Available online @ www.iaraindia.com
RESEARCH EXPLORER-A Blind Review & Refereed Quarterly International Journal
ISSN: 2250-1940 (P) 2349-1647 (O)
Impact Factor: 3.655(CIF), 2.78(IRJIF), 2.77(NAAS)
Volume XIII, Issue 43
July- 2024
Formally UGC Approved Journal (63185), © Author

THE SILENT WAR: CYBER ESPIONAGE IN THE 21ST CENTURY

VIKASHINI. G. S
II B.A LL.B (Hons.)
School of Excellence in Law,
Tamil Nadu Dr. Ambedkar Law University, Chennai
&
SAINIKITHA.OL
II B.com LL.B (Hons.)
School of Excellence of Law
Tamilnadu Dr. Ambedkar Law University, Chennai.

Abstract

Espionage, an age-old practice, evolves in the digital age, leading to cyber espionage. This paper explores its historical roots, emphasizing technological transformations. Since the late '90s, cyber espionage poses a formidable security challenge, utilized by major actors like the U.S., China, Russia, Iran, and North Korea. The study delves into historical roots, contemporary landscape, motives, impacts, and key players, underscoring the imperative for international cooperation and robust cyber security measures to counter evolving challenges. Today, cyber espionage stands as a potent tool wielded by nation-state threat actors, posing a critical security issue for organizations. Incidents of state-sponsored hacking, corporate espionage, and intellectual property theft have become rampant and widespread with implications extending across political, economic, and societal domains.

***Keywords**: Digital Espionage, Covert Tactics, Global Cyber security, Cyber Threats, Digital warfare.*

Introduction

"Dark Side of Cyberspace is a metaphor and conceptual framework defining a virtual environmental realm that includes all criminal, deviant, deceptive, harmful and malevolent activities in the abstract universe of cyberspace."Cyber espionage or cyber spying is a form of

unauthorized cyberattack aimed at accessing confidential data or intellectual property for economic, competitive, or political motives. In this type of attack, an individual or nation employs cyber techniques to clandestinely gather information from another party. Unlike traditional espionage, cyber espionage operates discreetly, leaving invisible footprints deeply embedded within servers and computer networks. The Tallinn Manual, a set of guidelines for nation-state cyber warfare published in 2013, seeks to establish definitions, procedures, and rules governing international cyber operations. According to the manual, cyber espionage is described as an act carried out clandestinely or under false pretences, utilizing cyber capabilities to gather information with the intention of communicating it to the opposing party. While many perceive cyber espionage as targeting secret information for malicious purposes, the manual's definition does not explicitly delve into the intent of the attack or specify the nature of the information stolen, it proves instrumental within the realm of international law. This definition empowers victim nations to undertake suitable countermeasures against cyber intrusions, especially considering the intricate legal and political challenges that often hinder effective defence against cyber threats. Cyber espionage attacks may be driven by monetary motives or deployed alongside military operations, cyber terrorism, or cyber warfare. **Origin and growth of Cyber Espionage**

The landscape of cyber espionage, a clandestine practice ingrained in the earliest days of internet connectivity, has undergone significant transformations which is propelled by rapid technological advancements and evolving global dynamics. Originating in parallel with the advent of the internet, the history of cyber espionage spans back to the late 1990s and early 2000s. During this period, nations recognized the potential of the digital realm for intelligence gathering, with events like Moonlight Maze and Titan Rain offering early insights into the future of state-sponsored hacking. The modus operandi of Cyber-Espionage threat actors involves gaining unauthorized access, maintaining a low profile, and compromising sensitive assets and data. Enabled by technology, these espionage actors operate swiftly, efficiently, and with evasive techniques that make attribution challenging. The genesis of cyber espionage can be traced back to the 1980s when the French intelligence agency, leveraging the "Farewell Dossier," exploited a KGB officer's computer for critical intelligence. Simultaneously, the Chaos Computer Club, a German hacker group, exposed vulnerabilities in government and military systems, marking the inception of digital espionage. **Target Assets of Cyber Espionage**

