Military Cyber Threats:

Transformations in Unconventional Security Threats

By Ehab Khalifa[1]

Coordinator- Monitoring Technological Developments Unit, Future Center for Advanced Research and Studies,

Abu Dhabi, UAE

[1] - Email: hoba_way@yahoo.com, Address: UAE, Abu Dhabi, Elmoror St, Aldana Area, Darwish tower, flat 303, Po Box: 111414

Abstract:

Cyber attacks have evolved from destroying and stealing data, to controlling weapons and infrastructure, which increases their damaging effect. An example of such cases are the Stuxnet and Flame virus that affected the Iranian nuclear program, and the successful operation to control American RQ-170 Drone by the Iranian authorities.

With the development of cyber power to be a military doctrine in defense and attack strategies, it has become an indispensable factor in military operations, as cyber attacks could include espionage, military and strategic data stealing and corruption, denial of service attacks, or even control on command and control systems. It is also contributing to the reinvention of international relations tools and the rejoining of new security concepts, like cyber diplomacy, cyber warfare, cyber intelligence, cyber

This report seeks to answer questions related to the effects of cyber power on military operations and the unconventional transformation in security threats.

Key Words: Power, Cyber, warfare, Intelligence, Military, espionage, Diplomacy.

Changing the Nature of Power

Man has always sought to discover and develop natural territories, starting from creating settlements on land, to traveling across oceans, to invading the outer space. Finding no more accessible natural environments to conquer, mankind started exploiting manmade environments, starting with "Cyberspace."

Irrespective to the fact that it is manmade (Nye, May 2010)[1], cyberspace has many similar characteristics to the previous environments like navigation, trading, communication, and exercising power. At the same time the geography of cyberspace is much more manageable than other environments; mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a button(Nye, June 2011)[2].

Before introducing any analysis, it is important to clearly define the term "cyberspace," which means "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers(Department of Defense Dictionary of Military and Associated Terms, 2010)[3]."

It is well known that technology has a significant impact on world politics, from the invention of 'movable type' in the fifteenth century that participated in the European reformation, to the invention of 'cyberspace' that contributed to the informational revolution. We can see the effects of changes in the nature of power from **Hard power,** which rests on coercion and payment using economic and military tools, to **Soft power** that rests on framing agendas, and attraction or persuasion, and finally evolving to **Cyber power** which can be defined in terms of a set of resources that relate to the creation, control and communication of electronic and computer based information, infrastructure, networks, software, and human skills (Nye, June 2013)[4].

While states seek to acquire power to promote their position in the international arena, especially cyber power, they began to develop cyber infrastructure, and adopt cyber strategies, not only to strengthen their cyber security but also to develop military, economic, and political strategies. Also many nations now are incorporating cyber warfare as a new part of their military doctrine (Hildreth 2001)[5].

Diffusion of Power

Because of the easy accessibility, low price of entry, anonymity, and vulnerability of cyberspace, more actors have a capacity to exercise cyber power. States are no longer the only actors in cyber domains, which are represented by power diffusions between a vast numbers of actors.

It is well known that non-state actors like multinational corporations, non-governmental organizations, terrorist groups, criminal groups, and individuals themselves have become actors in politics through cyber power.

We can also find power diffusion in both internal and external levels, with a minimal role of the state in favor of sub-state actors (Political Activists & NGOs) and transnational actors (Terrorist Groups & Criminal Organizations). This leads to the decline of state sovereignty, which initially had dominated international politics. In addition, information will not be a distinctive advantage and exclusive right for governments since it will be available to each actor in the cyber domain. States might have to start depending on private media and non-profit entities to get information, and they may have to adopt strategies to secure their information, such as hacking into other users information.

Cyber Warfare Tools

It is clear that cyberspace has its effect, not only on human behavior, but also on all aspects of life. The employment of cyberspace capabilities in different fields makes it a new source of power, and the actor who has, and is able to use cyber technology can achieve his/her goals and strategies. That is why the nature of power, as well as the sources of power and threats, are changing.

