, **adversaries may perceive cyber coercion** as a low-risk option.

Efforts and Initiatives in India's Cyber Preparedness

- **Institutional Framework For Cybersecurity:**
    - **National Critical Information Infrastructure Protection Centre (NCIIPC):** It was established as **an apex body** in 2014 under the **National Technical Research Organisation (NTRO)**, responsible for protecting India's **Critical Information Infrastructure (CII)**.
    - **Indian Computer Emergency Response Team (CERT-In):** It acts as the national nodal agency for responding to cybersecurity incidents.
        - **New directives issued by CERT-In** mandate organizations to report cybersecurity incidents within **six hours**, maintain logs for **180 days**, and synchronize with **Indian time servers** to improve incident response efficiency.
- **Policy and Strategic Frameworks:**
    - **National Cyber Security Policy (NCSP) 2013:** It remains the foundational policy document outlining India's vision for securing cyberspace.
        - A new **National Cybersecurity Strategy (NCS)** is currently in draft stage to update and address modern grey-zone and hybrid threats.
    - **National Cyber Security Coordination Centre (NCCC):** It functions as a real-time monitoring and coordination hub.

- **National Cyber Crime Reporting Portal**: It provides a centralized mechanism for citizens to report cybercrimes, particularly those involving **financial fraud, identity theft, and child exploitation**.

- **Capacity Building and Human Resource Development:**
  - **Cyber Surakshit Bharat Initiative:** It aims to promote cyber hygiene and awareness among government officials, especially at the state and district levels.
  - **Information Security Education and Awareness (ISEA) Programme**: It aims to create skilled manpower in cybersecurity through training programs in academic institutions.
  - **Defence Cyber Research:** Centre for Artificial Intelligence and Robotics (CAIR). under **DRDO**, leads R&D in cybersecurity, cryptography, and secure network communication technologies.
- **Legal and Regulatory Framework:**
  - **Information Technology Act, 2000 (Amendment 2008)**: It provides the legal foundation for addressing cybercrime, defining offences such as hacking, data theft, and identity fraud.
    - The **2008 Amendment** expanded its scope to include cybersecurity responsibilities for organizations and intermediaries.
  - **Data Protection and Digital India Act (Draft Stage):** It aims to replace the IT Act, introducing more robust provisions on **data governance**, **cyber liability**, and **critical infrastructure protection** in alignment with global standards.
- **Public–Private Collaboration:**
  - Partnerships between **NCIIPC**, **private utilities**, and **cybersecurity firms** for vulnerability assessments.
  - **Joint exercises** with telecom operators and financial institutions for threat response.
- **International Cooperation**:
  - **Bilateral agreements** with countries such as the **US, Japan, Australia, France, and Israel** on cyber threat sharing and capacity building.
  - Participation in **Quadrilateral Security Dialogue (QUAD)** cyber initiatives focused on supply chain security and critical infrastructure protection.
  - Membership in global frameworks like the **Budapest Convention on Cybercrime (observer status)** and **UN Open-Ended Working Group (OEWG)** on cybersecurity.

Way Forward: Towards a Coherent Cyber Strategy

- **Integration of Cyber Defence into Military Doctrine:** Cyber operations should form a core element of India's national defence planning, not a peripheral technical issue.
- **Joint Cyber Exercises:** Regular red-teaming and integrated civilian-military drills are essential for realistic preparedness.
- **Supply-Chain Security:** India must prioritise domestic manufacturing, rigorous audits, and secure sourcing of critical infrastructure components.
- **Capability Signalling:** Strategic communication is vital—deterrence depends as much on perceived credibility as on actual capacity.
- **Building Human Expertise:** Investing in cyber-technical education and operational training will bridge critical skill gaps in industrial systems defence.
- **Emerging Focus Areas:** India's evolving strategy reflects an understanding that cyber threats are merging with **hybrid warfare** and **grey-zone coercion**. Current focus areas include:
  - Developing **offensive cyber capabilities** for deterrence.
  - Enhancing **cyber-physical security** of power grids and telecom networks.
  - Establishing a **National Cyber Command** for unified strategic control.
  - Promoting **indigenous technology** for secure hardware and cryptography.
  - Integrating **AI and big data analytics** for predictive threat detection.

Source: ORF

Daily Mains Practice Question

[Q] In what ways does grey-zone warfare, particularly through cyber operations, challenge traditional notions of deterrence and sovereignty in international relations? Evaluate with reference to India's engagements with Pakistan and China.