National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

RCAF UAS CYBERSECURITY THREAT MITIGATION FRAMEWORK

Maj Jeff Szumlanski

JCSP 44	PCEMI 44
SERVICE PAPER	ÉTUDE MILITAIRE
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018

SERVICE PAPER - ÉTUDE MILITAIRE

RCAF UAS CYBERSECURITY THREAT MITIGATION FRAMEWORK

Maj Jeff Szumlanski

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

Word Count: 2384

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

Compte de mots: 2384

RCAF UAS CYBERSECURITY THREAT MITIGATION FRAMEWORK

AIM

1. To propose an organizational cybersecurity threat mitigation framework for integration within the Royal Canadian Air Force (RCAF) Technical Airworthiness Authority (TAA) management and acquisition processes of future unmanned aerial systems (UAS)[1].

INTRODUCTION

2. The Department of National Defence (DND) and Canadian Armed Forces (CAF) Joint Unmanned Surveillance and Target Acquisition System (JUSTAS) programme was established in 2000 with the objective of delivering a military UAS capability capable of supporting Arctic and maritime sovereignty and domain awareness through provision of complementary intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) capability.[2] The operational immediacy and warfighting benefit of having military UAS was reaffirmed during Operation *Athena* and publication of the 2008 *Independent Panel on Canada's Future Role in Afghanistan*, referred to as the "Manley Report", recommending that a high-performance UAS providing intelligence, surveillance, and reconnaissance (ISR) would greatly benefit the

[1] As noted across a diverse cross-section of published technical and research literature, there is varied reference to these types of aircraft as drones, remotely piloted vehicles, uninhabited air vehicles, unmanned air vehicles, unmanned aircraft, and unmanned aircraft systems. To maintain consistency and clarity with Department of National Defence (DND), Canadian Armed Forces (CAF) and other published literature, the preferred label of unmanned aircraft system (UAS) used by the RCAF Aerospace Warfare Centre (RAWC) and other DND/CAF researchers will be used.

[2] Conrad Edward Orr, "Can Unmanned Aircraft Systems Meet Canadian Air Power Needs?" *Royal Canadian Air Force Journal* 5, no. 3 (2016), 16.

Canadian mission's safety and effectiveness.[3] Project Noctua facilitated the lease of three medium altitude long-endurance (MALE) Israeli Heron UAS platforms until the conclusion of CAF combat operations in Afghanistan. Despite its proven operational effectiveness and track record, the Heron lease was terminated upon mission closure. The CAF has retained limited military UAS, namely the ScanEagle and Raven-B platforms. However, the 2017 Defence Policy Guidance sets out specific guidance for acquisition of additional UAS assets: RCAF initiative 50 specifies future investment in a medium altitude platform, while Canadian Special Operation Forces Command (CANSOFCOM) initiative 57 identifies operational need for airborne platforms[4], anticipated to be long-endurance ISR UAS.[5]

3. Commensurate with other modern allied armed forces, RCAF strategic projections affirm UAS will continue to transform and revolutionize the manner of warfighting[6], with a critical need to exploit sensors, space-based assets, and autonomous UAS ISTAR platforms to maintain operational advantage.[7] However, the Canadian Air Force future outlook also acknowledges that modern military UAS comprise a cyber-physical "system-of-systems"[8] formed by the aerial platform linked with a sophisticated topology of datalinks, satellite communications, and ground control stations (GCS) with interconnectivity to data fusion centres to receive and process sensor

[3] John Manley et al., *Independent Panel on Canada's Future Role in Afghanistan* (Ottawa: Minister of Public Works and Government Services, 2008), 38.

[4] Government of Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (Ottawa: Department of National Defence, 2017), 39-40.

[5] David Johnston, "Future Airpower: Trends and Implications for Canadian Special Operations Forces Command (CANSOFCOM)", *Canadian Military Journal* 17, no. 4 (2017), 17.

[6] J.L.D. Lachance, *Projecting Power: Alternate Futures for Canada's Air Force in 2020* (Trenton: Canadian Forces Aerospace Warfare Centre, 2010), 13.

[7] Canadian Forces Aerospace Warfare Centre, *Projecting Power: Canada's Air Force 2035* (Trenton: Canadian Forces Aerospace Warfare Centre, 2009), 67.

