Archived Content

Information identified as archived on the Web is for reference, research or record-keeping purposes. It has not been altered or updated after the date of archiving. Web pages that are archived on the Web are not subject to the Government of Canada Web Standards.

As per the [Communications Policy of the Government of Canada](), you can request alternate formats on the "[Contact Us]()" page.

Information archivée dans le Web

Information archivée dans le Web à des fins de consultation, de recherche ou de tenue de documents. Cette dernière n'a aucunement été modifiée ni mise à jour depuis sa date de mise en archive. Les pages archivées dans le Web ne sont pas assujetties aux normes qui s'appliquent aux sites Web du gouvernement du Canada.

Conformément à la [Politique de communication du gouvernement du Canada](), vous pouvez demander de recevoir cette information dans tout autre format de rechange à la page « [Contactez-nous]() ».

CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES
CSC 31 / CCEM 31

NEW HORIZONS

**SPACE SECURITY: THE MISSING LINK
IN
CANADA'S NATIONAL SECURITY POLICY**

By /par
Major Tammy Harris

<u>Introduction</u>

On the morning of September 11, 2001, the American population did what it did every morning: they woke up, they showered, they ate breakfast, they dropped their kids off at school and they went to work. For the most part, the American population felt safe. At approximately 0846 hours, an aircraft crashed into the North Tower of the World Trade Center. Initially, by-standers were shocked at how this accident could have happened and while the world watched a second aircraft crash into the South Tower; everyone realized that the forces behind these incidents were sinister and the continental United States of America (USA) was under attack. By the time the third aircraft crashed into the Pentagon, the USA and Canada were on alert and scrambling assets to address an unidentified enemy. Terrorists were able to take four passenger aircraft turn them into guided weapons and launch them towards predetermined targets without detection.

September 11, 2001 was a wake up call for the world specifically, the USA and Canada. In April 2004, Canada published its first National Security Policy (NSP). This policy concentrated on three main national security interests: "protecting Canada and Canadians abroad; ensuring Canada is not a base for threats to our allies; and contributing to international security."[1] Albeit an excellent starting point, the NSP contains several bold statements that are sweeping generalizations with no apparent means or identified resources to achieve their objective. For example, "The Government is determined to pursue our national security interests and to be relentless in the protection of our sovereignty and our society in the face of these new threats."[2] In addition to these broad statements, the NSP neglects to address space security and Canada's dependency on

---

[1]   Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: National Library of Canada, 2004), vii.
[2]   Privy Council Office, *Securing an Open Society…,* 1.

space-based assets for surveillance, intelligence gathering, reconnaissance, communications, navigation, situational awareness, meteorology and early warning.[3] The potential loss of these services would affect Canada's ability to react to threats in a timely and informed manner thereby, increasing the risk of compromising Canada's national security. To mitigate this risk, Canada must amend the National Security Policy to incorporate space security and develop a comprehensive space security policy, which will address the protection space-based assets and the preservation the space environment.

The paper will begin by examining the components of a space-based asset, principally highlighting the segments that Canada can influence, existing threats/vulnerabilities and the impact to national security if these assets become inoperable. The paper will then give emphasis to countermeasures that Canada can implement to protect these assets followed by a brief description of current space treaties and policies, which will define the acceptable uses of space. The paper will conclude with a cursory examination of the NSP underlining Canada's dependency on space-based assets and the proposed framework for a space security policy.

Space Based Assets

Some people associate the phrase space-based asset with the space shuttle or a satellite while others think of NASA (National Aeronautics and Space Administration), the truth is all these parts comprise a space-based asset. Every space-based asset can be

---

[3] Department of Defense, *Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs* (Washington, D.C.: U.S Government Printing Office, 2003), 12.

broken down into four parts: the launch vehicle, the space segment, the ground segment and the communication link. Currently, Canada does not have an in-house launch capability therefore; it relies on other countries, mainly the European Space Agency and the United States, to address this deficiency. Consequently, it cannot affect the security of the launch vehicle or the space segment without assistance of these countries. In recognition of this lack of capability, this paper will not discuss in-depth two of the four segments: the launch vehicle and the space segment. Instead, the focus will be to those areas that Canada can influence mainly, the ground and the communication (radio link) segments.

