Defense in the Cyber Domain

by **ME4 (NS) Weng Zaishan**

Abstract:

The proliferation of information and communications technology (ICT) in our everyday lives is becoming increasingly apparent. As such, there are new challenges revolving around cyber security. This article discusses the framework in which the Singapore Armed Forces (SAF) should function and collaborate with others in order to better maintain our cyber network and infrastructure. It also highlights the various changes required for our operations to actively achieve a high level of cyber security.

Keywords: Information and Communications Technology; Cyber Security; Cyber Warfare; Diplomacy and Deterrence

INTRODUCTION

The proliferation of information and communications technology (ICT) can be seen in every aspect of our daily lives. As of 2010, mobile networks are accessible to 90% of the world's population and internet users will surpass the two billion mark.[1] In Singapore, 81% of households had access to the internet by 2009.[2] The development of ICT has brought the world closer with increased connectedness and collaboration. However, the increase in efficiency and connectivity has created unprecedented interdependency that opens up opportunities for exploitation and sabotage by adversaries. At the national level, the security of these information and communication systems is viewed as a critical aspect of our economic resilience and the creation of a secure, trusted and strategic investment environment.[3]

With the exploitation of information technologies by the Revolution in Military Affairs (RMA), the network centric warfare of tomorrow sees our competitive advantage greatly determined by the reliability and effectiveness of the information and communication systems in coordinating operations and ensuring a successful campaign. The increasing dependency of military operations and society on information and communication systems has led to new challenges that entail exploiting and defending the cyber domain.

CYBER DOMAIN

Today, cyberspace has been widely considered the fifth domain of warfare after Land, Sea, Air and Space.[4] A common definition of the domain remains a challenge. The latest definition by the United States (US) Department of Defense is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Alternatively, the cyber domain can also be viewed as a metaphor for the array of mediums that provide information across the various parties. While it has also been popularly described as a virtual manmade environment, this

is only partly true. The construction of this domain, similar to the previous four domains, is built upon the physical properties and laws of nature. The technology of networks and communications are built upon the use of the physical properties of electrons and photons to transmit, store and modify information. The cyber domain is more clearly described and defined by using a layered approach.[6]

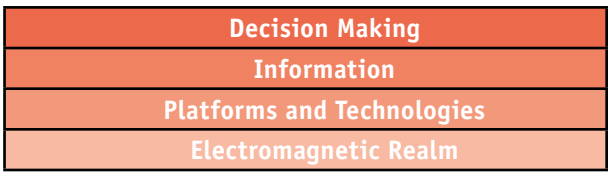

Figure 1: Layered illustration of cyberspace.

The first layer would be the physical **electromagnetic(EM) realm**, where electrons or photons are used as a wired or wireless medium of information transfer. While this physical layer is not visible to the human eye, it is nevertheless defined by the physical characteristics of frequency, wavelength and energy.

The second layer would be **platforms and technologies** that exploit the physical layer. They include all devices on which information can be stored, modified and transmitted through electrons and photons. This would consist of all the network infrastructure and physical hardware such as satellites, radio transmitters and receivers, telecommunications backbone, routers and switches, servers, individual computer nodes, fiber and copper cables, etc.

The increasing dependency of military operations and society on information and communication systems has led to new challenges that entail exploiting and defending the cyber domain.

The third layer consists of **information**. Information is collected, processed, stored, transmitted and received over cyberspace. Some of this personal, financial and secret military information are critical for the proper functioning of many daily activities.

The fourth layer would be that of decision making, which is based on the information acquired. This layer is made up of human interaction and cognition that stems from the information received. It is the domain where perceptions, awareness, understanding and beliefs help make sense of the situation and decide on the strategies to be employed in response.[7]

This layered illustration of the cyber domain will provide the basis for discussion on the common types of attacks that occur in the cyber domain.

CYBER ATTACKS AND THEIR IMPLICATIONS

There are many types of attacks in the cyber domain which could undermine effective information transmission and communication by affecting one or more of the layers described above.

Firstly, we have the conventional attacks on the platforms and equipment supporting the cyberspace environment. Such attacks include physical destruction of equipment and infrastructure such as routers, switches, fiber optic cables, etc. They include high-energy radio frequency (HERF) and electromagnetic pulse generators (EMP) that can be used to destroy electronic equipment.

