IAC-15.D5.1.4.X28438

# SPACE SYSTEMS AS CRITICAL INFRASTRUCTURE: AN APPROACH TO DEMONSTRATE RELIABILITY, RESILIENCE, AND SECURITY

Patrick Gavigan

DRDC Ottawa Research Centre, Canada, patrick.gavigan@drdc-rddc.gc.ca

This paper explores the issue of space systems as Critical Infrastructure (CI) and explores methods for demonstrating their reliability, resilience, and security in order to ensure the availability of key services provided by space systems. A case study based on the Anik F2 anomaly in 2011 is analysed from this perspective. Current practices for testing, modelling and simulating space systems in Canada and highlights of deficiencies in these practices with a specific focus on ensuring resiliency of CI are discussed. A recommended shift toward industry led standardisation of functional testing for demonstrating the effectiveness of anomaly mitigation techniques is presented.

## 1 Introduction

This paper explores the concept of reliability, resiliency, and security of space systems using concepts related to Critical Infrastructure (CI). Canada does not currently specifically identify space systems as CI, however it is noted that space systems do have a highly important role to play in many CI sectors [1, 2]. Considerations of how space systems can be demonstrated to be reliable, resilient, and secure can use similar approaches to those used for CI sectors. Parallels exist between how Canadian space systems, and the Canadian space sector in general, are managed and to how CI sectors are managed. For example, in the case of the Anik F2 anomaly in 2011, the loss of service from this space system clearly demonstrated the *cascade* effect of failures resulting from *interdependency* on this specific system.

Section 2 provides context by exploring how space systems are managed in Canada followed by Section 3, which introduces the concept of CI. The case of the Anik F2 incident of October 6th, 2011 is discussed in Section 4. This example serves to illustrate that the concepts of CI can apply to the space sector in Canada, even though Canada has not specifically identified space systems as being within the realm of its CI sectors. An exploration of policy approaches, frameworks and guidelines of CI that can be applied to the space sector in an effort to reduce the risk and impact of future events similar to Anik F2 is provided in Section 5. Finally, a discussion of the proposed risk framework for space systems from the perspective of CI is presented in Section 6.

## 2 Space Systems in Canada

The term *space systems* can be used to describe a wide variety of technologies including small spacecraft components, ground control stations of space missions, human space flight vehicles, launch vehicles, satellites, and end user systems that depend on space segments to function, such as satellite based communication terminals. For the purposes of this paper, the focus is primarily on space systems that provide operational services or effects to the Canadian public. This paper does not focus on Research & Development (R&D), experimental or scientific systems, although the concepts can be applied to these systems as well.

Applications of space technology of interest for this paper include Intelligence, Surveillance, and Reconnaissance (ISR) (can also be referred to as Earth Observation (EO)); Positioning, Navigation, and Timing (PNT); Space Situational Awareness (SSA); and Satellite Communi-cation (SATCOM). In Canada, these systems are often owned and operated by the private sector. From the per-spective of the Government of Canada, space systems are regularly operated through some form of partnership or contractual arrangement with the private sector or inter-national partners. For example the SAPPHIRE spacecraft is operated by a private operator on behalf of the Govern-ment of Canada. From this perspective, the interest is on having the needed services available, and not necessarily interested in owning and operating these systems them-selves. Therefore, as the Government of Canada does not operate these spacecraft directly, the government's role of ensuring that the public interest is satisfied must work in the context of their relationship with the private sector operators of the space systems. [3]

## 3 Critical Infrastructure

To properly learn from the CI for ensuring reliability, sur-

vivability, and resilience in the space sector it is important to understand the meaning of the term *Critical Infrastructure*. According to Canada's authority on critical infrastructure protection, Public Safety Canada [4], "Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government". The definition further states that "Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence." This definition of CI is interesting as it highlights the interdependency of these systems, as well as the fact that these systems can have impacts that cross political borders. Space systems in Canada are generally systems that have impacts in this way. An example is the Global Positioning System (GPS) network operated by the United States Air Force (USAF) which has use and impacts on a global scale with users worldwide depending on this system, and taking it for granted, for daily activities.