[8] J.L.D. Lachance, *Projecting Power*, 23.

data.[9] Viewed in a network-centric warfare (NCW) perspective, UAS create a force-multiplier, but system interconnectedness inherently render these systems vulnerable to adversary cyber exploitation.[10] Future aerospace assets will require freedom of action in cyberspace and pre-emption of cyber attack to maintain reliability, integrity, and control of UAS and the timely, secure provision of its sensor data.[11] This paper synthesizes various unclassified publications related to UAS cyber threats and mitigation strategies, focusing on the National Institute of Standards and Technology (NIST) risk management framework and Directorate of Cyber Force Development (D Cyber FD) cyber resiliency perspective towards Advanced Persistent Threats (APT) to high-performance military UAS.

DISCUSSION

4. UAS share similar threats associated with any network connected cyber-physical system, such as denial of service, data exfiltration, or espionage.[12] However, UAS introduce an additional challenge during flight operations as there is no human-in-the-loop as a last line of defence against system compromise. The unmanned nature of UAS, coupled with advanced technological capabilities for autonomous operation and inter-UAS network-connectedness, create the potential for cyber-hijacked "swarms". Combined with the possibility of weaponizing the aerial platform, the severity and attack vector scenarios fathomable by means of a proliferation of cyber comprised UAS platforms greatly increase risk associated with failing to improve UAS resiliency against cyber threats.[13] Small commercially available UAS (sUAS),

[9] *Ibid.*

[10] "Zeros and ones: tackling cyber at the tactical edge", *International Defence Review* 46, no. 12 (2013), 1-2.

[11] Canadian Forces Aerospace Warfare Centre, *Projecting Power: Canada's Air Force 2035*, 64-70.

[12] Gerrard Cowan, "Unmanned and under attack: Defending UAVs from cyber threats", *Jane's International Defence Review* 50, no. 2 (2017), 1.

[13] Manimaran Mohan, *Cybersecurity in Drones* (New York: Utica College, 2016), 2.

primarily manufactured for recreational or small business purposes, are classified by the United States Federal Aviation Association (FAA) as weighing 55 pounds or less. Constrained by size, weight, technology, and system cost to incorporate advanced security features this category of UAS are highly vulnerable and easily exploited by hackers, particularly GPS spoofing given lack of access to the military encrypted GPS P-code. Cyber threat mitigation strategies related to sUAS products focus predominantly on establishing mandated security standards for commercial manufacturers to fix security loopholes in their technology prior to making products available to the public.[14] This paper focuses specifically toward DND/CAF UAS cyber threat mitigation strategies involving complex, interconnected medium to large high-performance military systems.

5. The complexity associated with improving cyber threat resiliency of these advanced military systems is exponentially related to the number of technological components and interconnected networks in the system-of-systems comprising modern military UAS integrated into network-centric warfare battlespace.[15] For example, as depicted in Figure 1, Kim et al. use the Global Hawk example of interconnected system architecture to demonstrate the possibility of nefarious attack against one system component to induce failures elsewhere, representing a cyber threat vector if not adequately defended or resilient to exploitation.[16] An actual cyber threat of this nature occurred in September 2011 when an unknown actor executed a malicious code attack using the keylogger malware virus infection within Predator and Reaper GCS based at USAF

[14] Leela Krishna C.G. and Robin R. Murphy, “A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles”, *IEEE International Symposium on Safety, Security and Rescue Robotics* (2017), doi:10.1109/SSRR.2017.8088163, 196-197.

[15] Gerrard Cowan, “Unmanned and under attack”, 2.

[16] Alan Kim, Brandon Wampler, James Goppert, and Inseok Hwang, “Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles”, *American Institute of Aeronautics and Astronautics* (2012), last accessed 25 January 2018, https://arc.aiaa.org/doi/abs/10.2514/6.2012-2438, 3.

