A Perspective on Cyber in Space for National Security

Robert MAZZOLIN
RHEA Group
r.mazzolin@rheagroup.com

Abstract: Space systems have become a new enabler for nations to pursue national interests. They have become integrated in advanced socio-economic systems pertaining to data gathering, supply and production chains, communications, and are part of the backbone for many critical infrastructure systems. At the same time, they are an increasingly important part of military capabilities and of security processes. With this importance, comes an awareness of their vulnerabilities. This article argues that cybersecurity has become paramount to space operations and to national security and delineates some of the intricacies of cooperation and confrontation in cyber for space. In addition to individual nation research and mitigation measures, cooperation between spacefaring nations and between all relevant stakeholders will be required to enhance security.
Keywords: Space systems, Satellites, Cybersecurity, Resilience, National security

INTRODUCTION

National security is not restricted to securing the land, air and maritime boundaries and pursuing strategic interests but encompasses all aspects that have a bearing on the nation's well-being. Outer space and cyber space have emerged as the new enablers for nations, enhancing the speed and efficiency of national security and socio-economic efforts and also in providing novel applications in these areas.

In an information dominated world, they are instrumental in providing the competitive edge among the global community, strategic and tactical superiority in conflict situations, and projection of national power and influence. In addition to capability enhancement towards national aspirations, investments are also necessary for securing these capabilities against deliberate or unintentional intrusions or attacks and in ensuring safe and sustainable operations. Secure access to cyberspace is foundational to national security (Livingstone & Lewis, 2016).

Strong, modern, industrial nations are defined by prosperous economies and credible defence. The ability to assert and protect sovereign interests in cyberspace is key to achieving these objectives. Business executives, as senior defense and security leaders, depend on cyberspace for precisely the same things – to gain, move and use information to enable better and faster decision making than the competition (Williams, 2014). The data and information rich environment of the modern battlespace presents a key area of both strategic opportunity, but equally, vulnerability. Both cyber and space technologies, in particular, are the new battleground for competing great powers who seek to limit opponents' access to information, analytics and complex surveillance and reconnaissance information with which to inform decision making (Newcomb, 2016).

CYBER CONNECTION TO SPACE

With growing participation, commercialisation has become an integral part of space operations and is receiving active governmental support. The peaceful use of space and the military significance of outer space continues to increase with some 60 countries currently utilizing it for peaceful purposes, for communications, banking, monitoring environmental and climate change, disaster management, E-health, E-learning and communications, surveillance and guidance systems for military purposes (Weinzierl, 2018). As it regards vulnerabilities, while space operations have always been vulnerable to natural forms of interference, progressive developments in the domain have also resulted in the emergence of unique novel challenges to space security and the sustainability of the environment. The 2011 National Space Security Strategy of the US states that "space capabilities provide the United States and our allies unprecedented advantages in national decision-making, military operations, and homeland security" (NSSS, 2011). As opposed to first Golden Age of Space, with two superpowers having "symmetric capabilities and interests", the current landscape of space as a domain is made up of "disparate players with vastly different asymmetric capabilities and interests" (Cooper and Roberts, 2018).

Greater participation in the domain and commercial prospects has more players vying for prime orbital slots, the radio frequency spectrum, and a larger share of the market. Overcrowding and increasing space debris is adversely affecting the survivability of satellites. The environment is therefore becoming more contested, congested and competitive with the consequent increase in potential for disruption of operations (NSSS, 2011). Space is being used extensively by advanced space-faring nations for supporting military operations and most new entrants would also leverage their access for these purposes (Pomerleau, 2016). A corollary to this is that all assets in space providing a strategic or military advantage can be designated as valid targets in case of hostilities (DHS, 2020).

Consequently, advanced nations are making efforts to dominate and control the environment to protect their interests and assured access to the realm and the less capable ones would do the same to gain an asymmetric advantage through degradation and destruction of systems. Both these strategies demand development of counter-space capabilities that would include offensive activities, as well as those aimed at system negation (Pomerleau, 2016). Such capabilities in the hands of rogue nations or non-state actors, who have limited interests in the domain, could be extremely dangerous. In recent years, national security challenges have necessitated a tacit acceptance of the use of the domain for meeting national security objectives.