Public Safety Canada's definition of CI highlights the concept of *interdependency*. Related to dependency, interdependency refers to a mutual dependency between two parties, or in this case infrastructure sectors. In effect, CI sectors are interdependent on each other. As a result of this interdependency, failures or disruptions can result in *cascading impacts*. These are failures that result from the impacts of other failures, highlighting the importance of the original system that has failed. *First order* impacts are direct results of the specific failure or anomaly that has occurred. *Secondary* or second order impacts are impacts, failures, or anomalies that result from first order impacts and not directly from the original anomaly or failure. Following from this logic, *tertiary impacts* are caused by secondary impacts. [5]

In the United States (US), the Department of Homeland Security (DHS) defines CI as "the assets, systems, and networks, whether physical or virtual, so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." [6] The European Union (EU) definition of CI includes "systems that if disrupted or destroyed would result in a serious impact to health, safety, security or economic well being." [1]

## 4 The Anik F2 Incident: A Case Study of Space System Anomalies Resulting in a Cascade Effect

The Anik F2 spacecraft is a C-band, Ka-band, and Ku-band communications satellite located in the $111.1^o$ WL orbital slot in Geostationary Orbit (GEO). The spacecraft is a communications satellite for North America and Hawaii for direct broadcast, mobile communications and broadband in remote communities. These services are marketed to remote communities as well as general consumer, industrial and government clients. This spacecraft, manufactured by Boeing, is operated by Telesat Canada and was brought into service in 2004. [7]

At 06:36 Eastern Daylight Time (EDT) on October 6, 2011 the Anik F2 spacecraft experienced an anomaly caused by a software update which resulted in the spacecraft being put into *safe mode*[1] and pointing toward the sun to charge its batteries. As a result, all services derived from the Anik F2 spacecraft were unavailable until the anomaly was corrected at approximately 22:00 EDT. Full services were restored by 07:00 EDT the following morning. [8, 9, 10]

### 4.1 Anomaly Impact

As a result of this anomaly, communications services in communities in the Northwest Territories, Nunavut, Yukon, and Northern Ontario were unavailable. This included long distance telephone, internet, mobile phone, and television. Although Nunavut has multiple voice and data service providers, the vast majority of communities rely exclusively on the use of the Anik F2 satellite for communication and data traffic in and out of the region. As a result, the Anik F2 space system was a single point of failure for the region's communication services. Due to these disruptions, emergency response plans were activated in the affected regions. Medical facilities and first responders, including the Royal Canadian Mounted Police (RCMP) shifted from nominal communications systems to dependance on Iridium satellite phones. Furthermore, airline traffic was halted during the outage as air traffic control and emergency responder communications were compromised. First Air, an airline serving northern Canadian destinations, was forced to cancel 48 flights to the affected region. The finance and business sectors were also severely affected as banking, automated teller and credit card systems were not functional. Most banks were closed and any retailers that were open were operating on a cash only system. Most purchasing was simply delayed until services were restored. [8, 11, 12, 9, 10]

In an effort to understand the impacts of the Anik F2 anomaly, the Government of Nunavut did a study of the effects of the outage [8]. As part of this study, they surveyed the territory's population with respect to how the

[1] *Safe mode* generally refers to an emergency or troubleshooting mode that is used in space operations for ensuring that a space system is not damaged in the event of the occurrence of an anomaly. Typically this involves running the space system with only the bare minimum of needed systems in an effort to preserve power and other limited resources.

 

service outages had affected them. Respondents to the survey reported internet access loss in their community at a rate of 86%. Long distance telephone services were reported unavailable by 87% of respondents. Payment processing was reported unavailable by 87% of respondents. 59% of respondents also reported issues with local cell phone access. These effects ultimately resulted in almost 90% of respondents claiming that they had reduced productivity as a result of the disruptions of services. Respondents also expressed that they experienced isolation and concern over their inability to communicate with family members and the lack of information available to them with respect to the status of the anomaly which made the situation more stressful. They also noted that if the outage had occurred on pay day or for prolonged periods, effects could be expected to be far worse; 90% of respondents said that a week long outage would be seen as an emergency. Of particular concern was the impact on air travel, resulting implications for emergency medical travel and the availability of food and other supplies in the community. The Government of Nunavut finally identified that there were few options for restoring services in the event that the outage lasted longer. They anticipated that they would have had to point ground station antennas to alternative spacecraft with the help of technical personnel from outside of the region, a complicated endeavour when air travel is not available. Finally, respondents highlighted that they felt that it is a government responsibility to ensure that failures of services, such as the Anik F2 anomaly, do not occur again. [8]