Base Creech, Nevada. Although detected by internal computer network defence systems, reports indicate the malware was highly resistant to purging from GCS systems. [17]

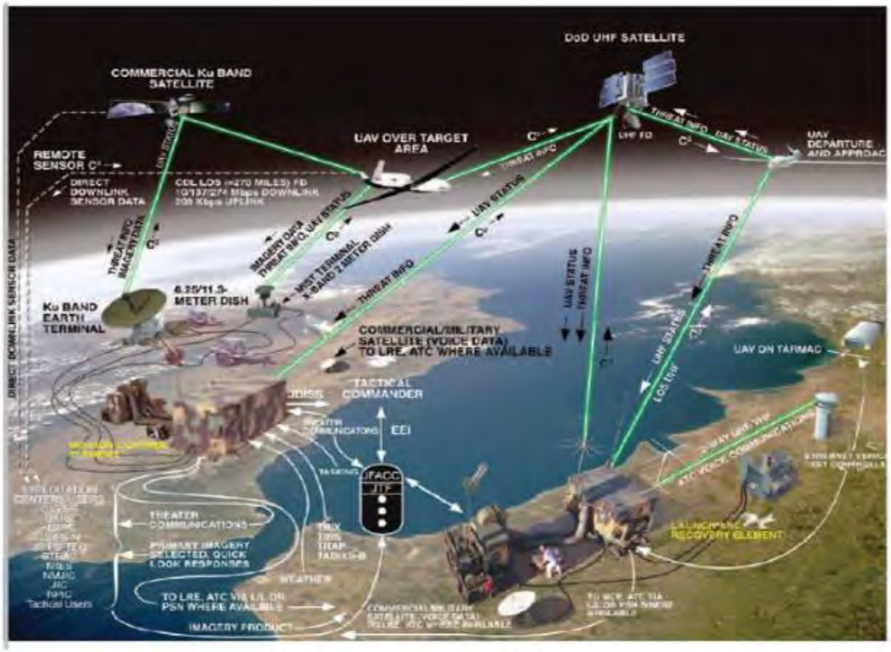
COMMERCIAL Ku BAND SATELLITE
DoD UHF SATELLITE
UAV OVER TARGET AREA
REMOTE SENSOR C²
DIRECT DOWNLINK SENSOR DATA
CDL LOS (≈270 MILES) FD 10/137/274 Mbps DOWNLINK 200 Kbps UPLINK
THREAT INFO. IMAGERY DATA
C²
UAV STATUS
IMAGERY DATA THREAT INFO, UAV STATUS
MIST TERMINAL X-BAND 2 METER DISH
THREAT INFO
6.25/11.3-METER DISH
Ku BAND EARTH TERMINAL
DIRECT DOWNLINK SENSOR DATA
COMMERCIAL/MILITARY SATELLITE (VOICE DATA) TO LRE, ATC WHERE AVAILABLE
UHF FD
UAV DEPARTURE AND APPROAC
UAV STATUS
THREAT INFO
UAV ON TARMAC
LOS FD
JDISS
TACTICAL COMMANDER
EEI
JFACC
JTF
TASKING
THEATER COMMUNICATIONS
PRIMARY IMAGERY SELECTED, QUICK LOOK RESPONSES
WEATHER
TO LRE, ATC VIA UL OR PSN WHERE AVAILABLE
IMAGERY PRODUCT
TRAP
LAUNCH AND RECOVERY ELEMENT
ATC VOICE COMMUNICATIONS
Tactical Users

Figure 1 – Interconnected Communication Links in a Global Hawk UAS Network[18]

6. A second distinguishing factor of UAS cybersecurity is the wireless communication aspect of flying the aerial platform whilst transmitting and receiving data travelling at high velocities, potentially hundreds of kilometres an hour at distances extending beyond line of sight (BLOS). A conventional military UAS aerial platform is depicted in Figure 2 showing its variety of different sensing and communication components.

[17] "Zeros and ones", 5.

[18] Alan Kim, Brandon Wampler, James Goppert, and Inseok Hwang, "Cyber Attack Vulnerabilities", 4.