The Ground Segment

The ground segment consists of several components: the tracking and control facility, telemetry, communications earth station, data reception and archival facilities.[4] Simply stated, the ground control segment has two major parts: the flight operations segment and the payload data segment. The flight operations segment is responsible for the command and control of the satellite where as the payload data segment is in charge of the management of the instrumental data.[5]

Upon achieving orbit, the satellite requires constant monitoring and tracking to ensure the orbit remains stable.[6] Satellite type and configuration will determine the amount of interaction required from the ground control segment. Satellites

---

[4]   Foreign Affairs Canada, "Military Questions to Space Vulnerabilities," http://www.dfait-maeci.gc.ca/arms/mcdougall2-en.asp; Internet;accessed 18 March 2005.

[5]   "Canadian Space Agency," http://www.space.gc.ca/asc/eng/satellites/envisat/about_segment.asp; Internet:accessed 17 April 2005.

[6]   D.J McCoubrey, and others, *Space Indoctrination Handbook* (Winnipeg: Canadian Forces School of Aerospace Studies, August 1996), 2-3.

that are more complex require constant communication to maintain a healthy orbit where as less complex satellites require minimal direction and are virtually independent from the ground control segment. In addition to restoring, maintaining and predicting the orbit, the ground segment relays orders to the satellite to execute operational missions while providing the interface between the customer and the satellite. [7] The ground segment is critical to the overall survival of the satellite and if the medium for transmitting data and information is comprised, the ground segment is ineffective. This medium commonly called the communication link is either direct from the ground segment to the satellite or relayed via another satellite or ground station.

The Communication Link

The communication link carries commands, communications, traffic, telemetry (science of remote measurement) and data back and forth from the tracking and control station to the satellite. [8] Every satellite is dependent on some form of a communication link to maintain viable operations. If the communication link is lost, for an undetermined period, the satellite will go into a safe mode for self-preservation; until communications are reestablished mission related operations cease functioning. [9] The communication link is not only the pathway for command and control, it also the medium to transmit information to users/customers. The communication link is to a space-based asset as the spinal cord is to the body; if severed the consequences are severe.

---

[7] Ed Wilson, "Securing The Heavens: A Perspective On Space Control" (Alabama: School of Advanced Airpower Studies Air University Maxwell Air Force Base, 1999), 24.
[8] Foreign Affairs Canada, "Military Questions to Space Vulnerabilities,"…18 March 2005.
[9] Wilson, "Securing The Heavens…, 68.

In summation, a space-based asset consists of four main components: the launch vehicle, the space segment, the ground segment and the communication segment. Once in orbit, the system requires all three major segments (ground, communications and space) to operate effectively. For that reason, the system is vulnerable to attack on the ground, in the air or in space. If one segment is offline, the entire system may fail hence; the probability for failure increases if no preventive countermeasures are in place. Fortunately, Canada has the capability to protect the ground and communication segments. An examination of the perceived threats to these components will follow.

Perceived threats to Space-Based Assets

It is important to remember that space-based assets are susceptible to attack at each major segment and the loss of any one segment renders the asset inoperable. Currently, there are numerous threats that threaten these assets and each segment faces a different set. Weaponization of space will be a considerable threat to space-based assets and the preservation of space. Currently, Canada has no intent or means to pursue this topic therefore; for the purposes of this paper, it will receive minimal discussion. Instead, this section will focus on the perceived threats to the ground and the communication segments.

Numerous avenues exist to attack a space-based asset. These avenues vary from delay, to deception, to disruption, to denial, to degradation, and finally, to destruction.[10] The ground segment is vulnerable to damage or destruction via direct fire, indirect fire,

---

[10]   Wilson, "Securing The Heavens…, 60.

ground, naval or air attack.[11] Vulnerability increases if the space asset is reliant on one ground station, which can also increase the risk to national security if the information it provides is, for example, early detection or surveillance. For a threat to be viable, an opponent must have the means, the capability and the intent to carry out an attack. "The appeal of physically attacking or sabotaging these ground control assets is that existing military assets can be used."[12] If intent is present, the potential to compromise the ground segment is highly possible because a large number of nations and terrorist groups have access to the required capability. By being proactive and defending against these threats, the probability of an attack lessens.