### 4.2 Cascade Analysis

In considering the effects of the Anik F2 incident, it is interesting to analyse this event from the perspective of the definitions of the CI presented at Section 3. In considering the effects of the spacecraft anomaly, there was clear dependency of multiple sectors on this particular space system. As shown in Figure 1, the primary impact of this anomaly was the loss of communication systems to the affected regions, however there are clear secondary and tertiary impacts. Due to the loss of communications, finance, transportation, emergency management, public, and business sectors were adversely effected through secondary and tertiary impacts. There is also evidence of interdependency, as the Government of Nunavut highlighted in their report, that extended service disruptions would have been difficult to resolve without easy access to technical support within the region. Without readily available transportation and compromised telecommunications, bringing the necessary assistance to bear would have been difficult. Public concern over communication access as well as the continuity of the supply of essential supplies, such as food and medical supplies, and medical evacuation support clearly demonstrates the importance of this system to Northern Canada. [8]

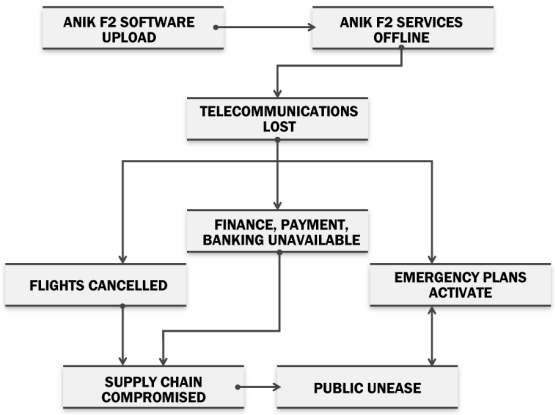


Figure 1: Anik F2 Impact Cascade.

It is noteworthy that this type of event is not unprecedented. In 1994 both Anik E1 and Anik E2 suffered similar anomalies within nine hours of each other. With missions similar to Anik F2, these anomalies caused significant disruptions communications disruptions. In this case, the cause was determined to likely be related to space weather phenomena. [13]

## 5 Critical Infrastructure Plans and Policies

In this section government plans and policies related to the management and protection of CI are discussed. Following this discussion, the current status of space systems from the perspective of CI is outlined.

### 5.1 Approaches to Managing Critical Infrastructure in Canada and the United States

In Canada, policies and plans for managing national critical infrastructure are the responsibility of Public Safety Canada [14, 15, 16]. In the US, this responsibility is given to the DHS [17, 18]. Canadian CI sectors include: health, food, finance, water, information and communication technology, safety, energy and utilities, manufacturing, government, and transportation [4, 5]. Many of these areas have major public sector involvement and responsibility, as operators of this infrastructure or as the primary service provider. In considering the level of risk associated with the operation of various infrastructure sectors, private sector operators take a variety of actions to ensure the reliability and resiliency of their systems. They must do so in the context of their need to remain profitable companies. Companies have financial incentives to address threats and risks that reside within their sphere of

influence and/or control but have limited means to address issues that are outside of this region, thus this falls to the public sector. Examining the interdependencies between multiple sectors, especially in the case of threats that are not within the control of private sector system owners or operators, falls to the public sector. [5]

Both Canada and the US identify similar approaches to identify and manage risks to CI sectors. Public Safety Canada states that its objectives are to "build partnerships, implement all-hazards risk approaches, advance timely sharing and protection of information among partners" [16, 15]. This approach points to the importance of public and private sector partnerships to ensure that systems are as resilient as possible, as market forces alone are not sufficient to push companies. Through these partnerships, an all-hazards approach to risk assessment and management is used where the public sector acts as an enabler for the resiliency of CI, especially in cases where the private sector manages the CI capabilities. [16, 15, 18]

From a more practical perspective, Public Safety Canada outlines several aspects to risk management for the CI sectors. Central to the approach is the establishment of *sector networks* involving public and private sector participation. This enables multiple perspectives to be included when performing risk assessment, planning of risk mitigation activities, exercises, etc. Information sharing is key to the success of the sector network approach. [14]