The next type of attack is a direct attack on the virtual realm targeted at disruption of the services. The most common form is the denial of service (DOS) attack. In 2007, Estonia fell victim to a huge wave of DOS attacks that originated from a global network of botnets, targeting several government and corporate sites and online services.[8] Georgia was hit by similar attacks in 2008.[9]

Another form of attack is aimed at sensitive information and involves illegal access, espionage, theft, manipulation, etc. In 2008, classified US military networks were breached through the introduction of malware, resulting in the theft of sensitive data.[10]

There can also be indirect attacks via the physical realm which involve shutting down critical networks and infrastructure by disrupting their decision making control mechanisms, such as disrupting the electrical power supply or shutting down satellites that supply targeting data to weapons systems.[11]

The implications of the cyber attacks can be broadly classified into five aspects: military, social, economy, civil and psychology.

In the military aspect, one of the serious implications is the theft of confidential and sensitive information. As the former US Defense Secretary Robert Gates said, "the US is under cyber-attack virtually all the time, everyday."[12] This was in response to a report showing that US$300 million worth of information on the F-35 Joint Strike Fighter program was stolen. The Pentagon has also reportedly spent US$100 million on employing manpower and technology to repair damage from cyber attacks between October 2008 to April 2009.[13] In network-centric warfare, information plays a very important role in providing situational awareness and strategic planning.[14] Compromising or distorting this critical information can disrupt the coordination and execution of operations.

In the civil aspect, cyber attacks affecting electrical power grids or fuel pipelines could impose huge costs on households, businesses and the public services. An estimate of the cost, with reference to previous incidents, easily reaches US$6-10 billion for a single incident.[15] Emergency, police and civil defense services would also be overwhelmed by the higher demands.

In the economic aspect, maintaining business continuity and dealing with cyber attacks can result in huge costs for businesses. In a recent report by Symantec, 75% of 2100 businesses surveyed reported experiencing some form of cyber crime in the last twelve months. On average, cyber attacks cost each company £1.2 million each year in terms of lost revenue, branding and customers.[16]

In the social aspect, the general public is exposed to hacking and intrusion attempts on their personal computers. Problems also arise when they are "spammed" and exposed to sites that contain extremist ideology, illegal gaming, encouragement to perform petty crimes, etc. It is estimated that social costs related to cyber attacks have cost the Americans about US$400 billion and Koreans about 70 trillion won.[17]

In the psychological aspect, the disruption of services from attacks on critical infrastructure and business operations would affect the psychological state of the country, affecting the will to fight. Another possibility is the creation of unrest and confusion through subversive propaganda. The recent Wikileaks incident, where over 200,000 US diplomatic cables were revealed on the internet, not only caused dismay among Americans, but also undermined the diplomatic working relationships between the US and other countries.

The effects of cyber attacks are wide ranging and affect the military, government, private and public sectors as well as the general public. The extent of damage and seriousness would depend very much on the type of attacks and the agencies behind these attacks. The SAF must work closely with other government agencies (e.g. Infocomm Development Authority of Singapore, National Infocomm Security Committee, Association of Information Security Professionals, Singapore Computer Emergency Response Team), private companies and the general population to deal with the situation.

In the next section, the actors behind these attacks are further discussed to provide insights into their motives and the scale of their attacks.

ACTORS BEHIND CYBER THREATS

Due to the open and low barriers to entry into the cyber domain, there is a wide variety of diverse agencies that seek to manipulate the cyber domain to their advantage. They include governments, criminal

agencies, terrorist groups, malicious hacker groups, individual hackers, unwitting individuals, etc. They can be broadly classified into four categories: nation states, political and ideological extremist groups, organized criminal organizations, as well as individuals who break the law for fame or petty gain.

Nation states are countries that use the cyber domain to their advantage and manipulate it in order to achieve their objectives. Nation states usually have great resources and advanced capabilities at their disposal. The objectives are usually political in nature and range from espionage to intrusion and DOS attacks to full scale operations that could cause physical destruction to the critical infrastructures. In 2007, Israel launched a cyber attack on Syrian detection systems before conducting an air strike on a suspected nuclear facility.[18] Cyber attacks on Estonia in 2007, and Georgia in 2008, which were coordinated with the conflict with Russia, are widely suspected to be linked to the Russian government.[19] As concerns grow, many countries are stepping up their capabilities to conduct cyber warfare, Russia, the US, China, Israel and Iran among them.