Many cyber-attacks have been launched in recent years, aiming to achieve political, ideological, military, and economic goals. These attacks use different kinds of weapons, not the traditional weapons used in warfare, but cyber weapons, like viruses, worms, Trojan horses, script attacks, rogue Internet codes, and denial-of-service (DDoS) operations. Although these electronic weapons are measured in kilobytes, they are extremely effective and can cause severe damage. An example of this is the virus "Flame and Student" that succeeded in slowing down Iran's ability to develop a nuclear weapon. The massive piece of malware secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare for a cyber-warfare campaign (Washington post, June 19, 2012)[6].

Military Applications

Cyber Diplomacy

Even during wartime, diplomacy and backdoor channels never cease to reach a compromise, therefore it is necessary to mention it.

Cyber diplomacy is considered the bridge between public diplomacy (social networks and media) and formal diplomacy (formal negotiations between governments), as it increases the ability of communication between people and gives them the chance to exchange cultures and ideas, while simultaneously allowing governments the chance to interact directly with people out of their executive authority.

The US government attempted launching a virtual embassy to help the Iranian people interact with the US government through a website, which included all the important and necessary information and procedures needed for the USA. However, the Iranian government blocked the website in Iran upon its launching. Still, it is considered the first attempt to interact directly with people with no governmental diplomatic relations.

Cyber Intelligence

The invention of cyber space has contributed to the evolution of espionage, with large security institutions such as The National Security Agency (NSA) contributing in the field and providing new methods of spying. Technology gives nations the opportunity to spy, not only on leaders and decision makers, but also on millions of people, by monitoring their daily communications, recording their telephone calls, saving their emails and chat conversations, and recording their digital life. Therefore, the problem is not in obtaining the information but rather in managing it.

One of a country's main goals to ensure its survival is to gather information about its enemies and even its allies. In the past, nations sent spies to gather critical and confidential information related to national security, nowadays technology has facilitated the ability to spy, not only on decision makers, but also on people. An example of this occurred by the United States when The National Security Agency recorded millions of French phone calls, including those involving individuals with no links to terrorism (france24, October, 2013)[7], even though France is not an enemy of the US. Another incident occurred on a higher level, when the NSA monitored the phone conversations of 35 world leaders (The Guardian, October 2013)[8].

Nations that have, and are able to produce, technology can record millions of phone calls, monitor billions of emails every day, and save individuals' private data. In other words, our daily lives become archived in technology companies and security agencies' databases. This makes the problem not in tracking or getting the information, but in analyzing and managing mega data to reach the correct decision.

Cyber Psychological Warfare

New media is like a two-sided sword; it can be used to ease communications, but it can also be used as a weapon for spreading ideas. Ideological groups, interest groups, and non-social movements, as individuals or nations, can use the Internet and new media tools to start Psychological warfare.

In 2003, before the Iraqi war, the American Army sent emails to the Iraqi troops through internal systems, asking them to leave their arms and go home, and informing them that they would resume their positions after the removal of Sadam Hussein. This has affected the Iraqi army's resistance as some soldiers left their positions.

The Defense Advanced Research Projects Agency (DARPA) launched a program in 2011 to help the military stay updated with what is being communicated through the social media, particularly in areas where troops are deployed (Centre for Research on Globalization, July 2011).[9]

Targeting Civil Cyber Infrastructure

The problem with critical infrastructure is that it depends largely on technology, like power plants, nuclear stations, high dams, transportation and aviation systems, and financial transactions. Since this type of infrastructure encompasses all assets, systems, and networks that are vital to a country, any incorrect exposure could have severe consequences and could result in great losses. Just a small virus, made of kilobytes, could infect the whole network and have a massive impact.

Every now and then we can see American officials accuse China of targeting American cyber infrastructure, especially in the economic and financial sector, that include stealing data of copyright products, or hacking financial networks for banks, stock markets or multinational corporations.

Targeting Military Cyber Infrastructure

Military infrastructure is not excluded from cyber-attacks, as virus maps and characteristics become more complicated. The obvious example is Stuxnet and Flame Viruses. It succeeded to slow down the Iranian nuclear program although economic sanctions didn't succeed, and it affected 16.000 computers, and caused the program delay because of centrifuges infection. His example could be sufficient to know how computer viruses could control physical infrastructure.

