Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 87 – 90 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CYBER WEAPONS AND NATION-STATES: THREATS AND RISKS

Dr. Nato Jiadze
Officer retired, MoD of Georgia, Invited lecturer at the Caucasus University
email: jiadzenatalia@gmail.com, njiadze@cu.edu.ge, njiadze@mod.gov.ge

ABSTRACT: As the digital landscape evolves, cyber weapons have become pivotal tools for nation-states to assert dominance, engage in espionage, and conduct warfare. This article will explore the growing role of cyber weapons in state-sponsored operations, focusing on how these digital tools are used to disrupt critical infrastructure, compromise national security, and manipulate political landscapes. By examining recent case studies and analyzing the evolving tactics of nation-states in cyberspace, the presentation will highlight the key threats posed by cyber warfare. It will also address the different levels of nation-state attackers, the dual-use nature of cyber weapons, the role of cyber-arms manufacturers, and the challenges of attribution.

KEYWORDS: Cyber weapons, Nation-states, APT, Dual use cyber weapons, cyber Militia, cyber-arms manufacturers.

INTRODUCTION:

The fundamental nature of national security threats has not changed, but cyberspace has introduced a new domain for conflict and warfare. It offers a delivery mechanism that amplifies the speed, stealth, precision, diffusion, and power of attacks. While activity in cyberspace does not automatically constitute a hybrid threat, cyber operations frequently complement other forms of harmful activity in hybrid scenarios.

Cyber interference consists of operations by state or non-state actors conducted in cyberspace. If this activity targets critical infrastructure, for instance, by cyber means to achieve political/military aims alongside other activity by an outside hostile actor – we have hybrid action. Cyber interference, in its priming phase, can effectively spy on and manipulate electronic and information systems. At this juncture, it would be premature to talk in terms of waging war. It is not possible at this point to know whether the activity will escalate into war.
Since the 1970s Information and Communication Technologies (ICTs) and digital technologies have become an increasingly crucial part of military command and control. The integration of digital technologies has allowed military operations to transform the defense industry, advances like smart weapons, real time battlefield management, network-centric solutions, superiority in air and outer space, and software-based solutions to ground troops all have key roles today.

HOW HACKERS CHANGE STATECRAFTS

Today one of the primary ways governments shape geopolitics is by hacking other countries. Government hackers continually find ways to advance their states interests and hinder those of their adversaries. Cyber operations show up again and again in the sophisticated modern states playbook. Hackers wiretap, spy, alter, sabotage, disrupt, attack, manipulate, interfere, expose, steal and destabilize. Government hacking has evolved and accelerated over past two decades.
A hack is any means of subverting a system's rules in unintended ways. The tax code isn't computer code, but a series of complex formulas. It has vulnerabilities; we call them "loopholes." We call exploits "tax avoidance strategies." And there is an entire industry of "black hat" hackers intent on finding exploitable loopholes in the tax code. We call them accountants and tax attorneys. Hacking

underpin our society: from tax laws to financial markets to democracy. Powerful actors using hacking tool to bend our economic, political, and legal systems to their advantage. [1]

GOVERNMENT CYBER THREATS AND CYBER-ARMS MANUFACTURERS

Nation-state cyber threats can be categorized into three levels:

- Advanced Persistent Threats (APTs): Highly sophisticated, state-sponsored cyber units with extensive resources and expertise. Examples include APT29 (Russia) and APT41 (China).
- Cyber-Arms Customers: States that purchase cyber weapons from external manufacturers due to a lack of domestic capability.
- Cyber Militias: Non-state actors or patriotic hackers who support state objectives, often with plausible deniability.

Advanced Persistent Threats (APTs)

APTs are typically nation-states with the capability to develop and deploy sophisticated cyber weapons. These countries possess the resources, expertise, and motivation to create their own tools and execute advanced cyber operations. While the list of such countries is debatable, it commonly includes the United States, the United Kingdom, Russia, China, Israel, North Korea, Iran, India, and, to a lesser extent, Argentina.
These nations engage in cyber activities that range from espionage to destructive attacks. APTs are often used for state-sponsored operations, targeting other countries to gain intelligence, disrupt critical systems, or achieve strategic objectives [2] [3].

Examples of notable cyber-attacks include:

- **2012**: The U.S under President Obama, accelerated cyber operations against Iran[4].
- **2018**: Russian hackers compromised DNS-based systems, with WikiLeaks revealing sensitive information.
- **2020**: China was implicated in a massive breach of U.S. government data.
- **2013**: The NSA was caught spying on Brazil.
- **2021**: The United Arab Emirates (UAE) launched its own cyber operations.
- **2008**: Russia conducted cyber-attacks against Georgia.
- **2022**: Russia deployed destructive malware against Ukraine ahead of its invasion[3]

These cases highlight the dual nature of cyber-attacks: some are focused on espionage, while others aim to cause tangible destruction. A particularly striking example is the ongoing conflict between Russia and Ukraine. In 2022, Russia utilized destructive malware against Ukraine in the early stages of its invasion, causing significant disruption. Interestingly, this cyber campaign was more effective in creating chaos before the physical conflict began. However, the effectiveness of cyber-attacks tends to diminish during active warfare, where kinetic operations often take precedence.