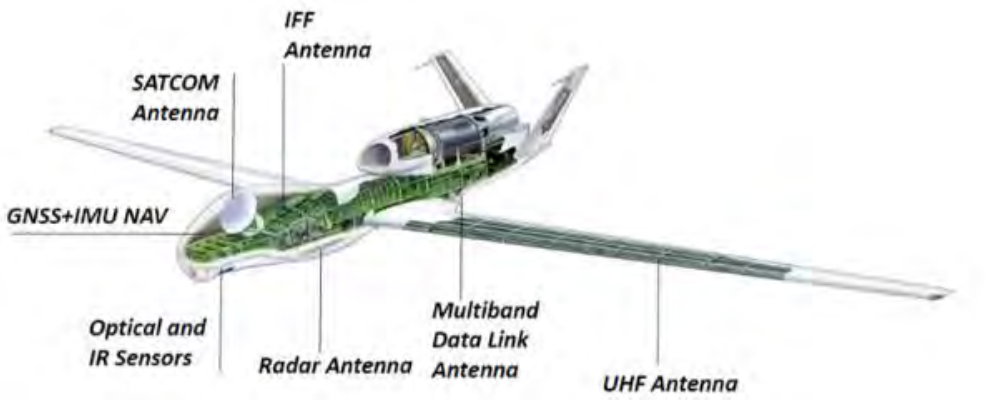

Figure 2 – Contemporary Sensing and Communication Components of a High-performance Military UAS Aerial Platform[19]

High-performance military UAS of interest to DND and the CAF normally includes multiple communication antennas in different frequency bands. The various antennas normally support frequencies used for air-to-air (ATA), air-to-ground (ATG), satellite communication BLOS navigation, in-flight data transfer, Global Navigation Satellite System (GNSS) for accurate flight positioning, onboard Inertial Measurement Unit (IMU) enabling relative position fixes based on kinetic vehicle sensors, and automatic dependent surveillance – broadcast (ADS-B), a form of air traffic control collision avoidance functionality. [20] However, the wireless, unmanned and autonomous nature of UAS reliant upon these multiple communication and navigation links inherently introduce cyber threat vulnerabilities that can be exploited by adversaries. GNSS signals are highly susceptible to spoofing attacks, enabling adversaries to capture the platform or cause mid-air collision by deliberately inducing navigation system errors. An example of this type of attack occurred on 4 December 2011 when an American Lockheed Martin RQ-170

[19] Vahid Behzadan, "Cyber-Physical Attacks on UAS Networks – Challenges and Open Research Problems", *Cornell University Library arXiv.org* (2017), last accessed 25 January 2018, https://arxiv.org/pdf/1702.01251.pdf, 2.

[20] *Ibid.*, 2.

Sentinel was captured after Iranian Forces jammed its satellite signals and spoofed the GNSS navigation. It was forced to land near the city of Kashmar, approximately 225 kilometres inside northeastern Iran.[21]

7. Research analysis and mitigation of UAS cyber threat vulnerabilities tended to approach the problem space in a similar methodological manner, first commencing with a classification of the various system components or network layers prior to examining architecture weaknesses and mitigation strategies in detail. Interestingly, researchers Krishna and Murphy proposed a UAS cyber vulnerability taxonomy based on a highly similar framework developed to study cyber threats to driverless cars; categories were expanded to include UAS-specific areas vulnerable to cyber exploitation highlighted by the green-shaded areas in Figure 3 below.

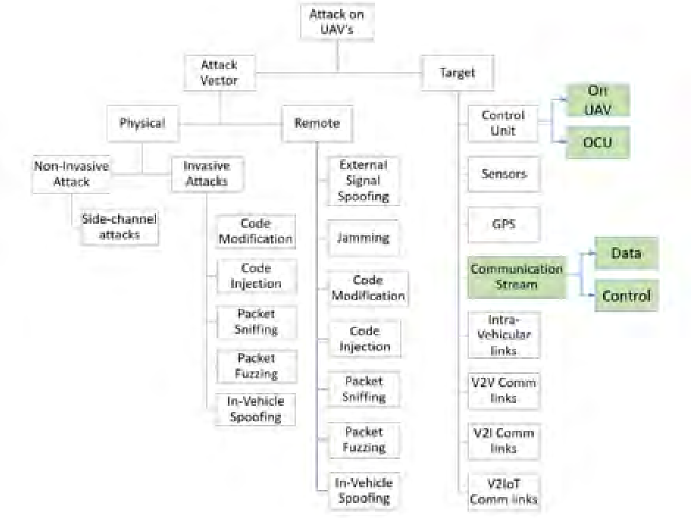

Figure 3 – Krishna and Murphy UAS Cyber Vulnerability Taxonomy[22]

[21] "Zeros and ones", 5.
[22] Leela Krishna C.G. and Robin R. Murphy, "A Review on Cybersecurity Vulnerabilities", 197.

