National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE 5TH DIMENSION OF OPERATIONS: A CASE FOR ACKNOWLEDGEMENT OF A SEPARATE CYBER DOMAIN

Maj R.J. Busbridge

JCSP 41	PCEMI 41
Exercise *Solo Flight*	**Exercice *Solo Flight***
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.
© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2015.	© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2015.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 41 – PCEMI 41
2014 – 2015

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE 5TH DIMENSION OF OPERATIONS: A CASE FOR ACKNOWLEDGEMENT OF A SEPARATE CYBER DOMAIN

Maj R.J. Busbridge

“This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

Word Count: 5076

“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”

Compte de mots : 5076

INTRODUCTION

Information is a key weapon in warfare. Knowing from where an enemy is about to attack and where their defences are weak enables advantages in defensive and offensive strategies that can mean the difference between defeat and victory. Throughout history, military commanders have employed scouts and spies to collect information on enemy dispositions in order to obtain tactical advantage over that enemy. That collected information was only of use if the scout was able to convey his observations back to the commander in a timely enough manner, such that it can be exploited while it was still relevant.

The Mongols of the 12th and 13th centuries employed scouts, communicating via a semaphore system, to locate and bypass opposing forces and attack defenceless capitals. In this way the Mongols were able to defeat armies that greatly outnumbered them. Arquilla and Ronfeldt equate this knowledge advantage to a game of chess where one player can only see his own pieces, but the other one can see all the pieces. “Under such conditions, the player with knowledge of both sides’ deployments could be expected to triumph with fewer pieces.”[1]

Throughout the ages, innovations in the ways information could be communicated have led to advancements in the ways wars were fought and won. From smoke signals, to semaphore, to the telegraph, to radios; each successive development allowed information to be communicated over greater distances in shorter time. Those who could stay at the forefront of those technologies would maintain the advantage in the information battle space. The invention of the computer, followed by the development of the means to connect computers for the exchange information, revolutionized the way that information could be stored and transmitted. Computer and network technologies have advanced to the point where they are now integrated into almost every aspect of military operations. It is the

[1] John Arquilla and David F. Ronfeldt, *Cyberwar is Coming!*, Vol. P-7791 (Santa Monica, Calif.: Rand Corporation, 1992), 34.

primary medium for command and control, communications, computer, combat systems, and intelligence capabilities.

The notional environment over which the interactions between computers take place is commonly referred to as cyber space. It is where the ones and zeroes of binary, the basis of computing, come together to form the packets of information that represent stored information, transmitted bits of information and the programs and processes that make up the backbone of the networks. Networked environments enable users to connect, to create, share and store information, and to communicate with each other. The information stored and communicated within the cyber space is of tremendous value to enabling command and control of modern military forces. This information is also of value to an adversary who is looking to exploit information to gain an advantage in warfare. It is vulnerable to be exploited or attacked by adversaries who are able to infiltrate networks, and must therefore be defended. These offensive and defensive activities within the cyber space form the basis for cyber war.

There is much debate over whether cyber war exists as an entity to itself or whether it is only a portion of greater conflict involving the physical battle spaces. As a subset of that debate is the question of whether the cyber battle space exists as a 5th domain of operations. This paper will argue that characteristics of cyber space and the unique activities undertaken to operate within it are significantly different enough from the physical domains to categorize it as a separate Cyber Domain. The first section will examine the properties of the Cyber Domain in comparison to the physical domains in order to determine its uniqueness. The second portion will examine the operational functions as they can be applied within the Cyber Domain to determine its suitability as a domain of warfare separate from the others.

CYBER AS A DOMAIN

Most military operations are defined by the domain in which they occur. There are four universally accepted domains in which warfare has historically been waged. These are the Land, Maritime, Air and Space domains. There has been much debate over the development of a new potential battlefield and whether it can or should be classified as its own unique battle space termed the Cyber Domain. This section will examine what constitutes a domain within a military context and show that the properties of a cyber space are uniquely different from those attributed to the other traditional domains and should therefore be considered its own unique domain of operations.

First off, what constitutes a domain? During a Joint Command and Staff Program seminar discussing cyber warfare, subject matter expert LCol Torrington-Smith, the Team Lead for the inaugural Joint Cyber Operations Team at the Canadian Joint Operations Command, explained that a domain is best viewed as a medium through which you deliver effects.[2] This matches a definition provided by LCol W.C. McGuffin in his Masters of Defence Studies thesis paper, where he stated that "domains are where the activity takes place to create effects and ultimately compel an adversary to comply with the will of the victorious state."[3] So, the question is whether activities that occur within cyber space can be attributed to one of the four accepted domains, or if the cyber space exists as a domain unto itself.