Political and ideological extremist groups exploit the cyber domain in two main ways. Firstly, they use the internet as a means to recruit members and spread their ideology and beliefs. This has created a global network of terrorist groups that are decentralized and have flat hierarchies. This is a growing problem and the internet is playing a crucial role in the recruitment of terrorists.[20] The number of extremist websites have increased from "a handful in 2000 to several thousand today."[21] These terrorist groups could also purchase malware or hire computer experts to perform malicious activities in the cyber domain.

Organized criminal groups make use of advanced cyber tools and technology for fraud, theft, hacking, intrusion and introduction of viruses.[22] The underlying intent of such groups is usually financial gain. Heartland Payment Systems disclosed in January 2009 that intruders had hacked their servers to process 100 million payment card transactions per month for 175,000 merchants.[23] Larger criminal groups such as the Asian Triads, Japanese Yakuza and East European Mafia could exploit the cyber domain for serious crimes such as money laundering, drug trafficking and

Members of "Anonymous," an infamous organization of hackers that conducts cyber attacks.

industrial espionage. These criminal groups may also be used by government agencies to promote a political agenda.[24]

There are also individuals who act independently and are usually motivated by petty theft, entertainment and amusement, seeking revenge and a sense of satisfaction through disruption or vandalism. These individuals are usually not well equipped and do not cause massive disruption or damage to critical infrastructure.[25]

Conflict in cyber domain blends crime, political extremism and state sponsored military action in ways that are hard to distinguish and differentiate. The lines between the different actors are also blurring, as can be seen in the use of criminal groups by states to fulfill their objectives or a combined attack by states and individuals who support the same cause. It is thus important to differentiate between common and small scale cyber attacks and devastating ones that cripple day-to-day operations and constitute cyber warfare.

CYBER WARFARE

> *"For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill."*
>
> *– Sun Tzu*

By analogy to air and sea power, cyber power is the ability to make use of resources in the cyber domain to gain an advantage over adversaries and, if the need arises, to deny or deprive adversaries of such an advantage. In one popular definition, cyber power is defined as "the ability to use the cyber domain to create advantages and influence events in other operational environments and across the instruments of power."[26] The conduct of warfare and operations in the cyber domain takes place in two broad forms. The first is the gaining of *information superiority* in the use of the cyber domain to transmit information, denial of such information to the adversary and collection of tactical information. The second form of warfare would be to attack enemy morale in a *contest of wills*.

Information superiority provides better situational awareness, leading to better decision making during operations. In contemporary operations that span multiple domains, the military has leveraged on cyber technologies and platforms to gain increasing efficiency in command and control and future battle concepts aim to provide every soldier with a high level of situational awareness and battlefield coordination. These operations can only be maintained with the aid of cyber power.

Efforts cannot stop at the protection and sustenance of these defense networks—there has to be a holistic effort to look into the design, planning and implementation of network architecture, the introduction of rules and regulations in its usage, and the training of personnel to operate effectively and securely in the domain and remain able to function should the network go down.

The **contest of wills** involves either propaganda aimed at manipulating or demoralizing the adversary.[27] Asymmetrical operations can be conducted where the effects far outweigh the resources used to stage the attacks. These attacks would be mainly targeted at critical infrastructure, financial databases and information repositories, causing social panic and unrest.

DEFENSE STRATEGIES IN THE CYBER REALM

The next section explores the implications of cyber warfare on the basic tenets of Singapore's defense strategy, *diplomacy* and *deterrence*, and the importance of *offensive cyber capabilities*.

The International Multilateral Partnership Against Cyber Threats (IMPACT) Global Headquarters, a United Nations-backed cybersecurity alliance.