The communication segment is vulnerable to threats of different nature. One of the most productive ways of degrading or disrupting this segment is with electromagnetic jamming. "The object is to saturate the RF medium with electronic noise at the same RF band being used to communicate."[13] By saturating the RF band, two-way communications are impossible and the potential for catastrophic failure exists for the space segment. Another way to cause disruption to the communication segment is via spoofing. Spoofing is the ability to interject false data into the communication loop with the intent to cause the satellite or the ground controller to react inappropriately to this data; the reaction may cause a chain of events resulting in a catastrophic failure to the system.[14] The risk of attack on the communication segment is higher than one may think due to the countless number of people who have the technology to hack, spoof and jam the system.

---

[11]   "Army Space Reference Text,"http://www.fas.org/SPP/military/docops/army/ref_text/chap08.htm; Internet; accessed 23 April 2005.
[12]   Wilson, "Securing The Heavens…, 61.
[13]   *Ibid,…,* 68.
[14]   *Ibid,…,* 67.

To illustrate this point, conduct a search on the Internet to find out how to build a GPS or satellite-jamming device. The results of this search will be several thousand of hits. Assuming that the majority of these hits did not produce a useable jamming device, one would only have to contend with the small percentage that did yield a useable product. The small number of useable jamming devices can potentially harass space assets by disrupting or denying the system at a critical time, which may result in a deadly outcome. In today's world of asymmetric threats that are, neither predictable nor easily identifiable one must be prepared to defend against the most likely and the most dangerous course of action. Canada's Chief of Defence Staff, General Rick Hillier stated that the threat has changed from the "Bear" (the former Soviet Union) to a ball of "Snakes" that ranges from terrorism, organized crime, and proliferation of weapons of mass destruction.[15] The tools used to counter these threats may be intelligence gathering, early detection, surveillance or some other means; all of which rely on some form of information provided by space-based assets to accomplish their mission.

In summation, space based assets are extremely vulnerable to a wide variety of threats. In particular, the ground segment is vulnerable to conventional attack and the communication segment is vulnerable to jamming or spoofing. Awareness of these vulnerabilities is the first step in gaining recognition that a comprehensive space security policy is required; the second step is educating Canadians in regards to the potential impact on Canadian society and way of life if an attack is successful in degrading, disrupting or denying critical services provided by these assets.

---

[15]   Graham Fraser, "Forget The Bear- Now It's Snakes," *Toronto Star,* 19 March 2005.

Potential Impact from the Loss of a Space-Based Asset

The rippling effects of 9/11 spread worldwide and even though, these attacks did not target a segment of a space-based asset directly, the consequences and outcome were similar. The financial district, mainly the New York Stock Exchange, remained closed for six days because of security issues, lack of worldwide connectivity and limited redundancies. Three years later, on 08 September 2004, Wall Street executives outlined to Congress newly implemented security measures that would deter the efforts of al-Qaeda to disrupt the U.S. economy. At that time, over one hundred million dollars was spent on improving physical and cyber security by improving redundancies, developing remote operations sites, and geographically dispersing fiber optic routing; plus numerous other developments that remain on going.[16]

One of Canada's greatest fears is an incident that would force the closure of the Canadian/American border thus disrupting and denying cross-border trade with Canada's largest trading partner. If the economy is the Achilles heel of most nations, it is plausible to hypothesize that if one could create a disruption causing economic instability; an opportunity would exist to exploit this instability thereby indirectly, threatening national security. The problem in Canada is that people believe it will never happen to them. If one could rewind the clock and do a survey on September 8, 2001, whereby asking several hundred Americans if they thought it was possible for terrorists to hijack four airplanes, within twenty-four hours and use them as guided missiles directed at the Pentagon, the World Trade Center and the White House, would the majority answer yes or no. It is safe to assume that on 08 September 2001, the majority of people polled