[2] Nicholas Torrinton-Smith, "Seminar Discussion: Military Responses to Malicious Cyber Activities" (Canadian Forces College, Toronto, 8 May 2015.

[3] W. C. McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, Vol. JCSP/PCEMI 39-48 (Toronto, Ont.: Canadian Forces College, 2013), 15.

The Recognized Domains

We will start by examining each of the recognized domains of land, sea, air and space, which are primarily characterized by the physical space in which those types of operations are conducted and have definite boundaries that separate one from the other.

Human beings are land based creatures and without the aid of technology we are constrained to living and fighting on the land. As civilizations emerged, the land naturally served as the location of mankind's earliest battles and can thus be established as the original operational domain of warfare.[4] This original domain serves as a launching point for operations in the other domains, with ships, aircraft and space vessels commencing their operations from seaports, airports and launch pads connected to the land environment. It also represents the most basic forms of warfare to which all conflict has the potential to devolve if capabilities are lost within other domains. The Land Domain is defined as "The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals."[5]

As mankind struck out across the seas, the ships added a new dimension to land warfare that allowed armies to move greater distances in shorter times and to potentially bypass masses of opposing armies. Soon, the unique aspects of the Maritime Domain gave way to a new form of warfare with ships battling amongst themselves to control the seas. The wholly different fundamentals of warfare at sea led to development of new military theories, a new breed of naval specialists and independence of naval forces from their counterparts on the land.[6] Modern navies are fairly self-sufficient and can operate at sea for long periods of time but, while navies operate quite independently from their land counterparts, no nation lives on the seas, so as stated by strategic theorist Colin Gray, "Navies fight at sea only for the

[4] Paul J. Springer, *Cyber Warfare: A Reference Handbook* (Santa Barbara, Calif.: Abc-Clio, 2015), 56.

[5] United States. Joint Chiefs of Staff, *Department of Defence Dictionary of Military and Associated Terms*, Vol. 1-02 (Washington, D.C.: Joint Chiefs of Staff, 2004), p143.

[6] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 93, p19.

strategic effect they can secure ashore, where people live."[7] The Maritime Domain is defined as "the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals."[8]

With the development of powered flight a new dimension was added to the battle space. Initially air operations began as a means of intimate support to ground warfare, but it quickly evolved as it was realized that air power was able to strike at strategic targets way beyond the reach of the land forces. As with the development of the maritime domain, aircraft began battling each other for control of the air and a new form of warfare had evolved.[9] The main functions performed within the Air Domain are aerospace observation, air strikes, air transport and air control. The first three are typically conducted in conjunction with the Land or Maritime Domains. The last, air control, is conducted completely within the air domain to enable the first three, and also to ensure security and freedom of movement for land and sea elements below.[10] The Air Domain is defined as "The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[11]

Finally, as man found a way to escape the gravitational pull of the earth, satellites were sent into orbit, enabling efficient worldwide communications, global positioning systems and the ability to capture imagery of the earth's surface. Sovereignty enjoyed by nations in their surrounding territorial waters and the airspace above their land do not extend to the space beyond the earth's atmosphere, which allowed nations able to operate in the Space Domain to park satellites in geosynchronous orbit

[7] Colin S. Gray, *The Leverage of Sea Power: The Strategic Advantage of Navies in War* (New York Free Press, 1992), 9.

[8] United States. Joint Chiefs of Staff, *Department of Defence Dictionary of Military and Associated Terms*, 152.

[9] Springer, *Cyber Warfare: A Reference Handbook*, 57.

[10] LCol Brian Murray, What Air Forces Do, Canadian Air Force Journal, 38.

[11] United States. Joint Chiefs of Staff, *Department of Defence Dictionary of Military and Associated Terms*, 7.

above a nation of interest and observe activities on the ground.[12] The Outer Space Treaty of 1967 forms the basis of international space law and prohibits the deployment of weapons of mass destruction into the Space Domain. "States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[13] The Space Domain is defined as "the environment where electromagnetic radiation, charged particles, and electric and magnetic fields are the dominant physical influences and that encompasses the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere."[14] The costs and technologies required to launch rockets into orbit are prohibitive to the point where only a handful of nations are capable of operating within the Space Domain.