More specifically, within a sector network, a sector operations document containing details about the "critical services and products", "interdependencies", "sector supply chain and supporting operations" related to the continuity of operations of that sector. This document requires a highly detailed description of the risk tolerance that is acceptable for that sector. To do this, it must include a sector risk profile, analysis to evaluate the highlighted risks, and risk mitigation plans. Objectives, actions, implementation, and validation measures must be included in this plan. Key are means to demonstrate the resilience of the sector through exercises plan. This approach is used to demonstrate that the goals and objectives for risk mitigation are achieved. These exercises can be tabletop, functional, and full operational exercises. Lessons learned from these exercises can complement experience from real world incidents and lessons learned and feedback into ongoing improvement for managing risks for the CI sector. [14]

### 5.2 Space as Critical Infrastructure

Although Canada does not specifically identify space systems as being CI, the US and EU have made statements that indicate a trend in this area. For example, the US has acknowledged that space systems are interdependent with many CI sectors. The 2003 strategy for CI security developed by the DHS for the US however only refers to space in the context of the telecommunications sector. Currently, the US PNT advisory board is pushing for GPS to be considered as CI by the DHS. The belief is that this designation would enable a stronger response to threats to the GPS system. PNT is acknowledged to be a critical enabler to almost all of the DHS identified CI. [1, 2]

## 6 Proposed Risk Framework for the Canadian Space Sector

Risk frameworks can formalize how organizations protect value. They are central to organizational or sector activities and processes as well as how decisions and plans are made. Well formulated risk frameworks address uncertainty and unknown parameters directly. A detailed knowledge of the area and context, both *internal* and *external* is required in setting up effective risk management. This cannot be done in isolation and must involve external stakeholders. ISO 31000:2009, for example, identifies means for establishing risk management processes, defining risk criteria, risk assessment, risk identification, risk analysis, risk evaluation, treatment, monitoring and review. [19]

Current industry norms for space system testing are tied to historical approaches for mitigating risks to space missions and lessons learned from historical failures, anomalies and incidents. The various companies in the space sector, each with their own proprietary designs and philosophies, approach this in their own way. In general, space system developers focus on risk factors associated with the space environment as well as functional testing of their specific designs. These companies, although they are generally focused on accomplishing the same goals, approach them from their own perspectives and experiences. This approach does not necessarily include risks associated with emergent sources of anomalies to space systems or necessarily address means of mitigating these risks [20, 21, 22]. Risk management from the perspective of continuity of operations is important but within constraints of financial viability of the project. In addition, knowledge about the sources of anomalies to space systems, lessons learned, data models, etc. are typically tied to individual companies proprietary information and reluctantly shared. In terms of financial risk mitigation, insurance rates for space systems that have had anomalies have been seen to increase by a factor of two [23].

The current paradigm for individual companies, with their own risk mitigation approaches, contrasts with the approach taken in CI sectors, where sector networks are encouraged to share risk information, experiences, and perspectives in order to achieve a more resilient sector is key to risk management. As such, applying the sec-

tor network approach used in CI to the space sector could help improve the status quo. Collaborative approaches to risk management can help to improve risk modelling issues as well as provide a forum for the sharing of perspectives on risks, mitigation strategies applicable to the sector, trials, experiments, etc. Other key issues for a space sector network to address include risk profiling, planning, modelling, simulation, trials, and experiments. These are all aspects of the *sector operations document* outlined in section 5. Modelling and simulation to support such an endeavour can be a complex and difficult task. For example, models can be weakened due to a lack of available data with respect to a risk source, or by contrast an overabundance of extremely complex data. Model sharing can also lead to issues where subtle parameters are different but these differences are not recognised. Uncertainties, and the meaning of results can be misunderstood as well. Understanding modelling results requires an in depth understanding of the model, processes being modelled, and modelling techniques. Isolation between organisations can compound these issues. As such, the sector network requires standardization of approaches in order to address these types of problems. [24]

As highlighted by some of the complexities to modelling mentioned above, simply joining a sector network alone cannot solve all the issues highlighted above. Standardizing approaches, sharing of risk profile information, partnerships between private and public sectors requires coordination. Standardization to ensure interpretability of modelling, simulation, and testing techniques can assist in this environment [25]. In an effort to investigate the scope of this risk modelling issue, the author is currently performing consultations with Canadian academia and industry with respect to how standardisation in the realm of space mission risks can be addressed. An architecture for consideration, called the *sandbox* and presented in Figure 2, could provide a mechanism for space systems to be tested in the context of various anomaly models, potentially provided from various sources. Using such an approach, details of the anomalies or proprietary components of the space system do not need to be shared in order to perform risk assessment trials.