---

[16]   Dan Verton, Computerworld, "For Wall Street, 9/11 Lessons Three Years in the Making", 08 Sept 2004, http://www.computerworld.com/securitytopics/security/story

would have answered no because that type of activity did not happen in the USA therefore; they felt safe from this type of threat. Canadians, also believe they in a country where bad things will not happen and it is this naïve outlook that makes it difficult to get the funding and support necessary to generate comprehensive policies that address confrontational issues such as space security. Hillier stated in a media interview that, "Canada and Canadians are at more risk now of direct attack than they have ever been during the Cold War…we've got to start treating Canada as an operational theatre."[17] He also suggested that if Canada were not involved in stability operations then instability would come to Canada.[18] Threats against Canada are real and two ways to defeat them is by acknowledging them and by developing countermeasures to defeat them.

Countermeasures

    With the knowledge that ground and communication segments are vulnerable to attack coupled with the potential security ramifications from losing these assets; it is prudent to implement countermeasures to mitigate or negate these vulnerabilities. There are several identifiable counter-measures available to defend against these threats: direct force, hardening, redundancy, terrain selection, early detection and finally, to more benign and diplomatic methods. Assuming that Canada will use direct force if the situation warrants and that the diplomatic channel is constant, these two countermeasures will not be discussed in-depth.

    Hardening or shielding is a countermeasure that tries to protect the electrical and electronic systems from threats that has potential to overload the system. Hardening

---

[17]   Fraser, "Forget The Bear- Now It's Snakes,"…19 March 2005.
[18]   *Ibid.*

mainly affects the communication segment by enabling enhanced encryption of the uplink and downlinks plus providing the ability to frequency hop, the ability to boost the signal power and if required, the ability to null the antenna to defeat the effects of jamming.[19]

Redundancy is a countermeasure, which allows for disruptions to components of the primary system without the loss of the entire system. If a component of the main system is unserviceable, then the back up system immediately kicks in without disrupting the overall system therefore; the transition is seamless to the user because the service remains uninterrupted. Redundant systems are separate from the primary system thus increasing the difficulty to deny the use of the system. The more critical the component, the more redundancies will be built into the system to ensure that the service cannot be disrupted.[20]

Early detection is one of the most productive countermeasures. Enhanced situational awareness enables one to predict a potential attack and develop a solution to prevent the attack or worst-case scenario a way to mitigate the impact. Coupled with early detection is terrain selection, which is extremely important when sighting the installation location for the components of the ground segment. Additionally, if in the ground station is located in a high-risk area then early detection is crucial, along with a force protection plan, i.e. theatre missile defence.[21] The ability to camouflage large items or equipment with distinctive signatures from would-be adversaries is critical to their survivability.

---

[19]   Foreign Affairs Canada, "Military Questions to Space Vulnerabilities,"…18 March 2005.
[20]   *Ibid.*
[21]   "Army Space Reference Text,"… 23 April 2005.

In summation, several countermeasures exist that Canada could implement to increase the security of their ground and communication segments of their space-based asset. These proposed countermeasures will incrementally increase the overall operating budget but the threat is out there. The development of a space security policy, which recognizes existing space treaties, would provide the guidelines and expertise necessary to counter these threats in a proactive way.

Space Treaties and Policies

The United Nations Committee on the Peaceful Uses of Outer Space currently, has five treaties and agreements actively in place:

1. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (commonly known as the Outer Space Treaty);

2. Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space;

3. Convention on International Liability for Damage Caused by Space Objects;

4. Convention and Registration of Objects Launched into Outer Space; and

5. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies.[22]

The aforementioned treaties/agreements provide countries with guidelines on the legal use and development of space. Canada is a ratifying member of four of the five treaties/agreements. Canada has not ratified the 1979 Moon Agreement. Currently, Canada does not intend to use force or commit hostile acts on the surface of the moon

---

[22]   United Nations, "Outer Space," http://www.oosa.unvienna.org/spacelaw/treaties.html; Internet; accessed 14 March 2005.

therefore; Canada has not ratified this treaty.[23] The United States, Russia, the United

Kingdom and China have demonstrated a concern over the use of space by ratifying the

same agreements/treaties as Canada and of note, global acceptance of these treaties is

high.[24] The development of a Canadian space security policy must acknowledge

Canada's ratification of these treaties/agreements by respecting the guidelines and

regulations established in these treaties.   For purposes of this paper, the two most

noteworthy are the Outer Space Treaty and the Convention and Registration of Objects

Launched into Outer Space.