The first category, attack vector, is further divided between physical means, such as virus code injection, and remote means, for example GPS jamming or spoofing. The second, attack target, specifically breaks out broad categories of UAS sub-system design, such as the sensors, control unit, or communication streams. Other research methodologies similarly stratify UAS vulnerabilities through sub-system groupings. For example, Kim et al. categorized general attack possibilities into three groups: hardware attack, wireless attack, and sensor spoofing.[23] Dufrene classified his UAS cyber security research across the physical, computer, and communications layer.[24] The significant commonality amongst these research approaches to UAS cybersecurity vulnerability analysis is a deliberate initial effort to standardize a common 'system-of-systems' taxonomy, model, or architectural frame of reference prior to studying the actual problem. Interestingly, viewed from a DND/CAF organizational perspective, this initial step has strategic benefit at the onset of any UAS project acquisition lifecycle as it enables greater clarity of communication across a broad number of differing agencies, mitigating potential cybersecurity gaps caused by differing frames of reference used in staff processes and documentation.

8. Furthermore, researchers Mansfield et al. contend that no UAS cybersecurity policy is complete without consideration of human threats that can be introduced by "system users and maintainers, careless mistakes, or inadequate practices…or policies."[25] Their threat model research of smart device use within Department of Defence (DoD) military UAS integrates application of the already established National Institute of Standards and Technology (NIST)

[23] Alan Kim, Brandon Wampler, James Goppert, and Inseok Hwang, "Cyber Attack Vulnerabilities", 6.

[24] Warren R. Dufrene, Jr., "Mobile Military Security with Concentration on Unmanned Aerial Vehicles", *IEEE* (2005), doi.10.1109/DASC.2005.1563475, 8.D.3-4.

[25] Katrina Mansfield, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani, "DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model", *Defence Acquisition Research Journal* 22, no. 2 (2015), 258.

Risk Management Framework for Information Technology Systems. [26] NIST has been designated as the authoritative cybersecurity framework for both American federal government agencies and private industry.[27] The six steps of the NIST process are presented in Figure 4. As aforementioned, notice that step 1, "categorize information system", involves development of a common architecture description as part of the basis within the initial step of the NIST cybersecurity framework that provides the foundation of all further organization efforts.

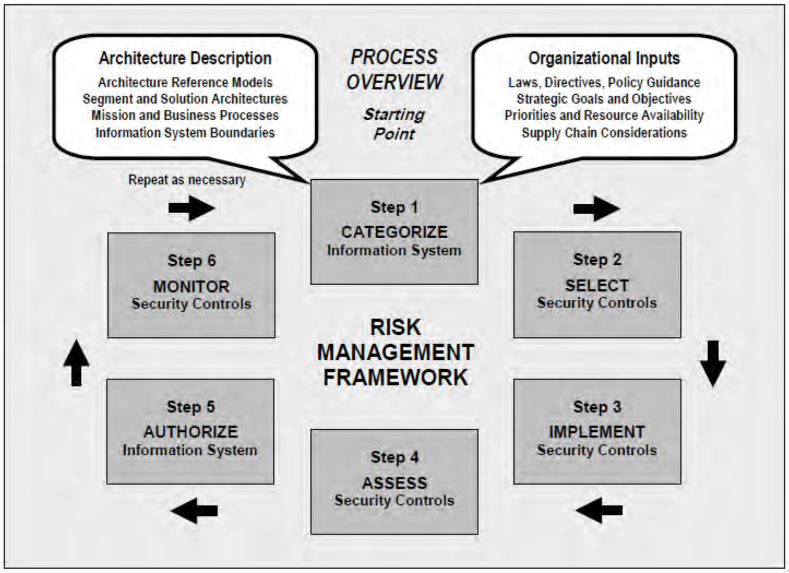
Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Figure 4 – NIST Cybersecurity Risk Management Framework[28]

Although adoption of the NIST Cybersecurity Risk Management Framework is currently voluntary by private companies, United States Government Executive Order (EO) 13636 states that Federal Department and Agencies are responsible for adopting NIST in advance of any

[26] *Ibid.*, 259.