THREATS TO SPACE SYSTEMS

Cyber space is a man-made domain consisting of the interconnected networks of computing and communication devices and the information contained on these networks (Williams, 2014). Satellites, along with any other space-based capabilities, represent digital critical infrastructure, and are therefore vulnerable to cyberattack. When considering our daily lives, there is not an operation or activity conducted anywhere at any level that is not somehow dependent on space and cyberspace. This interdependency could be used to attack space assets from cyberspace. From a cyberspace perspective, it is irrelevant how high above the ground a computer is positioned.

Cyber vulnerabilities associated with space related assets therefore present serious risks for critical terrestrial infrastructure, and the lack of security in the space-based environment will compromise economic activity and thereby pose risk to society. Advancements in the cyber domain have not required a protracted thrust by governments towards its development as the transformational nature of the technology, its commercial potential and cheaper access has caused a self-sustaining expansion of capabilities and capacities (Livingstone & Lewis, 2016).

Societies' increasing dependence on networks, however, has resulted in a surge in the number and sophistication of cyber-attacks that exploit the hardware or software vulnerabilities in the networks with diverse motivations and consequences. Cyber intrusions could target government agencies and departments, private corporations or individuals, with diverse impacts on national security. These could be undertaken for espionage, to commit cybercrime or for denying or disrupting critical national infrastructure systems like power grids, telecommunications networks, transportation systems, water services or financial and banking operations (Gheorghe & Schläpfer, 2006).

They could be used for social engineering - spreading disinformation and moulding public opinion with the intention to destabilise the internal security environment of the country as is currently being seen as part of the current western electoral dialogue, and supporting evolving hybrid warfare techniques that see aggressive state based actors conduct provocative activities that fall slightly below the threshold to provoke political sanctions or military response (Robinson et al, 2019).

As network centricity becomes integral to military operations, military equipment and operations could be attacked to gain strategic or tactical advantage. These attacks could even be used to cause kinetic effects, acts of sabotage or to hamper national response mechanisms, all of which would endanger lives, thereby impacting the credibility of governments and the underlying societal security frameworks. More widespread and systematic attacks could escalate tensions among states. The perpetrators of these attacks currently range from an individual to hacking syndicates that work independently or are covertly supported by governments and corporations. States as well as non-state actors could seek an asymmetric advantage by employing such attacks to undermine an adversary's security and stability.

With greater technological capability, the nature and scale of cyber-attacks has continued to evolve. They are now more targeted and decisive, with clear political, economic or military motivations and intentions. The traditional lines that would have earlier helped distinguish between the types of attacks and the motivation of their perpetrators has blurred. While the state actor could resort to an attack to undermine security or stability, a similar attack could now be undertaken by non-state actors for extortion or for obtaining information that could be sold to third parties.

Networks continue to expand and become more complex and their interdependencies continue to grow, further enhancing the vulnerabilities and increasing the difficulty in providing comprehensive protection. The environment is highly dynamic, and preventive and defensive counter-measures and reactive strategies, even with continuous efforts, are finding it difficult to keep pace with the rapidly evolving threats.

Cyber situational awareness; the ability to monitor the domain, identify the vulnerabilities and detect intrusions are still not sufficiently developed. Attempts at enhancement are hampered by concerns for privacy, freedom of speech, and the free flow of information. Even as detection rates have gone up through concerted efforts, cyber forensics need to be developed for attribution, as the attacker can easily hide his tracks in this intricate, borderless domain. International legal regimes have failed to keep pace with the rapid technological advancements in this discipline. Advanced nations, whose critical dependence on space and cyber space exposes them to asymmetric risks of disruption, are responding to these limitations by developing effective deterrence against misadventures, including offensive counter-attack capabilities (Pomerleau, 2016).