Cyber espionage strategically centres on influencing geopolitics and illicitly acquiring state and trade secrets, intellectual property rights, and proprietary information in crucial sectors. It involves the collaboration of actors from various domains, including the economy, industry, foreign intelligence services, and affiliated entities. Notably, a recent report highlighted that 71% of organizations treat cyber espionage and related threats as a

'black box,' indicating ongoing efforts to comprehend and counteract them. Primary targets of cyber espionage encompass large corporations, government agencies, academic institutions, think tanks, and other entities possessing valuable IP and technical data, which could confer a competitive advantage to other organizations or governments. Individuals, including prominent political leaders, government officials, business executives, and celebrities, are also susceptible to targeted campaigns.

Cyber spies commonly seek to access the following assets:

- Research & Development data and activity
- Academic research data
- Intellectual Property (IP), such as product formulas or blueprints
- Salaries, bonus structures, and other sensitive financial information
- Client or customer lists and payment structures
- Business goals, strategic plans, and marketing tactics
- Military intelligence
- Other proprietary information in strategic fields
- Think tanks or other organizations that possess valuable IP and technical data.

In developing economies, as in the case of India, the surge in technological advancements and economic growth presents an attractive target for cyber espionage. These nations, with burgeoning digital landscapes, house valuable information that ranges from intellectual property to strategic plans. However, limited resources and the novelty of digital technologies often fabricate vulnerabilities, making it crucial for these economies to invest in robust cybersecurity measures and international collaboration to mitigate evolving cyber threats and sustain their growth.

State Sponsored Digital Espionage

State-sponsored cyber espionage poses a growing global challenge, especially in developing economies, where hackers target commercial firms and universities for trade secrets. Cyber espionage, characterized by illicit access to confidential information, impacts industrial sectors and critical infrastructures globally. Russia's cyber operations in Estonia, Georgia, and Ukraine underscore its strategic use of cyber tools. The escalating threat, coupled with sophisticated hackers and a lack of international cooperation, poses risks to essential services and national security. The 2022 revelation of Chinese hackers targeting India's power grids exemplifies a persistent trend. Developing economies like India face shy high threats due to the expanding technological landscapes. As cyber espionage becomes more sophisticated, international cooperation, robust cybersecurity measures, and innovative defence strategies are crucial for countering this evolving threat. The UN and regional organizations like the EU and NATO aim to establish norms for responsible state behaviour in cyberspace. Governments enact laws and sanctions, while the private sector invests in cyber security measures to mitigate cyber espionage risks. The Moonlight Maze virus, detected in 1999, quietly extracted confidential information for two years

from entities like the Department of Defence and NASA. In 2012, the "Red October" malware exploited Microsoft vulnerabilities globally, remaining undetected for up to five years. Additionally, Russia's involvement in space-sponsored espionage raises concerns about the scope and persistence of their cyber activities.

Common tools of Digital Espionage

In addition to state-sponsored economic cyber espionage, various techniques are employed by cyber actors to infiltrate and compromise targeted systems:

1. Watering Hole Attacks:
   Malicious actors infect legitimate websites frequented by the victim or associated individuals with malware. This compromises user visiting these sites, leading to potential data breaches.
2. Spear-Phishing:
   Hackers specifically target individuals through fraudulent emails, texts, or phone calls to extract login credentials and sensitive information. This personalized approach increases the chances of success.
3. Zero-Day Exploits:
   Cybercriminals exploit undisclosed security vulnerabilities or software flaws before they are discovered and patched by developers or IT teams. This tactic allows unauthorized access to systems.
4. Hacking Techniques:
   Hackers exploit vulnerabilities in software, hardware, or network configurations, employing methods like zero-day exploits and spear-phishing campaigns. These attacks aim to infiltrate and compromise the target's systems.
5. Malware Usage:
   Malicious software, including spyware, Trojans, and keyloggers, is a prevalent method in cyber espionage. These tools infect devices or networks, discreetly recording data such as keystrokes, communications, and files.
6. Social Engineering:
   Cyber espionage actors employ social engineering techniques like phishing emails, pretexting, or baiting to manipulate individuals within the target organization. These tactics exploit human psychology to gain access to sensitive information.