Military Espionage and Stealing Information

One of national security's biggest concerns is that cyber technology could expose their military information, like military strategies, soldier deployment maps, weapon designs, and missile based deployments.

Most countries pay attention to securing secret and public military networks, and neglect military contractors who perform projects for defense ministries. As a result, military secrets can become vulnerable to cyber-attacks from those contractors.

A traditional example is the US-China cyber security case, when the US authorities accused the Chinese government of stealing information related to American national security, specifically economic and militarily information. China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program, the most advanced airplane ever designed (ROGIN, Jan 2010)[10].

Also the US Justice Department indicted five Chinese military officers in May 2014, with stealing data from six US companies and unions (The Guardian, May 2014)[11].

Another time, according to a confidential report prepared for the Pentagon leaders by the Defense Science Board, more than 22 major weapon systems, critical to the US missile defense and combat aircraft and ships, were compromised by Chinese hackers (The Washington Post, May 2013)[12].

Dominating Control and Command Systems

Military usage of cyber space is not limited to the available information it provides for manufacturing traditional and primary weapons, or securing information about a nation's critical military systems and weapons; it goes far beyond this.

Intelligence and military institutions are connected through wired networks, as are air defense, aviation, and missile guidance systems; satellites, nuclear submarines, and military industries, all rely on cyber space. Although they are highly secured networks, theoretically speaking, penetration is still possible.

Militaries monitor their aircrafts and naval fleets in the same way that individuals use GPS devices to monitor their cars and locations, however, this occurs at a much higher level.

If intelligence service agencies succeed to penetrate any of these networks, there would be deadly consequences for a nation's survival, as they would gain power over the nation's military system and therefore control the military's decisions. Although it seems difficult and unlikely, there are some examples on a lower scale, such as when the Iranian's defense forces brought down the American drone RQ-170 without shooting it (The Washington Post, December, 2011)[13].

Another incident occurred when the Israeli forces succeeded to penetrate the Syrian defense system and provided them with fake images[14] to launch air strikes that destroyed a nuclear reactor under construction in the Deir ez-Zor region in September 2007 (Cordesman, May 2013)[15].

Cyber Allies

Is it time for states to form allies confronting cyber-attacks? One of the main characteristics of cyber-attacks is that they can be used across borders. Computer devices can be used from anywhere to launch cyber-attacks through botnets, and affect the Internet service in many areas around the world. Hence it's important to encourage international cooperation between nations to start alliances focusing on cyber threats.

There are two ways in which cyber-attacks can be targeted. The first is for regional and international organizations to adopt new principles and policies of how their members will deal with these kinds of threats. NATO adopted this strategy in 2010 when the alliance asked its members to increase their awareness of, and defense against, the threat of cyber-attacks (DW, October 2010)[16]. The second way is to establish new alliances concerned only with cyber defense. This strategy was used when the US defense secretary asked Gulf defense ministers to enlarge cooperation in "air and missile defense, maritime security and cyber defense (The National, May 2014)[17]".

Although there are many benefits resulting from cyber alliances such as monitoring and tracking cyber-attacks, there are also several security concerns related to confidence, since there is no practical method to assure that states will not spy on each other and penetrate their critical cyber infrastructure, or monitor citizens' telephone calls or emails.

Conclusion

Cyberspace has become a source of threat to individual, national, and international peace and it will continue to grow as the world becomes more connected. Therefore, nations should develop strategies combating cyber threats and create means and procedures that can contribute to the achievement of specific national security objectives. Those means might be technological, organizational, or even human, and could include:

- Increasing global situational awareness about potential cyber threats and the circumstances in which they might arise.
- Promoting cyber threat awareness amongst parents, schools, and businesses, and enabling the workforce to secure their computers and take steps to protect their online identities, privacy, and finances.
- Designing an effective cyber defense strategy that protects a nation's homeland with a high priority for defending key infrastructure.
- Developing cyber infrastructure, and pre-emptive apparatus that can predict and fight cyber threats.