Cyber Militia

Some countries are not sophisticated enough to develop their own cyber weapons, so they purchase them from external sources. There is an entire industry of cyber arms manufacturers that produce and sell cyber weapons to nations that lack the in-house capability to create their own.
For example, in 2013, the Syrian Electronic Army used commercially available cyber weapons to attack Sweden and several other countries. Interestingly, instead of relying solely on commercial

tools, they also used hacker tools from the dark web. They downloaded criminal hacking tools and repurposed them for national interests.

Countries like China use both Advanced Persistent Threats (APTs), which are highly organized and state-sponsored cyber units, as well as cyber militias. Russia also benefits from cyber militias and patriotic hackers—individuals or groups who voluntarily assist the government in cyber operations. These hackers often carry out attacks on behalf of the state, and Russia does not sanction them because they are serving the state's objectives.

In this way, cyber militias provide governments with a flexible, cost-effective way to engage in cyber operations while maintaining plausible deniability.

Sometimes they are patriotic hackers , Russia do not prosecute them because they do the states work. The other case is patriotic hackers help to Ukraine, there were involved about 4000 hackers to support Ukraine at the beginning of war-they hacked Russian Transport system and slowed down movement of troops and transport.

CYBER ARMS MANUFACTURERS

Cyber-arms manufacturers are entities, often supported by their governments, that develop and distribute cyber weapons. These manufacturers are based in various countries, including Italy, Germany, the UK, and Israel. Interestingly, Israel has emerged as a prominent player in this domain. Israeli firms not only develop cyber tools for national security but also export these technologies as a tool of diplomacy, providing capabilities to other countries in exchange for political or strategic agreements.

Many of the products developed by these manufacturers are dual-use technologies, meaning they can be employed for legitimate purposes, such as surveillance and law enforcement, or for oppressive activities like censorship and political repression. For example:

- **FinSpy**: A surveillance tool used for monitoring individuals [5].
- **Pegasus**: A piece of spyware that has been used in both democratic and authoritarian states. While some governments, such as the FBI in the United States, use tools like Pegasus to track criminals, others, such as Uzbekistan, have employed it to suppress dissent [6]

Numerous documented cases highlight the misuse of Pegasus for attacks on journalists, activists, and opposition members.

Other products, such as Blue Coat Systems' tools, illustrate how seemingly legitimate security technologies can be misused. In Syria, for instance, Blue Coat tools have been deployed to censor the internet. Similarly, some police forces have used cyber tools for lawful criminal investigations while others have exploited them to spy on political parties, raising significant ethical concerns.

Compounding the problem, international restrictions on the sale of such tools can be circumvented by third-party transactions, allowing repressive regimes to acquire these technologies indirectly. This gray area makes regulating the industry particularly challenging, as it is often difficult to control who ultimately uses these products and for what purposes [7].

CONCLUSION

Unchecked, cyber weapons pose significant risks to global stability. They threaten to destabilize financial markets, undermine democratic systems, and disrupt societal norms. As artificial intelligence begins to amplify these capabilities, the potential for catastrophic consequences grows. However, understanding the hacker mindset and leveraging defensive technologies can mitigate

these threats. By fostering international collaboration and strengthening cyber defenses, the global community can strive for a more secure digital future.

cyber weapons have become indispensable tools for nation-states to assert influence and achieve geopolitical goals. As cyberattacks continue to evolve, the line between peace and warfare is becoming increasingly blurred. Nation-states, cyber militias, and cyber arms manufacturers all play significant roles in this landscape, and the dual-use nature of cyber technologies makes it challenging to regulate their development and deployment. As the cyber arms race intensifies, understanding the tactics, threats, and risks associated with cyber warfare is essential for maintaining global stability and security.

ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

REFERENCES

[1] Bruce Schneier - A Hacker's Mind. February 7, 2023.
[2] David E. Sanger -Obama Order Sped Up Wave of Cyberattacks Against Iran June 1, 2012.
[3] National Institute of Standards and Technology (NIST). "Advanced Persistent Threat Definition," 2011.
[4] Nicolae. Sfetcu, Cyber Warfare: A Comprehensive Overview. Chapter: APT Definition, History, and Features
[5] Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri, and John Scott-Railton You Only Click Twice FinFisher's Global Proliferation, March 13, 2013
[6] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert-Pegasus Spyware to Operations in 45 Countries, September 18, 2018
[7] Ben Buchanan - The hacker and the state cyber-attacks and new normal of geopolitics