Growing economies are investing heavily in computer networks and communication facilities to meet their aspirations, and have received a further boost with the smart phone revolution, increasing the density and diversity of appliances used for access to the internet. The diversity of machines makes it difficult to put in place comprehensive protection measures. Computers and networks rely mostly on foreign software and hardware, exposing them to risks associated with the global information technology supply chain. Most of the data generated in any country is exported and stored in foreign data banks. Digital and Smart City Initiatives and the increasing involvement of the private sector in nation-building endeavours are progressive steps that are also increasing the scope and complexities of cyber security efforts, and are further complicated by the Internet of Things (IoT). All of these make securing the domain an arduous task.

Clearly, it can be seen that most earth based activities are touched in some manner by space when one considers the wide array of applications associated with satellite communications, precision navigation and timing, and earth and space observation (Georgescu et al, 2019). Cyber-attacks against satellites include spoofing, jamming, penetration of communication networks; the targeting of control systems and mission payloads as well as terrestrial infrastructure including satellite control centers (Pomerleau, 2016).

The potential attacks include (Harrison et al, 2019), more specifically, space based cyber threats include tracking and monitoring satellites and their transmissions, electronic attack against services at the transmission site, the satellite, the communication link and user equipment. A key approach is to attack the ground segment that provides the telemetry, tracking and command of the space nodes and launch mission functions, and includes the satellite transmission and reception capabilities including GPS receivers. Radio Frequency energy attack against uplink and downlink signals to jam or spoof information flow through the space based asset can be achieved via Uplink Jamming to disrupt command and payload links; which has a broad based effect as all recipients of the target transmission are affected, and downlink jamming, primarily oriented at preventing selected users from receiving Satcom broadcasts and navigation signals. Smart jamming, as opposed to brute force jamming, emulates the satellite signal and provides targeted users with false data or information.

Additional space segment threats include the use of kinetic and directed energy replicating nuclear effects, however, these techniques are more esoteric. Satellite communications include special protocols used onboard and between satellites, ground stations and control

centers, both analog and digital and are increasingly moving towards the use of IP networks (Davenport & Ganske, 2019).

Emerging protocols convert serial transmissions to IP packets between satellite modems and the larger computing network. In doing so, one key security issue is that some gateways are not supported by authentication methods. Certain legacy military protocols such as the 25 year old ADCCP and 50 year old EXU protocols for Satellite, Data Center, and Relay Station Security are still in use, which again are cause for care (Bucovetchi et al, 2019).

As hackers typically target the weakest point, individual vendors could provide egress to a larger corporation's network. Satellites are also a vulnerability because security has historically not been given sufficient attention in this context. If a satellite could be disabled, the effects might be as widespread as a major internet outage (Falco, 2018).

This would be particularly devastating for many small countries that have recently launched their own satellites as they do not have a backup. Interconnected Satcom networks have particular vulnerabilities at the point where they cross IP networks. Progressive solutions work at the network and transport layer of the OSI model as the traditional approach of using firewalls and network segmentation is no longer viable, therefore trusted rules-based appliance and proxy server guards are now required. One crucial aspect of the satellite business is that it is very much international, which both enhances security while also posing unique risks. Every country, even the smallest, is assigned orbital space for satellites, just as they are assigned blocks of IP addresses. Of course, not all countries have satellites, so they sell or rent their space. This means that risks could already result from the simple fact of having potentially antagonistic political actors 'under the same roof".

At the same time, we must not discount the effect that economics have on security. The number of satellites is steadily increasing not only through lower launch costs, but also through the use of standardized system architectures and the increasing use of cubesats and smallsats which are in the financial range of smaller nations, universities and companies. According to Bryce (2019), of the 1.800 satellites launched between 2012 and 2018, 1,300 were smallsats (according to Bryce up to 600-1000 kg, depending on source of definition), of which 961 were cubesats, which are smaller still.

There have been discussions regarding the impact this trend has on the space debris threat, but this trend could only have resulted from the use of off-the-shelf hardware and software for cost advantages in development and production. Satellites using bespoke systems would have been far more expensive. But, according to Falco (2019), because of this trend, satellites are gaining the same exposure to cyber threats like commoditized malware that other systems which are part of the IoT and commercial-off-the-shelf trend are experiencing. They are losing the capacity for "security by obscurity" and are increasingly using components whose security features are never upgraded.

