P.L.RAJ IAS & IPS ACADEMY
Building Bureaucrats Since 2006

4. Cyber Warfare and International Law - Hybrid Warfare in The Digital Age - National

1. Why in News

1. Recent tensions involving US, Israel, Iran demonstrating rise of hybrid warfare where cyber operations increasingly complement conventional military action
2. Cyber incidents linked to groups like Handala Hack Team claiming responsibility for attacks including on US-based medical technology company
3. Challenge to existing international legal frameworks
4. Highlights difficulty in attribution, threshold determination, enforcement under international law

2. About Cyber Warfare

Definition

1. Use of digital attacks, hacking, cyber operations by states or non-state actors to disrupt, damage, or gain unauthorized access to another country's computer systems, networks, critical infrastructure
2. For strategic, political, or military purposes

Key Features

1. **Cross-border nature -** Transnational attacks without physical intrusion (WannaCry ransomware affected 150+ countries)
2. **Difficulty in detection, attribution -** Attackers hide using encrypted networks, fake digital trails
3. **Use of proxy networks -** States employ proxy groups maintaining plausible deniability
4. **Targeting civilian and military systems -** Simultaneously disrupting both increasing societal vulnerability
5. **Below threshold of conventional war -** Enables states avoiding direct military escalation (China-US cyber intrusions rarely escalating)
6. **Low-cost but high-impact -** Not Petya cyberattack caused billions in global losses
7. **Targeting critical infrastructure -** Power grids, banking, healthcare, transportation (Ukraine power grid attack)
8. **Information and psychological warfare -** Misinformation, narrative manipulation, public opinion influence (2016 US election interference)
9. **Speed and real-time execution -** DDoS attacks instantly disabling websites
10. **Asymmetric nature -** smaller states, non-state actors challenging advanced powers (North Korea targeting global financial institutions)
11. **Continuous and non-linear conflict -** Occurs during both peace, conflict periods; persistent espionage campaigns
12. **Difficulty applying international law -** Absence of universally accepted norms; debate over whether cyber-attacks qualify as "armed attack" under UN Charter

3. International Legal Framework Governing Cyber Warfare

UN Charter (Article 2(4))

1. Prohibits use of force against territorial integrity, political independence of states

2. Severe cyber-attacks on critical infrastructure may qualify as unlawful use of force
3. However, threshold for "use of force" in cyber context debated

Principle of State Responsibility

1. States can be held internationally responsible when cyber operations -
    1. Attributable to them
    2. Violate international obligations
    3. Cause significant harm
2. Challenge - Attribution extremely difficult

Budapest Convention on Cybercrime

1. Council of Europe framework combating cybercrime through international cooperation
2. Harmonization of domestic cyber laws
3. **Limitation -** Mainly addresses criminal rather than inter-state cyber activities

UN Convention against Cybercrime

1. Strengthens global cooperation against cyber-enabled crimes
2. **Limitation -** Limited provisions regarding state-sponsored cyber warfare, geopolitical cyber conflicts

Tallinn Manual

1. Non-binding document by NATO Cooperative Cyber Defence Centre of Excellence
2. Applies existing international law to cyber operations
3. Influential but lacks formal treaty status

4. Major Challenges in Applying International Law

Difficulty in Attribution

1. Cyber operations secretive, routed through multiple networks, jurisdictions
2. Gap between political certainty and legal proof
3. Technical evidence difficult translating into legally admissible form

Threshold Problem

1. International law lacks universally accepted standard determining when cyber-attack becomes prohibited "use of force" or "armed attack"
2. Below-threshold operations creating grey zone

Lack of Effective Judicial Forums

1. Sensitive cyber disputes unlikely heard by ICJ without state consent
2. Domestic courts face challenges due to sovereign immunity of foreign states
3. No dedicated international cyber tribunal

Evidentiary Challenges

1. Cyber incidents involve technical data, classified intelligence, complex causation chains
2. Difficult proving - Who carried out operation, damage caused, specific harm resulting
3. Makes legal action complicated, uncertain

Strategic and Political Concerns

1. States avoid legal proceedings fearing - Escalation, retaliation, exposure of sensitive capabilities
2. National security considerations overriding legal accountability

Limitations of International Conventions

1. Budapest Convention, UN Convention - Focus on cybercrime, law enforcement
2. Fall short addressing state responsibility in geopolitical cyber conflicts