[27] *Ibid.*

[28] Wayne Rockwell, *"Leverage System Security Engineering for Cyber Defense – Information Brief"* (Ottawa: Air Cyber Mission Assurance Workshop, 2018), last accessed 30 January 2018, https://acmaw.segfaults.net/

legislative action to enhance cybersecurity resilience within national critical infrastructure.[29] The EO instructs the Director of NIST and Secretary of Homeland Security to establish a voluntary program that "provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk."[30] Critical infrastructure as defined by the EO includes any systems or assets that would, if incapacitated or destroyed, either physical or virtual, have a national impact debilitating safety or security, which inherently include military UAS and their associated interconnected secure operations and maintenance systems.[31] The NIST framework is sufficiently flexible to complement any organization's existing cybersecurity risk management processes and program. However, any organization "without an existing cybersecurity program can use the Framework as a reference to establish one."[32] The Canadian Government 2017 Defence Policy Guidance instituted a similar mandate to DND/CAF by means of cyber initiative 87, seeking to "protect critical military networks and equipment from cyber-attack by establishing a new Cyber Mission Assurance (CMA) Program that will incorporate cyber security requirements into the procurement process."[33] Research demonstrates that vaguely written security policies often leave room for interpretation and "fail to hold the program manager of the defence contractor accountable for implementation of specific security parameters will be outweighed by costs, resources, mission requirements, time constraints and

[29] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity", *Federal Register* 78, no. 33 (February 19, 2003), last accessed 25 January 2018, https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf, 1.

[30] National Institute of Standards and Technology, *Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework*, last accessed 30 January 2018, https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf, 1.

[31] *Ibid.*

[32] *Ibid.*

[33] Government of Canada, *Strong, Secure, Engaged*, 73.

politics to meet the program schedule."[34] Thus, it can be argued the RCAF has an opportunity to leverage the NIST cybersecurity risk mitigation framework as an established, widely-recognized organizational process that would improve cyber resiliency across the entire UAS project lifecycle.

9. However, cybersecurity research conducted at Lockheed Martin Corporation argues that computer network intrusion and attack has become increasingly sophisticated, involving a new class of well-trained, supported, and politically-motivated state-level hacker given the label "Advanced Persistent Threat."[35] They contend conventional means of cyber security can be evaded, such as anti-virus algorithms, intrusion detection systems, and firewalls. These means of cybersecurity are thus insufficient against APT adversaries who conduct multi-year intrusion campaigns of an iterative nature, increasing their information superiority through knowledge gained by each attempt at infiltration.[36] To thwart the higher cybersecurity threat posed by APT to military UAS 'system-of-systems', the Lockheed Martin approach to organizational cybersecurity is premised on the Cyber Kill Chain model outlined in Figure 5. According to Lockheed Martin, the theory underpinning this model requires that organizations perceive APT cyber intrusions as a series of phased events, not as singular intrusions. By disrupting one element in the chain thwarts the overall objective of the adversary. By analyzing various repetitive indicators of an APT, an overall intelligence picture is compiled to develop a holistic understanding of the adversary, and their persistence becomes a liability as each additional

[34] Katrina Mansfield, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani, "DoD Comprehensive", 249.

[35] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", *Lockheed Martin Corporation* (2011), last accessed 30 January 2018, https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf, 1.

[36] *Ibid.*, 1-2.

intrusion attempt adds greater perspective to the overall intelligence profile developed by computer network defence personnel.[37]

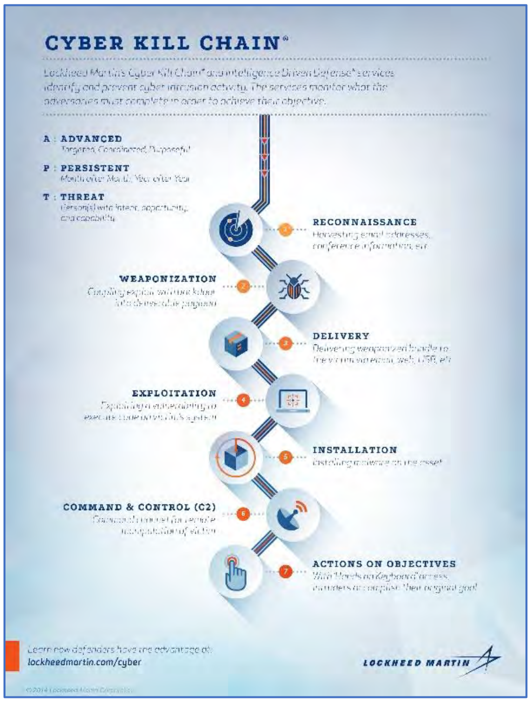
CYBER KILL CHAIN®
Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.
A : ADVANCED
Targeted, Coordinated, Purposeful
P : PERSISTENT
Month after Month, Year after Year
T : THREAT
Person(s) with intent, opportunity, and capability
1
RECONNAISSANCE
Harvesting email addresses, conference information, etc
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goal
Learn how defenders have the advantage at:
lockheedmartin.com/cyber
LOCKHEED MARTIN
© 2014 Lockheed Martin Corporation