Each new domain represented an advancement of technology that still represents a hierarchy of ability to operate within them. All nations can operate on land and have some form of an army. Lesser developed nations may not have a navy or an air force. Because of the cost prohibitive nature and highly technical requirements for a space program, very few nations have been able to commit the expertise and resources to developing any form of space capability.

The main feature that differentiates the four recognized domains is that each is based on a different corporeal element that displays distinctive physical properties which require unique capabilities to operate within them. You need things that can float to operate in the Maritime Domain, things that can fly to operate in the Air Domain and things that can function in zero atmospheres, as well as the ability to get them there, in order to operate in the Space Domain. Each new capability came with fundamentally different technological expertise and requirements for tactics and strategy that did not

[12] Springer, *Cyber Warfare: A Reference Handbook*, 58.

[13] Singh, Nagendra; McWhinney, Edward (1989). Nuclear weapons and contemporary international law. Martinus Nijhoff, 236.

[14] United States. Joint Chiefs of Staff, *Department of Defence Dictionary of Military and Associated Terms*, 226

exist in previous domains of warfare. The uniqueness of each domain led to development of specialized forces trained and equipped specifically to operate in that domain. As argued by Paul Springer, a military studies professor at the US Air Force's Air Command and Staff College, "In each of these domains, military leaders have repeatedly argued that specialization within the domain is the only means by which a commander can possibly function in the modern war environment."[15]

The 5th Domain

Enter the cyber space. The Canadian Armed Forces defines the Cyber Environment as "the interdependent networks of IT structures, including the Internet, telecommunications networks, computer systems, and embedded controllers, as well as the software and data that reside within them."[16] It uses the term Computer Network Operations to refer to the activities that occur in cyber space and breaks those down into three types of tasks: Computer Network Defence, Computer Network Exploitation and Computer Network Attack.

The cyber space is unique in that, although the physical components of networks, the computers, servers, wires and users, exist within the physical space, the interactions with the ones and zeroes that make up the cyber space take place within a void that has no physical properties. This makes the cyber space vastly different that the spaces that define the Land, Maritime, Air and Space Domains. Many people refer to the cyber space as the 5th dimension, a term used synonymously with domain and battle space to indicate a 5th location in which to wage war. The term dimension is actually very fitting because the cyber space, lacking tangible physical properties, does not exist within the 3 dimensional battle space to which we are accustomed, so it represents a new dimension that must be conquered.

[15] Springer, *Cyber Warfare: A Reference Handbook*, 58.

[16] Canada. Dept. of National Defence, *Canadian Armed Forces Cyber Operations Primer* (Ottawa, Ont.: Chief of Force Development, Dept. of National Defence, 2014), 1.

In LCol W.C. McGuffin's 2013 Masters of Defence Studies thesis *Soldiers of Fortran: Militarization of the 5th Dimension*, the writer uses a similar process to compare the attributes of the Cyber environment with the existing domains to determine if it can be classified as a distinct domain. Ultimately he concludes that cyberspace should not be classified as a domain because cannot be constrained physically, nor can it be inhabited, which sets it apart from the other established domains.[17]

My conclusion from similar analysis and findings is that it is exactly the fundamental differences between Cyber and the recognized physical domains that make the cyber space stand out as a new battle space within the contemporary operating environment. The user that is engaged in cyber operations could be sitting in a tent, on a ship, in a plane or on a space station. The fact that the user could interact with the cyber space from virtually anywhere makes their physical location irrelevant to determining the domain in which they are operating. When they are at a workstation conducting cyber operations, their actions are happening within the Cyber Domain. All of the other domains are characterized by where they operate within a physical space. The cyber space, where cyber operations are conducted, does not exist as a physical space and cannot be constrained to any of the physical sectors that serve to define the other domains. If cyber does not fit within any or all of those physical spaces it must be considered its own domain.

THE OP FUNCTIONS IN CYBER

Now that I have concluded that the Cyber Domain is distinctly different from the other domains, I will examine the operational functions to determine that there are definite elements of each that can be employed within the Cyber environment. "Operational functions are the functional capabilities

[17] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 49.

required by a JTF in order to effectively employ forces."[18] The five operational functions in use within Canadian Forces doctrine are Command, Sense, Act, Shield and Sustain.