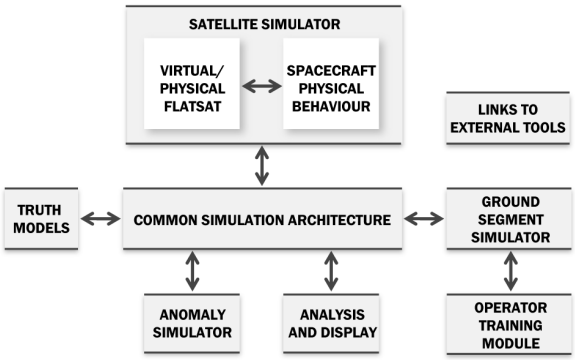


Figure 2: Proposed Sandbox.

## 7 Conclusion

Although Canada does not currently identify space systems as critical infrastructure, this paper has highlighted the interdependency of space systems within Canada and its CI sector as well as means for using the approaches used for ensuring the reliability and resilience of CI on space system services. This was emphasised in the example of the Anik F2 spacecraft incident in 2011, where a software update to the spacecraft resulted in a complete loss of services from the spacecraft. The loss of service resulted in a cascade effect with impacts on the telecommunications, transportation, emergency management, and other sectors in Canada's northern communities. Based on the clear parallel between how Canadian space systems in the context of CI sectors, where the private sector has a key role in managing systems of public importance.

This paper has recommended adapting approaches from the CI sectors to the space sector in an effort to reduce the risk of major space system anomalies or failures in Canada in the future. Included in this paper is the proposal of a sector network with public and private participation for the sharing of information regarding risk profiles, mitigation measures and plans, as well as performing trials to demonstrate the resiliency of the sector to these risks. A proposed method of sharing risk scenarios in a common simulation architecture, called the *sandbox* is currently being investigated. This will also require industry led standardisation in the area of modelling and simulation in order for the sharing of models to be viable and useful.

## References

[1] M. Hesse and M. Hornung, ``Space as critical infrastructure," in *Handbook of Space Security* (K.-U. Schrogl, P. L. Hays, J. Robinson, D. Moura, and C. Giannopapa, eds.), vol. 1, ch. 10, pp. 157--201, New York: Springer Science+Business Media, 2015.

[2] D. A. Divis, ``PNT advisory board debates critical infrastructure designation for GPS." `http://www.insidegnss.com/node/4536`, June 2015. Accessed: 2015-08-10.

[3] P. Gavigan, ``Operational use of small satellites for the canadian armed forces," in *65th International Astronautical Congress*, no. IAC-14.B4.4.7, (Toronto Ontario Canada), IAF, September 2014.

[4] Public Safety Canada, ``Critical infrastructure." http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx, Mar. 2014. Accessed: 2015-07-19.

[5] T. Macaulay, *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742: CRC Press Taylor & Francis Group, 2009.

[6] United States Department of Homeland Security, ``What is critical infrastructure?." http://www.dhs.gov/what-critical-infrastructure, Oct. 2013. Accessed: 2015-08-11.

[7] Telesat, ``Anik F2." https://www.telesat.com/sites/default/files/satellite/anikf2_letter.pdf, 2004. Accessed: 2015-07-25.

[8] Nunavut Broadband Development Corporation, ``Nunavut's october 6 disconnection: The impact of the Anik F2 satellite failure on Nunavut," tech. rep., Nunavut Broadband Development Corporation.

[9] J. Murray, ``Anik F2 satellite anomaly causing service disruptions." http://www.netnewsledger.com/2011/10/06/anik-f2-satellite-anomaly-causing-service-disruptions/, Oct. 2011. Accessed: 2015-07-25.

[10] R. Marowits, ``Telesat says a software error triggered Anik F2 satellite to shut down." http://www.huffingtonpost.ca/2011/10/07/telesat-says-a-software-e_n_999899.html, Oct. 2011. Accessed: 2015-07-25.