Figure 5 – Lockheed Martin Cyber Kill Chain Model[38]

10. Both the NIST and Cyber Kill Chain frameworks promote cyber mission assurance of military UAS by advocating the D Cyber FD principle of computer network "defence in depth", rather than individual ad-hoc firewalls and patches applied in reaction to adversarial intrusions.[39] Although the Lockheed Martin model provides a systematic model to mitigate UAS cyber threats, particularly against APT, the model is aptly suited as a cyber-focused risk assessment and identification tool suited for NIST Step 4, "Assess Security Controls". The RCAF requires a

[37] *Ibid.,* 3.

[38] Lockheed-Martin, *"Infographic: Cyber Kill Chain"*, last accessed 1 January 2018, https://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html

[39] Major Guillaume Vigeant, Cyber Network Operations (CNO) Instructor, Directorate Cyber Force Development (D Cyber FD) – RMC Kingston Detachment, email dated Tuesday 30 January 2018.

holistic UAS cybersecurity threat mitigation framework that facilitates organizational processes throughout the entire system lifecycle. The NIST model is ideal, offering a well-recognized, established cybersecurity framework for rapid organizational adaptation with the objective to "develop a robust technical basis to allow organizations to align this guidance with their organizational practices."[40] NIST also includes aspects of both internal and external accountability. Thus, the NIST framework is ideally suited to government military UAS project acquisition and maintenance initiatives.

CONCLUSION

11. The 2017 Defence Policy Guidance contains military UAS acquisition initiatives for both RCAF and CANSOFCOM ISR requirements. The RCAF strategic outlook recognizes the benefit UAS provide in a network-centric warfare battlespace but accedes that cybersecurity resilience within the information domain is critical to leveraging this aerial platform as a force multiplier. High-performance military UAS are an interconnected 'system-of-systems' inherently vulnerable to cyber attack given their unmanned, wireless, and autonomous characteristics. The emergence of a new class of cyber APT threat increases the complexity of computer network defence mechanisms required. Cyber Mission Assurance initiatives within the latest Defence Policy Guidance are ideally aligned with both the NIST Cybersecurity Risk Management Framework and Lockheed Martin Cyber Kill Chain model that reinforce the importance of organizational threat mitigation strategies that examine computer network defence "in-depth". However, to inculcate a comprehensive organizational cybersecurity threat mitigation framework across the entire UAS project lifecyle, including accountability processes that encourage compliance of external entities outside of DND/CAF to prioritize robust cybersecurity best practices as well, the

[40] National Institute of Standards and Technology, *Improving Critical Infrastructure Cybersecurity*, 2.

NIST Cybersecurity Risk Management Framework provides the RCAF a recognized and established process to integrate within future high-performance military UAS acquisition and management initiatives.

RECOMMENDATION

12. It is recommended the RCAF, as TAA for DND/CAF UAS acquisition and project management, implement the recognized and established NIST Cybersecurity Risk Management Framework across all military UAS project lifecycle activities as part of a well-funded, robust strategy integrating cyber mission assurance processes within the overall organization. Figure 6 shows the recommended NIST model rebranded as the RCAF UAS Cybersecurity Risk Management Framework that will improve cyber resiliency and threat mitigation in future CAF military ISTAR platforms and their interconnected 'system-of-systems'.