The Outer Space Treaty, promulgated in 1967 by the USA, the United Kingdom

(UK) and the Russian Federation, is one of the founding documents for space

development. The core principles of this Treaty are: the exploration of space shall

benefit all mankind, outer space shall be available for the exploration and use of all

states, outer space can not be occupied by any state in order to make a sovereignty claim,

outer space is not to be armed with nuclear weapons or weapons of mass destruction, and

the moon and other celestial bodies are to be used for peaceful purposes.[25]

In summation, the basic framework of the Outer Space Treaty prohibits the use of

space for non-peaceful purposes and promotes humanity through the mutual benefit of

space exploration for all humankind therefore; the Treaty is an excellent supporting

document for the proposed space security policy. The intent of the proposed security

---

[23]   Foreign Affairs Canada, "The Non-Weaponization of Outer Space," http://www.dfait-maeci.gc.ca/arms/outer3-en.asp#4; Internet; accessed 18 March 2005.
[24]   Andrei Terekhov, *AnnualReport-2001,* Report Prepared for the Standing Committee on the Status of International Agreements Relating to Activities in Outer Space (Paris: International Institute of Space Law, 2001), 10-15.
[25]   United Nations, "Outer Space,"…14 March 2005.

policy is to increase national security by providing protection to the assets that have increased Canada's ability to predict, detect and defend against potential threats. The Outer Space Treaty is supportive of this initiative.

The Convention and Registration of Objects Launched into Outer Space requires mandatory registration of all assets launched into space. The space object registry helps mitigate the following problems: traffic management, enforcing safety standards and establishing liability.[26] The establishment of this registry coupled with the enforcement safety standards is an added layer of protection for space-based assets. Citing this Convention as a higher authority in the proposed space security policy will add substance and credibility.

Canada's National Security Policy

Canada's National Security Policy (NSP) released in April 2004, consists of six key strategic areas: intelligence, emergency planning and management, public health, transport security, border security and international security.[27] Each of these areas relies on the ability to exchange information and communicate rapidly, which necessitates the requirement for state of the art technology. This type of technology is dependent on space-based assets and for that reason, the need to identify and protect these assets is vital to the day-to-day operations required to maintain national security.

To illustrate how these strategic areas are reliant upon space-based assets, an in-depth examination of one of the six key strategic areas will follow. Canada's NSP recognizes intelligence gathering as one of its top priorities, "to manage risk effectively,

---

[26]   Foreign Affairs Canada, "The Non-Weaponization of Outer Space…18 March 2005.
[27]   Privy Council Office, *Securing an Open Society…*, viii-ix.

we need the best possible information about threats we face and about the intentions,

capabilities and activities of those who would do us harm."[28] Modern day collection

methods are human intelligence (HUMINT), imagery intelligence (IMINT), measurement

and signature intelligence (MASINT), open source intelligence (OSINT) and finally,

signal intelligence (SIGINT).[29] These different methods share a degree of reliance on

space-based assets to accomplish the task. For example, Special Operations Forces

(SOF) working in a hostile environment relaying targeting data over a secure satellite

phone or intelligence personnel interpreting the contents of satellite photos, both require

the services provided by a space-based asset. The NSP recognizes the need to increase

intelligence capabilities, create an integrated threat assessment centre and enhance review

mechanisms but it does elaborate on how it will secure the assets required to support

these objectives.[30] Albeit, it does acknowledge the requirement to improve cyber-

security in order to increase its effectiveness.

In summation, Canada's reliance on space-based assets to implement the goals of

the NSP is a concern, which needs to be addressed. Technological advances increase

effectiveness and efficiency but at the same time, increase vulnerabilities to attack.