As space systems are part of critical space infrastructures involving other space assets, ground stations, communication links and other elements (Georgescu et al, 2019), the vulnerabilities being built into a large portion of newly launched satellites become systemic entry points for aggressors of all types.

MITIGATION

To address some of these challenges, some solutions include the use of traditional security monitoring tools or Security Information and Event Management uniquely designed for satellites. A useful endeavor for any satcom provider is the conduct of cyber security assessments. Eventually, any cybersecurity regulations will extend into space, so providers will need to write audit plans and move toward compliance. Further support through the life cycle management of any space system needs to be supported by detailed modelling and simulation of the infrastructure in association with concurrent design methodologies that integrate security into the fabric of system design, development, production and operations (Air Force, 2019).

Further potential operational management approaches such as "Moving Target," currently the subject of research, requires defenders to develop and deploy diverse strategies and capabilities that continuously change over periods of time to create complexity and impose cost to threat agents, thereby minimizing vulnerability exposure and associated opportunities for attack in order to increase system resiliency (DHS, 2020). Additionally, Quantum satellites are in the initial phases of implementation as they are seen to be virtually tamper-proof based on the related physics.

Space is evolving from the domain of select wealthy states and highly resourced academia, to one where market forces dictate the terms and conditions. The current, rapidly evolving technology base affords capabilities in space to states, international corporations, entities and individuals that, even a few years ago, had no realistic possibilities in this vein; and capabilities that only a few years ago were solely within the domain of government security agencies are now commercially available.

Space and cyber, both technologically intensive domains, need to be harnessed optimally for national security. Formulation and articulation of an all-encompassing national security policy would help define domain specific strategies and roadmaps. There is a global trend towards increased instability in these domains as nations develop offensive capabilities. Consequently, space has been labelled as the fifth, and cyber, the fourth, domains of warfare at NATO level.

The current international legal regime is ill equipped to prevent the weaponization of these environments. Meanwhile, the mutual distrust among nations and the unpredictability of non-state actors are thwarting efforts in this direction. In the future, defensive counter-measures might prove to be inadequate to contain the threat. Nations need to evaluate development and deployment of offensive capabilities along with their supporting structures as part of the deterrence strategy. International collaboration with nations with congruent interests should be enhanced for capability and technology development, sustenance of operations and enhancing collective security capabilities. At the same time, nations should maintain activity in important global forums highlighting the global implications of destabilising incidents in the space and cyber domains to continue efforts toward promoting safety, stability, and security.

There is an urgent requirement for an adaptive, multilateral space and cybersecurity regime. Although international cooperation will be critical, highly regulated government or institutional actions will in all likelihood be too slow to permit the establishment of appropriate responses to space based cyber threats. Alternatively, moderate regulatory approaches through industry led standards, based on risk assessment, collaboration, the exchange of knowledge and information and innovation, will result in greater agility and effective responses to threats.

An international community of willing and capable partners presents the most effective avenue to

developing a space-based cybersecurity regime able to address the rapidly evolving and increasing nature of threats. An international space and cybersecurity regime made up of select, capable states and critical stakeholders, i.e. space industry supply chain and insurance community, could be solicited to develop relationships between key actors within the space and cyber communities, in order to create a mechanism to deliver practical leadership to enhance security within the global space sector.

Klein (2016) notes that "deterrence, dissuasion, and the Law of Armed Conflict have applicability when considering space strategy, just as in other media of warfare". All of these require cooperation through diplomacy – cyber, military, science -, also in order create and embed norms against aggressive behavior on the part of actors contesting the international order. These norms also involve a harmonization of views on hostile intent, hostile act, and also on what constitutes armed attack in the space domain. Over time, concepts such as extended deterrence and the Third Offset (Massie, 2016) may become relevant and they depend on the full use of all instruments of state to establish deterrence, including partnerships, formal and informal, based on interoperability and using and generating trust.

TECHNOLOGY RESEARCH AREAS

As it regards potential research areas, given the congested nature of the electromagnetic spectrum, potential signals intelligence risks and associated bandwidth limitations with reliance on such capabilities, increasing emphasis on the development of quantum key distribution capabilities, further potential areas of research would be in the area of optical communications or means that do not involve the electromagnetic spectrum.