Major cases of Cyber Espionage

"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm." - Anna Maria Chavez

While some cyber spies operate within the bounds of legitimate intelligence activities, numerous notorious instances reveal a more sinister agenda. Here are noteworthy examples of cyber espionage:

1. Aurora (2009):
   In 2009, Google exposed a significant cyber espionage breach targeting Gmail accounts of Chinese human rights activists. Subsequent investigations revealed similar attacks on prominent companies like Adobe and Yahoo. A total of 20 companies were acknowledged falling victim to this exploitation of an Internet Explorer vulnerability, which has since been addressed.
2. COVID-19 Research (2020):

Recent cyber espionage activities have focused on COVID-19 research, with intrusion attempts reported since April 2020 against laboratories in the U.S., U.K., Spanish, South Korean, Japanese, and Australian regions. Russian, Iranian, Chinese, and North Korean actors have been implicated in these activities. It is understandable that the healthcare and pharma industries are major victims of the global digital espionage game.

3. CyFirma (2021):

In March 2021, a Singapore-based company, CyFirma, revealed that a Chinese state-backed hackers' group had targeted the information technology systems of two Indian vaccine makers—Bharat Biotech and the Serum Institute of India (SII). These companies' vaccines have been the most critical element of India's national vaccination programme and vaccine diplomacy. Chinese hackers' targeting of SII is significant when examining the reach of its vaccine, Oxford-AstraZeneca/Covishield, which is being used in 183 countries, as against almost half-reach of China's flagship Sinopharm vaccine (used in 90 countries).

Cases in India

1. Operation Shakti (Targeting Nuclear Capabilities):

Operation Shakti exemplifies nation-state-backed cyber espionage directed at India's nuclear capabilities. This case underscores the vulnerability of critical infrastructure and the potential geopolitical ramifications of cyber-attacks on national security assets.

2. GhostNet (A Massive Cyber Espionage Network):

The discovery of GhostNet revealed a large-scale cyber espionage network operating within India, targeting government and private-sector entities.

3. APT-C-23 (Targeting Defence and Aerospace):

APT-C-23, a threat group with suspected nation-state affiliations, highlights focused cyber espionage efforts on India's defence and aerospace sectors. This case study emphasizes the urgency of enhancing cybersecurity measures, particularly in critical industries crucial for national security.

Key Players

In the realm of cyber espionage, major players include the United States, China, Russia, Iran, and North Korea. Each country possesses unique cyber capabilities, targets, and strategies. The U.S. and China focus on intellectual property and trade secret thefts, while Russia leans towards political manipulation, seen in alleged election interference incidents. Prominent nation-state actors and well-known cyber espionage groups include:

1. Pioneer Kitten (Iran):

Active since at least 2017, Pioneer Kitten is suspected to have a nexus with the Iranian government. The group has engaged in targeted intrusions supporting Iranian government interests. Notably, there have been potential attempts at revenue stream diversification through network access sales.

2. Fancy Bear (Russia):

Operating since 2008, Fancy Bear employs phishing messages and spoofed websites. The group targets U.S. political organizations, European military entities, and victims globally. Fancy Bear gained infamy for the 2016 DNC and Podesta leaks and its attacks on anti-doping agencies in 2019.

3. Goblin Panda (China):

First observed in September 2013, Goblin Panda targets defence, energy, and government sectors in Southeast Asia, particularly Vietnam.

Helix Kitten (Iran):

Active since at least late 2015, Helix Kitten targets aerospace, energy, financial, government, hospitality, and telecommunications. The group is known for well-researched spear-phishing with custom PowerShell implants. Notably, Helix Kitten was involved in the 2013 New York Dam hack and attacks on the Australian Parliament House in 2019.