Command

The Command function is "The human dimensions of command embedded within competency, authority, and responsibility; the creative expression of human will necessary to accomplish a mission; the establishment of common intent; and, the structures and processes necessary to manage command."[19]

The cyber space was essentially created in order to enable command. The internet is a descendant of the ARPANET (Advanced Research Projects Agency Network), a US Department of Defense project to enable sharing of data between stations across the country, which birthed their MILNET (Military Network) in 1984 and eventually evolved into their current NIPRNET (Non-secure Internet Protocol Router Network) for unclassified communications.[20] Networks initially enabled the storage and transmission of data as well as near immediate written communications via email, but they evolved to include voice communications followed by video conferencing, real time chat, systems to visually represent the battle space and to provide situational awareness of events as they occur. The value of networked communications is obvious and it has allowed for tremendous advancements in the ways that militaries exercise command and control. They enable tightening of the OODA loop.

The OODA loop refers to a decision making cycle used in combat operations. The quicker that an entity can go through the process, the greater the advantage they will have against their opponent. The

[18] Canada. Dept. of National Defence, *Canadian Forces Publication 3.0: Operations* (Ottawa, Ont.: Joint Doctrine Branch, Dept. of National Defence, 2011), 1-5.

[19] Canada. Dept. of National Defence, *Capability Domains: Definitions* (Ottawa, Ont.: Chief of Force Development, Dept. of National Defence, 2009).

[20] Wikipedia, "ARPANET," http://en.wikipedia.org/wiki/ARPANET (accessed 5/8, 2015).

letters represent, in order of execution, the steps within the cycle, to Observe, Orient, Decide and then Act. Networks streamline inputs into the decision making process through immediacy of data and situational awareness, shortening the time it takes for commanders to observe and orient on a problem in order to decide on the way forward. Once the decision is made, networks enable the outputs of the process through rapid transmission of orders and direction through verbal, written and visual means.

These command support systems provided through the cyber space enable Command in all operational domains. They also provide a vulnerability that can be targeted through the cyber space. If you can affect the inputs going to a commander, or disrupt the outputs coming from the commander you can affect the adversary's ability to respond to a situation in a timely and effective manner.

Sense

The Sense function is "A single comprehensive entity that collects, collates, analyses, and displays data, information, and knowledge at all levels. Tactical, operational, and strategic assets are integrated into a single continuum."[21] It is tied very closely to Intelligence, Surveillance, Target Acquisition and Reconnaissance activities conducted within all domains. The purpose of these activities is to gather information on the operating environment and on the adversary's disposition and activities in order to determine their intent and to enable decision making by commanders.[22] There are a number of Sense operations, ranging from passive to active, which can be undertaken Within the Cyber Domain. While active means may involve intrusion into other systems, the goal is to avoid detection in order to protect the value of the information stolen.

[21] Canada. Dept. of National Defence, *Capability Domains: Definitions.*

[22] Robert Shimonski, *Cyber Reconnaissance, Surveillance, and Defense* (Amsterdam ; Boston: Elsevier/Syngress, 2015), 45.

Passive scanning of one's own systems can detect unauthorized intrusions into your own network. Monitoring these intrusions can give indications to which nations or non-state actors may be interested in your systems and what their intents might be. It can also reveal weak points in the system's defences that are attracting malicious attention and need shoring up.

Computer Network Exploitation is "directed, covert activity conducted through the use of computer networks o remotely enable access to, collect information from, and/or process information on computers or computer networks."[23] Organizations store vast amounts of data on their computer networks and, if penetrated, their systems could reveal details about their strength weaknesses and intents. In 2013 a Chinese hacker was able to infiltrate Boeing's systems and steal data related to a variety of US military aircraft, including the F35 under development.[24] China is in the process of developing their own 5th generation fighter, and gaining access to plans for NATO's 5th generation fighter could give them a competitive edge. We all know how the Rebel Alliance's ability to steal the plans for the death star enabled them to find and exploit a weakness to defeat the looming Imperial threat.[25]

Cyber operatives do not need to resort to covert mans to collect information on an adversary. There is ample information available through open sources on the internet and through social media sites that can yield valuable information about an enemy's capabilities, vulnerabilities and personnel.

Sense activities are very relevant in the Cyber Domain as they are not only able to support operations in cyber space, but can also be used to provide insights of value to operations taking place in all domains. Likewise, the Cyber Domain might benefit from activities taking place in one of the physical domain in order to enable its actions. Developers of the STUXNET virus that was used to disable uranium enrichment facilities in Iran required security clearances to be stolen from a computer technology

[23] Melanie Bernier and Joanne Treurniet, "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO," (2010), 230.