Diplomacy

In diplomacy, it is important for the definitions of the cyber domain and cyber attacks to be ironed out at the various summits and for the region to work together to combat the problem of cyber attacks. In the long run, more rules and regulations have to be established. At the recent November 2011 NATO summit in Lisbon, the gathered heads of states pledged to combine efforts on dealing with cyber threats. Similarly, regional cooperation could be pledged to deal with the cyber issues collectively in our region. Drawing lessons from other domains such as land, sea, air and space, it will take time and many discussions before an international standard of defined boundaries and common understanding of the cyber domain can be reached.

Deterrence

Deterrence can be developed by a few factors. The first factor to an effective deterrence policy is **resilience**. It is imperative for redundancies, servers that are able to handle increased network traffic and a secure backup channel, to be established. For critical infrastructure and services, a separate degraded mode of operation that can function without connecting to the wider internet would provide for the worst-case scenario. In the 2007 Estonia incident, the government had to shut off access to the internet to regain control of its systems and block out certain IP addresses. China has companies that control firewall access to guard against cyber attacks. The Infocomm Development Authority of Singapore and National Infocomm Security Committee are working on enhancing the resilience of our ICT systems through initiatives like the Infocomm Security Masterplan where the government and private companies cooperate to reinforce the robustness of critical infrastructures and services. In the same way, there is a need for a dedicated effort to ensure the resilience of defense networks. Efforts cannot stop at the protection and sustenance of these defense networks—there has to be a holistic effort to look into

the design, planning and implementation of network architecture, the introduction of rules and regulations in its usage, and the training of personnel to operate effectively and securely in the domain and remain able to function should the network go down.

The next factor would be **detection and identification**, which is the ability to detect and identify the aggressor. There is a need for active and preventive defense where the attacks are detected even before they breach the system. This would enable early identification and elimination of the threats before significant damage has taken place. The ability of tracing in the cyber domain has to improve so that agencies can be identified and dealt with despite the anonymous nature of the medium. The development of cyber forensics would help the identification of such adversaries.

It is important for the SAF to put continued emphasis on defense network systems to stave off cyber attacks

The last factor would be the possession of **offensive abilities** that could be used against identified aggressors. The ability to reduce cyber domain capabilities and mete out punishment in the form of a counter attack would serve to deter our potential adversaries.

24th Air Force – Air Forces Cyber 33rd Network Warfare Squadron members working hard in a Central Control Facility at Joint Base San Antonio.

Offensive Capabilities

The development of offensive cyber capabilities will add to the effectiveness of the military. The ability to launch cyber operations to achieve information superiority, disrupt and deny our adversaries access to the same and diminish their fighting will be a major advantage in military operations.

CONCLUSION

There has been a rapid increase in the dependence on ICT in all aspects of modern life. Technological advances have resulted in greater efficiency and effectiveness of many existing processes but have also introduced new vulnerabilities that many adversaries seek to exploit.

In this new domain, the general public, private companies, government and military are interwoven and highly interdependent. This calls for greater collaboration to deal with emergent challenges. Today, several initiatives and projects are underway to improve the robustness of cyber networks and infrastructure through the cooperation of stake holders at the national level. Similarly, it is important for the SAF to put continued emphasis on defense network systems to stave off cyber attacks.

New strategies of offense and defense in the cyber domain have to be formulated to deal with new threats. There has to be active management in navigating the rapidly evolving threat landscape of the cyber domain and the development of new cyber capabilities to provide a force multiplier for our own operations.

ENDNOTES

1. "The World in 2010 ICT Facts and Figures," International Telecommunication Union, 2010, http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

2. "Annual Survey on Infocomm Usage in Households and by Individuals for 2009," Infocomm Development Authority of Singapore, 2010, http://www.ida.gov.sg/doc/Publications/Publications_Level3/Survey2009/HH2009ES.pdf