Securing government systems through good command and control systems that permit coordinated multi-regional and homeland responses to cyber threats (Kugler, 2009, P332)[18].

- Creating partnerships, between governments and the private sector that dominate cyberspace, to share information they deem relevant to cyber threats.
- Developing effective legal frameworks and enforcement capabilities to target and prosecute cybercrime.
- Promoting a secure, flexible, and trusted global cyber operating environment that supports international cyber security.

With the development of cyber power into a military doctrine in defense and attack strategies, it has become an indispensable factor in military operations since cyber attacks could include espionage, military and strategic data stealing and corruption, denial of service attacks, or even control on command and control systems. It is also contributing to the reinvention of international relations tools and the rejoining of new security concepts, like cyber diplomacy, cyber warfare, cyber intelligence.

[1] - Nye, Joseph, , **Cyber Power**, Cambridge: Harvard Kennedy School, Belfer center for Science and International affairs, May 2010, P1.

[2] - Nye, Joseph, Power and National Security in Cyberspace, in Kristin M. Lord and Travis Sharp Editors, **America's Cyber Future Security and Prosperity in the Information Age**, Volume 2, Center for a new American security, June 2011, p9.

[3] - Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, 2010. P70. accessed June 17, 2013. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[4] -Joseph S. Nye, Jr, **Cyber Power**, P4 on https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf On 8 June 2013

[5] - Hildreth, Steven A., , **Cyber warfare**, CRS Report for Congress, June 19, P1.

[6] - Nakashima, Ellen, U**.S., Israel developed Flame computer virus to slow Iranian nuclear efforts**, access date on 25 May 2014.http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware

[7] -**France summons US ambassador over 'spying',** May 19, 2014 http://www.france24.com/en/20131021-usa-spy-agency-nsa-recorded-millions-french-phone-calls/

[8] -**NSA monitored calls of 35 world leaders after US official handed over contacts**, May 19, 2014 http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

[9] -**Pentagon Seeks to Manipulate Social Media for Propaganda Purposes**, 19 May 2014, http://www.globalresearch.ca/pentagon-seeks-to-manipulate-social-media-for-propaganda-purposes/25719

[10] - ROGIN, JOSH, **The Cable: The top 10 Chinese cyber attacks (that we know of)** http://thecable.foreignpolicy.com/posts/2010/01/22/the_top_10_chinese_cyber_attacks_that_we_know_of

[11] - **Chinese military officials charged with stealing US data as tensions escalate**, 20 May 2014 http://www.theguardian.com/technology/2014/may/19/us-chinese-military-officials-cyber-espionage

[12] - **Confidential report lists U.S. weapons system designs compromised by Chinese cyber spies**, 28 May 2013, http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weaponsConfidential%20report%20lists%20U.S.%20weapons%20system%20designs%20compromised%20by%20Chinese%20cyberspies-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?hpid=z1

[13] - **Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing**, on May 23, 2014 http://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html

[14] - Clarke, Richard A., Knake, Robert, **Cyber War: the Next Threat to National Security and What to Do about It**, ecco publisher, USA, 2012, P P 16-20.

[15] - Cordesman, Anthony H., **Syria's Uncertain Air Defense Capabilities**, on 24 May 2014, http://csis.org/publication/syrias-uncertain-air-defense-capabilities

[16] - **NATO includes threat of cyber attack in new strategic concept document,** on May 27, 2014, http://www.dw.de/nato-includes-threat-of-cyber-attack-in-new-strategic-concept-document/a-6072197

[17] - **Pentagon chief Chuck Hagel to meet GCC ministers in Saudi Arabia** on May 27, 2014 http://www.thenational.ae/world/americas/pentagon-chief-chuck-hagel-to-meet-gcc-ministers-in-saudi-arabia#ixzz32vBclkbK

[18] - Kugler, Richard L., 2009, "Deterrence of Cyber Attacks", In Franklin D. Krammer, Stuart Starr, And Larry K. Wentz. Eds, **Cyber Power And National Security**, Washington, D.C: National Defense Up, P332.