[24] Doug Stanglin, "Chinese Hackers Breach Top Weapons Designs," *USA Today*28 May 2013.

[25] George Lucas, *Star Wars* (Beverly Hills, CA: 20th Century Fox Home Entertainment, 1977).

company.[26] This physical act of espionage helped create a virus that was able to sabotage Iran nuclear program.

Act

The Act function is "The use of a capability to influence events across the spectrum of conflict and in either or both of the physical and moral domains. Act reflects an integration of capabilities from a variety of sources tactical, operational, or strategic."[27] Within the Cyber Domain, Act operations could constitute attacks on the integrity of an adversary's network systems, insertion or adjustment of data contained on an adversary's system to compromise its integrity, or causing the system to take an action that has deleterious effects in the physical domains. The *Canadian Armed Forces Cyber operations Primer*, produced by Chief of Force Development, introduces the term Offensive Cyber Operation as one that "produces effects, passive and active, within the cyber environment to disrupt, deny, degrade, distort and/or destroy information in support of mission success."

Denial of service is a disruption activity that involves sending a barrage of inputs to a network that overwhelms its capacity to process that data and prevents it from being able to provide its intended services to its intended users. In 2008, concurrent to the Russian invasion into the independent state of Georgia, Russian cyber forces conducted denial of service attacks on Georgian government websites to dislocate the government from the people and prevent a coherent response to the invasion.[28]

Another form of attack is corruption, in which malicious code is introduced with the intention of changing how a system functions without the operator's knowledge. The STUXNET attack is a perfect example: through an incredibly complex operation, an air-gapped industrial system was caused to

[26] Julian Richards, *Cyber-War: The Anatomy of the Global Security Threat* (Houndmills, Basingstoke, Hampshire ; New York, NY: Palgrave Pivot, 2014), 38.

[27] Canada. Dept. of National Defence, *Capability Domains: Definitions.*

[28] Springer, *Cyber Warfare: A Reference Handbook*, 37.

imperceptibly malfunction and cause long term damage to production. Such attacks are by far the most complicated due to the level of target system knowledge required and the means of defence likely to be encountered (depending on the target's value).

Other potential targets for a cyber attack include anything that relies on a computer for some aspect of its function, such as systems for power generation, media broadcasts, GPS augmentation systems etc. In military terms, this could include command and control systems as well as systems that control offensive and defensive systems. In 2007, Israel conducted a bombing raid against a nuclear reactor site in Syria. To enable its fighters to slip through the highly capable Syrian air defence network, Israeli forces wire able to insert a kill-switch into the network controlling the air defence system. As the attack went in the air defence system was shut down and the aircraft were able to enter Syrian airspace, execute the attack and return home without detection.[29]

These examples represent but a few ways in which Act activities can and have been perpetrated within the Cyber Domain.

Shield

The Shield function is "Force protection measures taken to contribute to mission success by preserving freedom of action and operational effectiveness through managing risks and minimizing vulnerabilities to personnel, information, materiel, facilities and activities from all threats."[30] Many nations choose not to, or do not openly admit that they do, actively engage in Computer Network Attack and Computer Network Exploitation activities. However, all nations that employ computer networks to support their operations engage in Computer Network Defence, which is "an activity conducted through

[29] Thomas Rid, *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013), 16.

[30] Canada. Dept. of National Defence, *Capability Domains: Definitions.*

the use of one's own computer networks to protect, monitor, detect, analyze and respond to unauthorized activity within computers and computer networks."[31]

Militaries dependent upon computer networks are vulnerable to intrusions via cyber space and must present an active defence to prevent further incursions. We've discussed the types of Act and Sense activities that can occur within the Cyber Domain and the potential advantage that can be gained by the adversary employing them. Command and control systems could be compromised, presenting erroneous data to a commander and eliciting ill-informed decisions. Worse yet, a compromised command and control system could provide an adversary access to information on force dispositions, locations and upcoming plans, giving them an advantage on the battlefield. The *Canadian Armed Forces Cyber operations Primer* introduces the term Defensive Cyber Operations to describe those operations that "defend friendly cyber capabilities, including data, necessary to maintain a commander's situational awareness and the ability to employ forces."[32] These Defensive Cyber Operations involve near constant monitoring within the cyber space to detect and repel intrusions into networked systems in order to protect the integrity of the information stored within.