Fortunately, the NSP recognizes the need to enhance cyber-security to protect critical

systems and infrastructure from potential terrorist attacks and other threats.[31] If the scope

of this enhanced cyber-security expanded to include the components of the ground and

communications segments and addressed identified threats and vulnerabilities, then the

---

[28]   Privy Council Office, *Securing an Open Society…*, 15.
[29]   *Intelligence Collection,* http://ffaculty.ncwc.edu/toconnor/427/427lect02.htm; Internet; accessed 16 March 2005, 2.
[30]   Privy Council Office, *Securing an Open Society….*, 15.
[31]   Privy Council Office, *Securing an Open Society…*, *26.*

skeleton of a space security policy would appear. If one were to put meat on those bones, then the framework for a comprehensive space security policy would soon develop.

Space Security Policy

Recently, Canada released its new International Policy Statement (IPS). This policy listed rogue states, failed and fragile states, international crime, weapons proliferation and terrorism as new and emerging threats against Canada. Prime Minister Martin also acknowledged that Canadians must make tough decisions to safeguard Canadian freedom, security, prosperity and way of life.[32] Previously mentioned, the first step to developing a space security policy was awareness and the second step was education. Formal recognition in the IPS of the threats who are most likely to attack space-based assets to degrade Canada's ability to conduct reconnaissance, surveillance, early detection, and intelligence gathering is a step in the right direction. As technology advances, Canada, like other countries, becomes more reliant on space-based assets and this reliance makes Canada vulnerable to significant economic disruption and possible security infractions if these assets are successfully denied.

The development and adoption of a space security policy will enhance Canada's overall security by mandating protection of space-based assets and supporting the preservation of the environment in which they operate. The report, *Space Security 2003,* prepared for the International Security Bureau of the Department of Foreign Affairs states, "space security is secure and sustainable access and use of space, and freedom

---

[32] Department of Foreign Affairs and International Trade, *Canada's International Policy Statement: A Role of Pride and Influence in the World* (Ottawa: Her Majesty the Queen in the Right of Canada, 2005), forward.

from space based threats."[33] In essence, space security is the ability to utilize space and space-based assets at a nation's will without the concern of deliberate disruption or denial of these assets. Unfortunately, in today's world of asymmetric threats, concern over the vulnerability of space-based assets is a reality therefore; the proposed security framework must be credible, sustainable and feasible.

The proposed framework for the Canadian space security policy consists of four sections: the legitimate uses and requirements of space, threat assessment, countermeasures and design guidelines.   Important to note, as Canada's ability to influence the space environment grows, the proposed policy will expand and adapt to address new capabilities or concerns.

The first section acknowledges the legitimate uses of space as outlined in all existing space treaties and agreements that Canada has ratified. The purpose of this section is to establish the operating parameters of space and delineate the arcs by which Canada can protect this environment and space assets. This section would require amending if Canada gained an in-house launch capability and changed its position on weaponization of space.

The second and third sections go hand in hand and currently are the most relevant to Canada. As quickly as technology evolves so does the threat. Canada's reliance on space-based assets for tasks critical to maintaining national security creates the requirement for continuous threat assessment. A proposal to satisfy this requirement would be to create a space security threat assessment team responsible for threat assessment and countermeasure development. In theory, this team could work in the NSP proposed integrated threat assessment centre. The team would track changes in

---

[33]   Department of Foreign Affairs, Space *Security 2003* (*Ottawa*: Eisenhower Institute, 2004), 2.

technology, threats of interest and propose the best solutions within Canada's means to counter these threats. As Canada's subject matter experts, they could conduct security evaluations on existing Canadian ground and communication segments, highlighting areas of deficiency and suggested ways to mitigate the problem.

The final section deals with standards and design guidelines. This section would be classified and available to approved companies who design and develop the components of space-based assets for Canada. For example, these guidelines could stipulate degrees of hardening and redundancy capabilities. A component of this section would be distributed to companies who sell services to Canada, i.e. information or services critical to maintaining national security. This section would be responsible for establishing the level of security required for each asset; hypothetically, if the information provided is crucial to Canada, the asset providing the information must have three back up systems per major segment and a redundancy capability built into the asset.