3. "Infocomm Security Masterplan 2," Infocomm Development Authority of Singapore, 2008, http://www.ida.gov.sg/Infrastructure/20060816193152.aspx.
4. "Cyberwar: War in the Fifth Domain," *The Economist*, 1 July 2010, http://www.economist.com/node/16478792.
5. Joint Education and Doctrine Division, "Department Of Defense Dictionary of Military and Associated Terms as amended through 31 December 2010," Joint Publication 1-02, 8 November 2010.
6. Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," US Army College DIME Publication, 2008, http://www.carlisle.army.mil/DIME/CyberSpace.cfm.
7. Alberts, Garstka, Hayes and Signori, *Understanding Information Age Warfare* (Library of Congress, August 2001).
8. Clark Boyd, "Cyber-war: A Growing Threat Warns Experts," *BBC News*, 17 June 2010, http://www.bbc.co.uk/news/10339543.
9. Cooperative Cyber Defense Center of Excellence, "Cyber Attacks Against Georgia: Legal Lessons Identified," US Army College DIME Publication, November 2008, http://www.carlisle.army.mil/DIME/CyberSpace.cfm.
10. "Infected USB Drive 'Significantly Compromised' Pentagon Computers," *Computer Weekly*, 26 August 2010, http://www.infosecurity-us.com/view/12051/infected-usb-drive-significantly-compromised-pentagon-computers/.
11. Ten, Govindarasu, and Chen, "Cybersecurity for Electric Power Control and Automation Systems," *Systems, Man and Cybernetics*, 10 July 2007.
12. "Gates: Cyber Attacks a Constant Threat," *CBS News*, 21 April 2009, http://news.cnet.com/8301-1009_3-10224637-83.html.
13. "Pentagon Bill To Fix Cyber Attacks: $100M," *CBS News*, 7 April 2009, http://www.cbsnews.com/stories/2009/04/07/tech/main4926071.shtml?source=RSSattr=SciTech_4926071.
14. Olen Kelley, "Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative," US Army College DIME Publication, 15 March 2008, http://www.carlisle.army.mil/DIME/CyberSpace.cfm.
15. Anderson Economic Group, "Northeast Blackout Likely to Reduce US Earnings by $6.4 Billion," 19 August 2003.
16. Emma Barnett, "Cyber Attacks Cost Businesses an 'Average of £1.2 million' a Year," *Telegraph*, 22 February 2010,http://www.telegraph.co.uk/technology/news/7294810/Cyber-attacks-cost-businesses-an-average-of-1.2-million-a-year.html.
17. Brattle Group. "Economic Cost of the August 14th 2003 Northeast Power Outage: Preliminary Estimate," 18 August 2003.
18. David Fulghum and Douglas Barrie, "Israel used electronic attack in air strike against Syrian mystery target," *Aviation Week and Space Technology*, 8 October 2007, http://www.aviationweek.com/aw/generic/story.jsp?id=news/aw100807p2.xml&headline=Israel%20used%20electronic%20attack%20in%20air%20strike%20against%20Syrian%20mystery%20target&channel=defense.
19. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.
20. "Cyberwar: War in the Fifth Domain," *Economist*, 1 July 2010, http://www.economist.com/node/16478792.
21. Daniel Schorn, "Terrorists Take Recruitment Efforts Online," *CBS News*, 4 March 2007, http://www.cbsnews.com/stories/2007/03/02/60minutes/main2531546.shtml.
22. "A World Wide Web of Terror," *Economist*, 12 July 2007, http://globaltechforum.eiu.com/index.asp?layout=rich_story&doc_id=11062&title=A+world+wide+web+of+terror.
23. "Crimes in Cyber Space," Computer Crime Research Center, 28 May 2008, http://www.crime-research.org/analytics/computer_crime22/.
24. Byron Acohido. "Hackers Breach Heartland Payment Credit Card System," *USA TODAY*, 23 January 2009. http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm.
25. "Virtual Criminology Report 2009," McAfee Inc, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF.
26. Cornish, Hughes and Livingstone, "Cyberspace and the National Security of the United Kingdom," Chatham House Report, March 2009, http://www.chathamhouse.org.uk/publications/papers/view/-/id/726/.
27. Kuehl, "From Cyberspace to Cyberpower."
28. "Information Warfare," *Wikipedia*, 2007, http://en.wikipedia.org/wiki/Information_warfare.

ME4 (NS) Weng Zaishan is currently a Management Associate with Fung Group, having left service recently. He graduated from Nanyang Technological University in Electrical and Electronic Engineering (1st Class Honors), and went on to complete his Masters in Business Administration with Distinction at the University of Oxford. His last posting was with DyOC, Display and Processing Flight, Air Logistic Squadron, Air Defence & Operations Command.