The principle of confidentiality is commonly employed to assure information security and it involves segregating information by its value and restricting access to those with the proper authorizations or need to know.[33] This is not a new process as it was well established prior to the digital age, but it still remains a necessity, perhaps even more so, in the cyber space. Sensitive information is protected using access controls, encryption and authentication protocols. The Canadian Armed Forces operates DWAN, TITAN and SPARTAN systems to handle unclassified, secret and top-secret material respectively and likely employs additional systems that are outside of my need to know in order to

[31] Bernier and Treurniet, *Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO,* 230.

[32] Canada. Dept. of National Defence, *Canadian Armed Forces Cyber Operations Primer*, 4.

[33] Christian Czosseck and Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Vol. 3 (Amsterdam; Washington, DC: Ios Press, 2009), 214.

handle further segregated material. Unclassified systems are present in almost every workspace, are most accessible to the outside world and are therefore the most at risk to intrusion. Systems higher up in the classification chain are less abundant, have more restrictions on ho can access them and employ increased physical security protocols to prevent unauthorized access to the greater value information contained within. While these defence mechanisms involve differing networks that are usually accessed from physically distinct networks, the data they contain exists in cyberspace and is at risk to exploitation or attack.

The computer systems that ran the Iranian uranium processing plants that were attacked by the STUXNET virus were isolated from the outside world. It is believed that the virus, released via the internet, found its way onto the system of a network administrator at the plant, who inadvertently transferred the virus to the closed system when he manually patched into it to perform a system update.[34] This demonstrates one of the most effective ways to gain access to a network, which is to target poor information security practices of individual users. Users who connect unauthorized devices or fail to properly scrub them from viruses before introducing them to the system put the system at risk to intrusion. Poor practices such as weak or obvious passwords also make the system vulnerable. Part of Computer Network Defence involves maintaining robust security protocols to prevent physical intrusions into the system as well as education of users to reduce the instances of bad practices introducing vulnerabilities to the system.

Sustain

The Sustain function is “A grouping of all functions necessary to generate, deploy, employ, and redeploy a force. As an operational function, the term is to be taken in it broadest possible context.

[34] Richards, *Cyber-War: The Anatomy of the Global Security Threat*, 37.

Sustainment concerns are loosely grouped into three subordinate functions: materiel, personnel, and engineering."[35] With near constant evolution taking place in cyber technologies, network systems have a very limited shelf life and require continual adjustments in order to stay relevant in the cyber fight.

Each of the subordinate sustain functions referred to in the definition has a requirement to support the Cyber Domain. As technologies continually evolve, hardware, the materiel, needs to be upgraded to handle increasing requirements for bandwidth, storage capacity and computing power. The sustainment of the ones and zeroes that form the backbone of network systems, the engineering, is a perpetual effort. The wear and tear caused by thousands of authorized, and some unauthorized, users necessitates persistent monitoring, troubleshooting and management of user privileges and activities. Cyber warfare is a highly technical field requiring a high degree of specialization and constant training to stay on top of emerging technologies. The knowledge and experience of the cyber warriors that execute Computer Network Defence, Exploitation and Attacks must be effectively managed in order to sustain the ability for a military to remain competitive in the Cyber Domain.

For each of the Op Functions there are activities that take place within the cyber space, as well as supporting activities within the external physical domains, which enable the execution of operations within the Cyber Domain. LCol McGuffin argues that the Sustain function is where the case for a Cyber Domain fall short, stating that all sustainment in the cyber domain takes place in the physical domains. He offers up examples where ships, aircraft and even satellites can be replenished within their own domains, but "there is no comparable example for sustainment in cyberspace."[36] I return to my example of the cyber warrior sitting at a physical terminal in order to conduct activities within the cyber space. Regardless of his physical location, the effects he is creating are taking place within the Cyber Domain. The same is true for a system administrator who is conducting maintenance on the code that serves as

[35] Canada. Dept. of National Defence, *Capability Domains: Definitions.*

[36] McGuffin and Canadian Forces College, *Soldiers of FORTRAN: Militarization of the 5th Dimension*, 46.

the backbone for a network. Regardless of his physical location, the code he is maintaining is in the cyber space, so that sustainment activity is happening within the Cyber Domain.