[11] T. Malik, ``Canadian satellite malfunction leaves thousands without communications." http://www.space.com/13213-canadian-communications-satellite-malfunctions-anik-f2.html, Oct. 2011. Accessed: 2015-07-25.

[12] CBC NEWS, ``Satellite problems ground nunavut flights." http://www.cbc.ca/news/canada/north/satellite-problems-ground-nunavut-flights-1.1018771, Oct. 2011. Accessed: 2015-07-25.

[13] H.-L. Lam, D. H. Boteler, B. Burlton, and J. Evans, ``Anik-E1 and E2 satellite failures of january 1994 revisited," *Space Weather*, vol. 10, no. 10, pp. n/a--n/a, 2012. S10003.

[14] Public Safety Canada, ``Risk management guide for critical infrastructure sectors," tech. rep., Public Safety Canada, July 2010.

[15] Public Safety Canada, ``Action plan for critical infrastructure 2014-2017," PS4-66/2014E-PDF ISBN: 978-1-100-23291-1, Public Safety Canada, 2014.

[16] Public Safety Canada, ``National strategy for critical infrastructure," PS4-65/2009E-PDF ISBN: 978-1-100-11248-0, Public Safety Canada, 2014.

[17] United States Department of Homeland Security, ``Critical infrastructure." http://www.dhs.gov/critical-infrastructure, Aug. 2015. Accessed: 2015-08-10.

[18] National Infrastructure Advisory Council, ``Critical infrastructure resilience final report and recommendations," tech. rep., United States Department of Homeland Security, 2009.

[19] Canadian Standards Association, ``Risk management - principles and guidelines," Standard CAN/CSA-ISO 31000-10, Canadian Standards Association, 2015.

[20] M. Zenko, ``Dangerous Space Incidents." http://www.cfr.org/space/dangerous-space-incidents/p32790, 2014. Accessed: 2014-11-17.

[21] B. Garino and J. Gibson, ``Space System Threats," in *AU-18 Space Primer* (Air Command and Staff College Space Research Electives Seminars, ed.), ch. 21, pp. 273 -- 281, 131 West Shumacher Avenue, Maxwell AFB AL 36112-5962: Air University Press, September 2009.

[22] W. Gavins and J. Hemenway, ``Cybersecurity: A joint terminal engineering office perspective," in *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, pp. 918--923, Oct 2010.

[23] A. Ellery, *An Introduction to Space Robotics*, ch. 20.3.2, pp. 594--596. Springer Praxis Books / Astronomy and Planetary Sciences, Springer, 2000.

[24] S. Barr and R. Kohli, ``Understanding the limitations of models and analyses," in *Proc. of '3rd IAASS Conference – Building a Safer Space Together'*, (Rome Italy), ESA, October 2008.

[25] E. Özalp, ``Integrated standarization for space industry for future cooperations," in *Proc. of '3rd IAASS Conference – Building a Safer Space Together'*, (Rome Italy), ESA, October 2008.

 

## A Biography

Patrick Gavigan is a Defence Scientist for Defence Research and Development Canada. He has a bachelor's degree in computer systems engineering from Carleton University and a master's degree in aerospace engineering from the University of Toronto. He is also a graduate of the Space Studies Program of the International Space University.

## B Acknowledgements

The author gratefully acknowledge the support Robin Nagy and Katherine Baskey in the DRDC library as well as to Dana Rakus for assistance with the graphics. In addition, the author is grateful to Catherine Marchetti, Lauchie Scott, Anne Young and Brad Wallace for their support in reviewing and helping to refining the scope of this work paper as well as to John Weaver for the opportunity to present this work at IAC 2015.

## Acronyms

**CI** Critical Infrastructure.

**DHS** Department of Homeland Security.

**DRDC** Defence Research and Development Canada.

**EDT** Eastern Daylight Time.

**EO** Earth Observation.

**EU** European Union.

**GEO** Geostationary Orbit.

**GPS** Global Positionning System.

**ISR** Intelligence, Surveillance, and Reconnaissance.

**PNT** Positioning, Navigation, and Timing.

**R&D** Research & Development.

**RCMP** Royal Canadian Mounted Police.

**SATCOM** Satellite Communication.

**SSA** Space Situational Awareness.

**US** United States.

**USAF** United States Air Force.