In summation, Canada's dependency on space-based assets and the existence of a credible threat demands that Canada develop a policy that will address these concerns. The proposed space security policy is reflective of Canada's position on the use of space and is within Canada's means to implement.   The creation of a team who are responsible to assess threats, develop countermeasures and evaluate assets will enhance Canada's national security levels by providing continuity to the security process.

Conclusion

On 11 September 2001, the world, as Canada knew it, changed. The events that

transpired were horrific but like the phoenix that rose from the ashes, Canada's National Security Policy grew from Ground Zero. The NSP identified three national security interests and addressed six key strategic areas. Examination of these key strategic areas revealed a heavy reliance on space-based assets yet neglected to address space security. Each space-based asset consists of four components, all of which are necessary for maintaining an operating capability. Currently, Canada has no in-house launch capability therefore; it cannot influence the launch vehicle or the space segment but it was determined that Canada could influence the ground and communication segments. An assessment of existing threats revealed that space-based assets are vulnerable to a wide variety of threats. Further analysis of these potential threats exposed means, capability and possible to intent to execute an attack; thus, necessitating the need for a space security policy. The proposed security policy addressed Canada's limitations but allowed for the possibility of growth and expansion in the future.

Canada's Chief of Defence Staff believes that Canada is a potential theatre of operations with a ball of snakes for threats. As Canada's dependency on space-based assets continues to grow so does it vulnerability to attack. Dependencies equate to weaknesses and weaknesses, if not addressed, eventually become a single point of failure; once discovered by your enemy, they can be exploited for their advantage. As a result, the need to secure, the assets that provides valuable day-to-day information for national security activities require immediate attention therefore; Canada must amend the National Security Policy to incorporate space security and develop a comprehensive space security policy, which will address the protection space-based assets and the preservation the space environment.

Bibliography

McCoubrey, D.J., DeLory, Steve, Fournier, Brad, Hanak, Dave. *Space Indoctrination Handbook.* Winnipeg: Canadian Forces School of Aerospace Studies, August 1996.

Terekhovv, Andrei. *AnnualReport-2001.* Report Prepared for the Standing Committee on the Status of International Agreements Relating to Activities in Outer Space. Paris: International Institute of Space Law, 2001.

Wilson, Ed. "Securing The Heavens: A Perspective On Space Control." Alabama: School of Advanced Airpower Studies, Air University Maxwell Air Force Base, 1999.

Canada. Department of Foreign Affairs and International Trade. *Canada's International Policy Statement: A Role of Pride and Influence in the World.* Ottawa: Her Majesty the Queen in the Right of Canada, 2005.

Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy.* Ottawa: National Library of Canada, 2004.

Canada. Department of Foreign Affairs. *Space Security 2003.* Ottawa: Eisenhower Institute, 2004.

United States. Department of Defense. *Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs.* (Washington, D.C.: U.S Government Printing Office, 2003.

Fraser, Graham. "Forget The Bear- Now It's Snakes." *Toronto Star,* 19 March 2005.

"Army Space Reference Text," http://www.fas.org/SPP/military/docops/army/ref_text/chap08.htm; Internet; accessed 23 April 2005.

"Canadian Space Agency," http://www.space.gc.ca/asc/eng/satellites/envisat/about_segment.asp; Internet:accessed 17 April 2005.

CTV. "Canada Says No to Missile Defence: Martin, 25 February 2005." http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1109264770244_1; Internet; accessed 18 March 2005.

Foreign Affairs Canada. "The Non-Weaponization of Outer Space." http://www.dfait-maeci.gc.ca/arms/outer3-en.asp#4; Internet; accessed 18 Mar 2005.

Foreign Affairs Canada. "Military Questions to Space Vulnerabilities." http://www.dfait-maeci.gc.ca/arms/mcdougall2-en.asp; Internet; accessed 18 March 2005.

Intelligence Collection. http://faculty.ncwc.edu/toconnor/427/427lect02.htm; Internet; accessed 16 March 2005.

Office of the Prime Minister. "Government of Canada Releases Comprehensive National Security Policy." http://pm.gc.ca/eng/news.asp?id=186; Internet; accessed 15 March 2005.

United Nations. "Outer Space." http://www.oosa.unvienna.org/spacelaw/treaties.html; Internet; accessed 14 March 2005.