4. Double Dragon (China):

Active since 2012, Double Dragon engages in both state-sponsored espionage and financially motivated cybercrime. The group conducted a massive global hacking campaign in 2020. Double Dragon, also known as Cicada, is a Chinese state-sponsored espionage group with a dual identity. By day, it operates as a state-backed entity, engaging in espionage operations against various countries since 2012, including the United States and the United Kingdom. The group's activities extend beyond espionage, as it is known to delve into financially motivated cybercrime for personal gain during the night. In 2020, Double Dragon demonstrated its prolific nature by attempting to exploit vulnerabilities in hardware. Moreover, the group continued its operations, targeting government institutions across multiple countries and infiltrating companies spanning diverse industries.

5. Lazarus Group (North Korea):

Active since 2010, Lazarus Group is known for Operation Troy, WannaCry attack, and COVID-19 vaccine data theft. Backed by the Pyongyang regime, Lazarus Group operates as a profitable enterprise for North Korea. The group is infamous for infiltrating targets over time and orchestrating high-profile cyberattacks, including the WannaCry ransomware attack in 2017.

Recommendation

- Actively engage in global initiatives and forums such as the Paris Call for Trust and Security in Cyberspace, UN, EU, and NATO to establish norms for responsible state behaviour and foster international cooperation against cyber espionage.
- Allocate resources to enhance national cybersecurity capabilities, focusing on critical sectors like defence, government, and healthcare, to effectively counter evolving cyber threats.
- Foster collaboration between government and private-sector organizations, facilitating the sharing of threat intelligence and best practices to coordinate responses against cyber threats.
- Promote cybersecurity education and training programs to enhance overall

cyber hygiene and reduce susceptibility to common attack vectors.

- Develop and enforce robust legal frameworks addressing cyber espionage, ensuring appropriate consequences for state-sponsored cyber activities.

References:

1. Kurt Baker, WHAT IS CYBER Espionage? February 28, 2023, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/ (last visited Dec. 20, 2023).
2. National counterintelligence and security centre, foreign economic espionage in cyberspace (2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf (last visited Dec. 21, 2023).
3. Nitin Abhishek, Protection of Trade Secrets and Confidential Information in India, DEPENNING & DEPENNING (Dec. 12, 2023), https://depenning.com/blog/trade-secrets-confidential-information/?utm_source=mondaq&utm_medium=syndication&utm_term=Intellectual-Property&utm_content=articleoriginal&utm_campaign=article (last visited Dec. 22, 2023).
4. Author, "Title of the Article," DIGIALERT (November 30, 2023), available at https://www.linkedin.com/pulse/cyber-espionage-indian-context-case-studies-role-nation-states-7tvoc/ , last accessed on Dec 24, 2023.
5. SAMEER PATIL, Expanding Chinese cyber-espionage threat against India, RAISINA DEBATES (Apr. 18, 2022), https://www.orfonline.org/expert-speak/expanding-chinese-cyber-espionage-threat-against-india ,accessed on Dec 23, 2023, OBSERVER RESEARCH FOUNDATION.
6. Namrata Biji Ahuja, "Everything on the internet is monitored': Israel's cyber security head," THE WEEK (December 29, 2023), available at https://www.theweek.in/news/world/2023/12/29/everything-on-the-internet-is-monitored-israels-cyber-security-head.html (last visited Jan. 2, 2023).
7. Dana Rubenstein, "Nation State Cyber Espionage and its Impacts," https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/ (last modified Dec. 1, 2014), last accessed Dec. 23, 2023.
8. CIO&Leader, "Rise In Cyber Espionage For India In 2022: Report," https://www.csoforum.in/article/2022/01/14/rise-cyber-espionage-india-2022-report (Jan. 14, 2022), last accessed Dec. 24, 2023.
9. Dr. Gatra Priyandita, Bart Hogeveen, and Dr. Ben Stevens, "State-sponsored economic cyberespionage and the risk to nations' prosperity," Briefing Note to G20 Leaders' Summit, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-11/State-sponsored%20economic%20cyberespionage%20-%20Briefing%20note.pdf?VersionId=MBLZXniUgZCtf0OSXTA9vxUlzlNcfo32, last accessed Dec. 25, 2023.