# Chapter 4
# Cyber Warfare and Blurring Lines Between State and Non-State Actors

**Vidisha Shekhawat**
https://orcid.org/0009-0009-7816-3591
*Manipal University Jaipur, India*

**Pranjal Khare**
https://orcid.org/0000-0002-9937-9588
*Jindal Global Law School, O.P. Jindal Global University, India*

**Kiet Le Hoang**
https://orcid.org/0009-0002-9968-1952
*Vietnam National University, Hanoi, Vietnam*

## ABSTRACT

*Cyber warfare has transformed the digital realm into a critical conflict domain, marked by an increasing convergence of state and non-state actors. Initially dominated by nation-states, cyberattacks now involve a diverse range of entities, from hacktivists and cybercriminals to terrorist groups wielding sophisticated capabilities. The rise of state-sponsored cyber operations has initiated a new cold war characterized by persistent digital espionage and sabotage. Concurrently, non-state actors are employing cyber tools for various motives, often achieving levels of sophistication comparable to state-level attacks. This blurring of lines complicates attribution, heightens the risk of unintended escalation, and challenges established international norms. The future of cyber warfare anticipates greater complexity*

DOI: 10.4018/979-8-3373-1727-4.ch004

*with the proliferation of advanced technologies. The growing interconnectedness of critical infrastructure will expand vulnerabilities, necessitating novel defence and deterrence strategies to address the evolving threats posed by both state and non-state actors in this domain.*

## INTRODUCTION

The times when wars were fought only on battlegrounds are gone; now they happen in silence within the realms of cyberspace making the nations fall & rise with digital clicks. The traditional warfare included lands, seas, and air as battlegrounds, however, with growing technology a fifth dimension has found its way to hostilities that require data breaches and hackers rather than soldiers. Cyberwarfare involves digital attacks to incapacitate a nation's military e-mail systems, derail trains, damage power grids, and even uncontrollable satellites. Technology led to the creation of the internet making the world accessible to almost everything breaking all barriers. There are numerous iterations through which cyber warfare takes place; they include hacking and cyber espionage, disinformation campaigns, cyber-attacks on critical infrastructure, and so on. Cyberwarfare is roaring, too rapidly due to several reasons including lower costs, ambiguity in legal frameworks, and requiring lesser human resources while prompting numerous threats. Stealing data and information has serious repercussions; it is limited to hacking for profit making or bank frauds, and it involves bringing down a nation's governance. Cyber warfare attacks are made to cripple a nation's military by other nation's governments. However, the geopolitics in cyber warfare does not only involve the state actors but nonstate actors as well. The growing participation of non-state actors and private entities has made it the most difficult problem to resolve. When there are no barriers, security becomes the utmost concern requiring sturdy weapons to fight back to attacks. In other words, digitally stored data includes confidential and private content that requires to be protected from breach which can only be done through strong and reliable cyber security. There is ample awareness amongst the nations regarding the threats that cyberspaces impose; the UK, USA, and even NATO have been spreading awareness and attempting to recommend nations to operate with the domain of legal approach in this new fighting arena (Robinson et al., 2015).

State actors have been using cyber warfare as their military strategy for a couple of decades to ensure national security; from espionage to information warfare many operations have been conducted. The operations ensure plausible deniability while garnering power in cyberspace. One of the examples is China allegedly infiltrating the U.S. networking to cripple its corporate network and defence mechanism. There have been multiple high-profile attacks used as tactics to overpower other states to