Also, sustainment activities in support of a domain do not have to take place within that domain. While ships and aircraft may be able to be refueled within their domains, they each have to return to the land domain for maintenance, repairs and crew rotation. If the validity of those domains remain despite their reliance on presence in the land domain, so too can the validity of the Cyber Domain.

CONCLUSION

Domains are characterized by unique differences in their physical properties that require differing capabilities and distinctive practices in the ways operations are conducted within them. The Land Domain is characterized by the land, where mankind evolved and continues to reside. It is from the Land Domain where warfare was born, evolved and extended into the other domains. Ultimately, it requires no unique capabilities as, when technologies fail or other warfighting capabilities have been expended, warfare can always devolve to the most basic of practices, with armies squaring off on a battlefield with rudimentary weapons. The Maritime Domain is characterized by water and requires ships capable of floating. The Air Domain is characterized by air and requires aircraft capable of flying. The Space Domain is characterized by the lack of atmosphere and requires a space program capable of launching assets into orbit. The Cyber Domain is characterized by the ones and zeroes used to create, manipulate, store and transmit data within an artificial environment that has no physical properties. Its lack of physical properties makes cyber space unique as it cannot be attributed to any of the existing domains. The Cyber Domain requires cyber warriors who can manipulate the cyber space to protect friendly data and to exploit and attack the data belonging to an adversary.

Domains are also characterized by the ability to perform the operational functions of Command, Sense, Act, Shield and Sustain within them. Although the Cyber Domain requires a footprint within the physical space where computers, servers and cyber warriors can exist, each of the operational functions have been shown to have applications within the Cyber Domain.

Given that the cyber space's physical properties, or lack thereof, are uniquely different from those of the physical domains, and that cyber warfare involves all the operational functions, there is a clear case that cyber exists as a full warfighting domain alongside the Space, Air, Maritime and Land Domains.

BIBLIOGRAPHY

Arquilla, John and David F. Ronfeldt. *Cyberwar is Coming!*. Rand Corporation. Vol. P-7791. Santa Monica, Calif.: Rand Corporation, 1992.

Bernier, Melanie and Joanne Treurniet. "Understanding Cyber Operations in a Canadian Strategic Context: More than C4ISR, More than CNO." (2010).

Canada. Dept. of National Defence. *Canadian Armed Forces Cyber Operations Primer*. Ottawa, Ont.: Chief of Force Development, Dept. of National Defence, 2014.

———. *Canadian Forces Publication 3.0: Operations*. Ottawa, Ont.: Joint Doctrine Branch, Dept. of National Defence, 2011.

———. *Capability Domains: Definitions*. Ottawa, Ont.: Chief of Force Development, Dept. of National Defence, 2009.

Czosseck, Christian and Kenneth Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Cryptology and Information Security Series. Vol. 3. Amsterdam ; Washington, DC: Ios Press, 2009.

Gray, Colin S. *The Leverage of Sea Power: The Strategic Advantage of Navies in War*. New York: Free Press, 1992.

Lucas, George. *Star Wars*. Beverly Hills, CA: 20th Century Fox Home Entertainment, 1977.

McGuffin, W. C. and Canadian Forces College. *Soldiers of FORTRAN: Militarization of the 5th Dimension*. Masters Thesis (Canadian Forces College). Vol. JCSP/PCEMI 39-48. Toronto, Ont.: Canadian Forces College, 2013.

Richards, Julian. *Cyber-War: The Anatomy of the Global Security Threat*. Houndmills, Basingstoke, Hampshire ; New York, NY: Palgrave Pivot, 2014.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press, 2013.

Shimonski, Robert. *Cyber Reconnaissance, Surveillance, and Defense*. Amsterdam ; Boston: Elsevier/Syngress, 2015.

Springer, Paul J. *Cyber Warfare: A Reference Handbook*. Contemporary World Issues. Santa Barbara, Calif.: Abc-Clio, 2015.

Stanglin, Doug. "Chinese Hackers Breach Top Weapons Designs." *USA Today,* 28 May 2013, 2013.

Torrinton-Smith, Nicholas. "Seminar Discussion: Military Responses to Malicious Cyber Activities." Canadian Forces College, Toronto, 8 May 2015, .

United States. Joint Chiefs of Staff. *Department of Defence Dictionary of Military and Associated Terms*. Jp 1-02. Vol. 1-02. Washington, D.C.: Joint Chiefs of Staff, 2004.

Wikipedia. "ARPANET." . Accessed 5/8, 2015. http://en.wikipedia.org/wiki/ARPANET.