Mismatch Between Technology and Law

1. Rapid cyber warfare capabilities advancement outpaced legal frameworks

2. Laws designed for physical world inadequately addressing digital domain

Weak Enforcement Mechanisms

1. Limited legal consequences despite increasing attack frequency, severity
2. Weak enforcement, jurisdictional challenges
3. Absence of credible accountability creating minimal deterrence

5. Why Cybersecurity Is Important for India

1. **Growing digital dependence -** Finance, energy, governance, healthcare, communication relying on digital systems
2. **Critical infrastructure protection -** Cyber-attacks on power grids, banking, transport, government platforms threatening security
3. **Rising vulnerability -** Digital governance expansion increasing exposure to ransomware, data breaches, espionage
4. **National cyber resilience -** Strengthening capabilities ensuring resilience against strategic infrastructure attacks
5. **Shaping global norms -** Major digital economy; strong stake in attribution, accountability, responsible state behaviour discussions
6. **Bridging law-cyber gap -** Ensuring harmful cyber operations don't remain beyond international accountability
7. **Sovereignty protection -** Protecting strategic assets, digital economy from hostile actors

Institutional Mechanisms in India

Institution	Role
CERT-In	Nodal agency (MeitY); responding to cyber incidents, issuing alerts, coordinating cybersecurity
NCIIPC	Protecting critical information infrastructure (power, banking, telecom, transport, defence)
NCCC	Cyber surveillance, threat intelligence platform detecting, monitoring, coordinating responses
Defence Cyber Agency (DCA)	Tri-service agency; cyber warfare operations, military cyber capabilities
NTRO	Cyber intelligence, surveillance, strategic digital infrastructure protection
Cyber Swachhta Kendra	Botnet cleaning, malware analysis; improving cyber hygiene
I4C (Indian Cyber Crime Coordination Centre)	MHA coordination against cybercrime, cyber fraud
NCSC	National cyber security strategy, inter-agency cooperation under NSC Secretariat
DSCI	Industry body; cybersecurity standards, skill development, public-private collaboration
National Cyber Security Policy 2013	Policy framework securing cyberspace, protecting critical infrastructure
Digital Personal Data Protection Act 2023	Personal data protection, digital data security, privacy
Cyber Surakshit Bharat	Cyber awareness, capacity building in government departments

Indian Cyber Command (Proposed)	Integrating offensive-defensive cyber warfare capabilities

6. Way Forward

Strengthen Domestic Cyber Resilience

1. Enhance cybersecurity architecture, protect critical infrastructure
2. Improve preparedness against cyber-attacks targeting essential sectors
3. Regular cyber drills, vulnerability assessments, incident response planning

Develop Attribution Capabilities

1. Investment in cyber forensics, intelligence-sharing mechanisms
2. Indigenous cyber expertise development
3. Accurately identify, respond to cyber threats

Shape Global Cyber Norms

1. Active participation in UN cyber governance discussions
2. International cyber law negotiations, global norm-setting
3. Advocate for binding multilateral cyber treaty

Promote Responsible State Behaviour

1. Principles - non-targeting civilian infrastructure, protection of critical services, transparency
2. Confidence-building measures in cyberspace between nations
3. Bilateral cyber agreements

Enhance International Cooperation

1. Expanding cyber intelligence sharing
2. Joint cyber exercises with partner countries (India-US, India-EU, Quad cyber cooperation)
3. Strengthening multilateral cyber frameworks

7. Conclusion

Cyber warfare transforming modern conflict by blurring boundaries between war-peace, civilian-military spaces, domestic-international domains as demonstrated by US-Israel-Iran tensions with Handala Hack Team attacks on civilian infrastructure. Key features include cross-border nature, attribution difficulty, proxy network use, asymmetric capability, continuous non-linear conflict operating below conventional war threshold. International legal framework—UN Charter Article 2(4), state responsibility, Budapest Convention, UN Cybercrime Convention—formally applies but challenges persist - attribution difficulty (political certainty vs legal proof gap), threshold problem (no standard for "armed attack"), lack of judicial forums, evidentiary challenges, weak enforcement creating minimal deterrence. India's cybersecurity importance spans critical infrastructure protection, rising digital vulnerability, sovereignty safeguarding, global norm shaping. Institutional mechanisms—CERT-In, NCIIPC, Defence Cyber Agency, NCCC, I4C—require strengthening through domestic cyber resilience enhancement, attribution capability development, active participation in UN cyber governance, promoting responsible state behaviour, enhanced international cooperation ensuring cyberspace doesn't become unregulated conflict arena threatening global stability.

Source - https -//www.thehindu.com/opinion/op-ed/cyber-warfare-is-outpacing-global-legal-accountability/article71011864.ece