Chapter 7
Dispute Between Countries, a Corresponding Attack on Cyberspace:
The New National Security Challenge

Siddhardha Kollabathini
Jawaharlal Nehru University, India

ABSTRACT

Today, cyberspace is a fact of daily life, and cyberspace's impact has not bypassed states' national security. Cyberspace, a manmade technological advancement over the past decades, transformed the way economies work around the world, reshaping social interactions and a paradigm shift in politics. Cyberspace being boundaryless, omnipresent across multiple domains, and anarchic has been considered to attack whenever there are any disputes between two countries. In the context described above, a pressing question arises. Cyberspace is not a domain like land, water and air, and it is an environment inhabited by information and knowledge, existing in electronic form. If cyberspace is a mere inhabitation of information and knowledge, why do states want to consider cyberspace as an arena for confrontation in any dispute between countries? This chapter proposes discussing this new phenomenon, looking into the evaluation and analysing aspects of the recent phenomenon.

INTRODUCTION

Over the past decades, cyberspace, a manmade technological advancement, transformed the way economies work worldwide, reshaping social interactions

DOI: 10.4018/978-1-6684-6646-9.ch007

and a paradigm shift in politics. Today cyberspace is a fact of daily life, and it cuts across multiple domains. Cyberspace plays a vital role in atomic energy, space, communications, defence, education, agriculture, manufacture, services, entertainment, and employment generation and in addressing national priorities. Similarly, cyberspace became indispensable in the area of national security and defence. The protection of cyberspace has become a significant challenge to states as cyberspace is intertwined with other warfare domains, namely land, water, air and space.

Interestingly in the realm of the computer networks, state actors are not less in exploiting the incognito, precession impact, cost-effective, minimal human resources requirement characters of cyberspace, which is an informative environment, to achieve national interests. The attacks and threats to national security that are pervasive offline have begun to penetrate the world online. Thus cyberspace has become a new arena of confrontation leading to cyber-insecurity. Such an attack took place in 2007 on Estonia, where Estonia was subjected to systematic distributed attacks for three weeks. The cyber attack crippled the critical information infrastructure of financial centres, banks, parliament, ministries, security and public transport. The cyber attack on Estonia is the first "documented proper cyber attack" and is the beginning of cyber warfare.

Similarly, the attack on Georgia's cyberspace in 2008 changed the threat landscape for all the states that rely on cyberspace. One distinctive characteristic of the cyber attack on Georgia in the above context is – the outbreak of physical hostilities between Georgia and Russia over Abkhazia and South Ossetia landed up in the cyber domain. 'Europe', which became a battlefield for World War One and World War Two, coincidentally became a theatre for confrontation in the cyber domain.

Till the cyber attacks against Estonia 2007 and Georgia 2008, the cyberspace does not have strategic security attire. Pre Estonia 2007 and Georgia 2008 cyber attacks, cyberspace was viewed as a twenty-first-century technological infrastructure, a platform for socio-cultural concepts and a predominant support structure for economic activities. The Estonia and Georgia cyber attacks led to the conclusion that the cyberspace meant to conduct commerce, communicate with the citizens and interface with the critical infrastructure via electronic means can be a battle space and has become a central security concern for governments across the world.

The phenomenon – "whenever there are any disputes between two countries, a corresponding attack on the digital space has been seen" become more common in recent times. The 2010 Stuxnet cyber attack to cripple Iran's nuclear enrichment program; Operation Nitro Zeus 2015 an elaborate plan developed by the US for a cyber attack on Iran, in the event that diplomatic efforts to limit Iran's nuclear program failed and resulted in a military conflict; and, more recently in 2020 the India-China border clash at Galwan valley led to heightened cyber attacks on India