Additionally, as we have highlighted, it is clearly acknowledged that space is becoming increasingly contested. and no longer the safe preserve as in the past. Within this contested space, contemporary actors should be interested in resiliency, and platform based defence. Such capabilities could include self-healing satellites, capabilities that would enable satellites to recognize activities from a software or command and control perspective, and shed nonfunctioning portions, reroute capabilities within space platforms in anticipation of human intervention so that the spacecraft may continually stay functional. To that end, a greater emphasis is required on cyberspace when one considers how military forces approach this domain.

Cyber includes the entire continuum between network operations to offensive cyber operations to enable war fighters to both project or influence offensively as well as protect defensively (NSSS, 2011). Some examples of useful advanced technology tools include autonomous and goal seeking network capabilities that can gain access to, and exploit communication networks. Further potential capabilities focus on human-machine interfaces and performance augmentation; biometric security; and low-powered data protection that is flexible, scalable and reliable to enable cross-domain operation.

Increasingly, capabilities transcend or become composite capabilities between space and cyber. As cyber is a critical element of contemporary military operations, one key area includes cognitive electronic warfare capabilities that further raise the potential to bring artificial intelligence and big data analytics into this realm. A further step in this AI/data analytics vein is to fuse the copious information coming from many sources for decision making in support of system management and network defence to ensure mission integrity (Air Force, 2019).

Improved human-machine interfaces and capabilities to translate the massive quantities of data collected into actionable intelligence potentially serves as a game-changing technology area to be pursued. This will become a key element of emerging battle management capabilities as improvements are made to Space Operations Centres and Joint Interagency Combined Space Operations Centres, given the large amounts of data ingested and processed. The greater provision of autonomy afforded to operators to enable them to rapidly and efficiently respond to any situation would be important. For example, tools that are capable to differentiate between human driven events, intrusions or attacks against space capabilities and natural occurrences. In the case of cyber, systems that would be able to tell if a natural or human initiated threat is occurring; or if it is a space or weather driven event. Such a capability, especially in legacy systems currently in orbit, to be able to understand if a command intrusion into a ground system or spacecraft is occurring and the ability to protect against that by uploading new code or software would enhance operational staffs' ability to best posture space-based capabilities to greater operational effect Air Force, 2019).

CONCLUSION

In summation, the threat manifests itself in a variety of forms on a daily basis. Lacking a coherent way forward, the collective accumulation of the variety of impacts from the myriad of cyber-attacks across the breadth of critical systems could serve to drain Western innovation, economy and commerce without reaching the threshold of triggering meaningful government, military and commercial engagement and response. There has never been a more important time or imperative for us to act upon this issue given the increasing potential existential threats posed to our societies and make this a more central element of our public agenda. The potential now exists for a revolution to drive space-based security through technological development, security policy, cooperation between states, international organisations and other stakeholders such as companies.

REFERENCE LIST

Air Force Space Command (2019) The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop. 5 September, 2019, http://www.spaceref.com/news/viewsr.html?pid=52822

Bucovețchi, O., Georgescu, A., Badea, D., Stanciu, R.D. (2019) Agent-Based Modeling (ABM): Support for Emphasizing the Air Transport Infrastructure Dependence of Space Systems, in Sustainability; Vol. 11(19):5331

Cooper, Z., Roberts, T. (2018) Deterrence in the last sanctuary. War on the Rocks, 2 January 2018, https://warontherocks.com/2018/01/deterrence-last-sanctuary/

Davenport, B., Ganske, R. (2019) "Recalculating route": A realistic risk assessment for GPS. War on the Rocks, 11 March 2019, https://warontherocks.com/2019/03/recalculating-route-a-realistic-risk-assessment-for-gps/

Department of Defense (2011) National Security Space Strategy. As NSSS (2011). https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy

Department of Homeland Security (2020) Definition for Moving Target Defence. As DHS(2020). https://www.dhs.gov/science-and-technology/csd-mtd

Falco, G. (2018) Job One for Space Force: Space Asset Cybersecurity. Cyber Security Project, Belfer Center, Harvard University, July 12, 2018, https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity

Georgescu, A., Gheorghe, A., Piso, M.-I., Katina, P.F. (2019), "Critical Space Infrastructures: Risk, Resilience and Complexity", Topics in Safety, Risk, Reliability and Quality, Series 36, eBook ISBN 978-3-030-12604-9, DOI 10.1007/978-3-030-12604-9, Springer International Publishing

Gheorghe, A., Schläpfer, M. (2006) Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical

Infrastructures, Systems Man and Cybernetics 2006. SMC '06. IEEE International Conference, vol. 1, p. 580-584

Harrison, T., Johnson, K., Roberts, T. (2019) Space Threat Assessment 2019, Center for Strategic and International Studies, 4 April 2019, https://www.csis.org/analysis/space-threat-assessment-2019

Klein, J. (2016) Space warfare: deterrence, dissuasion and the Law of Armed Conflict. War on the Rocks, 30 August 2016, https://warontherocks.com/2016/08/space-warfare-deterrence-dissuasion-and-the-law-of-armed-conflict/

Livingstone, D., Lewis, P. (2016) Space, the Final Frontier for Cybersecurity?. Royal Institute for International Affair, International Security Department, ISBN 978 1 78413 120 3, https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

Massie, A. (2016) Reframing the Third Offset as a 21st century model for deterrence. War on the Rocks, 28 March 2016, https://warontherocks.com/2016/03/reframing-the-third-offset-as-a-21st-century-model-for-deterrence/

Newcomb, A. (2016) Hacked in Space: Are Satellites the Next Cybersecurity Battleground?. CNBC News, 3 October 2016, https://www.nbcnews.com/storyline/hacking-in-america/hacked-space-are-satellites-next-cybersecurity-battleground-n658231

Pomerleau, M. (2016) Air Force outlines space and cyberspace tech R&D priorities. C4ISRNET, 22 August 2016, https://www.c4isrnet.com/special-reports/space-missile-defense/2016/08/22/air-force-outlines-space-and-cyberspace-tech-r-d-priorities/

Robinson, J., Robinson, R., Davenport, A., Kupkova, T., Martinek, P., Emmerling, S., Marzorati, A. (2019) State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints, Prague Security Studies Institute, Prague, available online at: http://www.pssi.cz/download/docs/686_executive-summary.pdf

Weinzierl, M. (2018) Space, the Final Economic Frontier, The Journal of Economic Perspectives, Vol. 32, No. 2 (Spring 2018), pp. 173-192, ISSN 1944-7965

Williams, B. (2014) Cyberspace: What is it, where is it and who cares?. Armed Forces Journal, 13 March 2014, http://armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares/

Robert MAZZOLIN

BGen (Ret'd) Ph.D., P.Eng., OMM, CD, SMIEEE, currently serves as the Chief Cyber Security Strategist for the RHEA Group, a space system engineering and security organization delivering security solutions to large enterprises, governments and institutions in Canada and Europe. He recently retired from the Canadian Armed Forces after serving as the Vice Director of Strategic Plans and Policy at United States Cyber Command at the National Security Agency in Fort Meade, Maryland. Notable appointments include the Director General Information Management Operations responsible for all CAF and DND strategic network, signals intelligence, electronic warfare and cyber operations, Commander of the Canadian Forces Information Operations Group, Director Land Command Systems Program Management, Commanding Officer Canadian Forces Station Leitrim and Canadian Forces Signals Intelligence Operations Centre. He served in a variety of other Command and Staff roles and was one of the Canadian Forces leading experts in Communications and Information systems, Signals Intelligence, Network Operations and Electronic Warfare. He holds a Bachelor of Electrical Engineering, Master of Science (Electronics and Guided Weapon Systems), Master of Arts in Security and Defence Management and Policy, and a Ph.D. in Engineering Management. He is a licensed Professional Engineer in Ontario, Senior Member of the Institute of Electrical and Electronics Engineers, an Officer of the Order of Military Merit. Included among other awards, are the United States Legion of Merit, United States Meritorious Service Medal, Italian Army Chief of General Staff Commendation for professionalism and courage for actions in Somalia and Chief of Defence Staff Commendation.