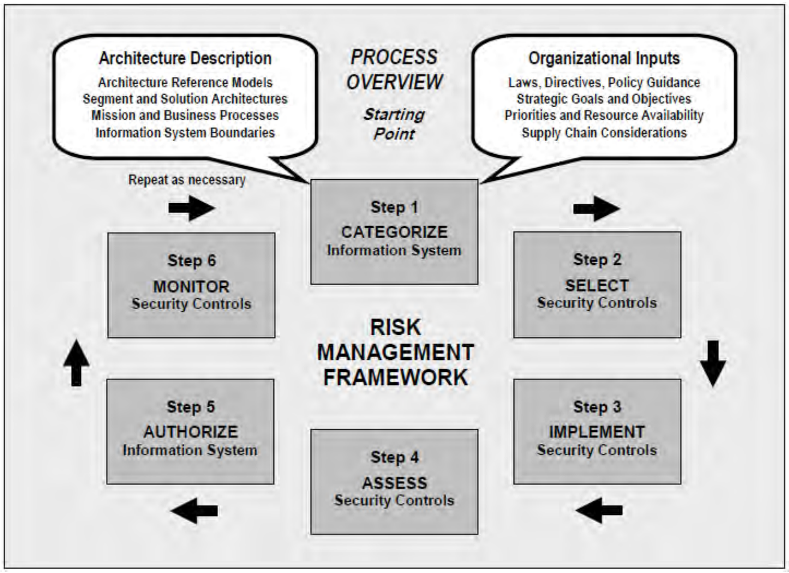
Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Figure 6 – Proposed RCAF UAS Cybersecurity Risk Management Framework

BIBLIOGRAPHY

Behzadan, Vahid. "Cyber-Physical Attacks on UAS Networks – Challenges and Open Research Problems." *Cornell University Library arXiv.org* (2017). Last accessed 25 January 2018. https://arxiv.org/pdf/1702.01251.pdf.

Canadian Forces Aerospace Warfare Centre. *Projecting Power: Canada's Air Force 2035.* Trenton: Canadian Forces Aerospace Warfare Centre, 2009.

Cowan, Gerrard. "Unmanned and under attack: Defending UAVs from cyber threats." *Jane's International Defence Review* 50, no. 2 (2017).

Dufrene, Warren R., Jr. "Mobile Military Security with Concentration on Unmanned Aerial Vehicles." *IEEE* (2005). doi.10.1109/DASC.2005.1563475.

Executive Order 13636. "Improving Critical Infrastructure Cybersecurity." *Federal Register* 78, no. 33 (February 19, 2003). Last accessed 25 January 2018. https://www.treasury.gov/ press-center/Documents/Supporting%20Analysis%20Treasury%20Report %20to%20the%20President%20on %20Cybersecurity%20Incentives_FINAL.pdf.

Government of Canada. *Strong, Secure, Engaged: Canada's Defence Policy.* Ottawa: Department of National Defence, 2017.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Lockheed Martin Corporation* (2011). Last accessed 30 January 2018. https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf.

Johnston, David. "Future Airpower: Trends and Implications for Canadian Special Operations Forces Command (CANSOFCOM)." *Canadian Military Journal* 17, no. 4 (2017).

Kim, Alan, Brandon Wampler, James Goppert, and Inseok Hwang. "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles." *American Institute of Aeronautics and Astronautics* (2012). Last accessed 25 January 2018, https://arc.aiaa.org/doi/abs/10.2514/6.2012-2438.

Krishna, Leela C.G. and Robin R. Murphy. "A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles." *IEEE International Symposium on Safety, Security and Rescue Robotics* (2017). doi:10.1109/SSRR.2017.8088163.

Lachance, J.L.D. *Projecting Power: Alternate Futures for Canada's Air Force in 2020*. Trenton: Canadian Forces Aerospace Warfare Centre, 2010.

Lockheed-Martin. *"Infographic: Cyber Kill Chain."* Last accessed 1 January 2018. https://www.lockheedmartin.com/us/news/features/2014/isgs-cyber-kill-chain.html.

Manley, John et al. *Independent Panel on Canada's Future Role in Afghanistan*. Ottawa: Minister of Public Works and Government Services, 2008.

Mansfield, Katrina, Timothy Eveleigh, Thomas H. Holzer, and Shahryar Sarkani. "DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model." *Defence Acquisition Research Journal* 22, no. 2 (2015).

Mohan, Manimaran. *Cybersecurity in Drones.* New York: Utica College, 2016.

National Institute of Standards and Technology. *Improving Critical Infrastructure Cybersecurity Executive Order 13636, Preliminary Cybersecurity Framework.* Last accessed 30 January 2018. https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf.

Orr, Conrad Edward. "Can Unmanned Aircraft Systems Meet Canadian Air Power Needs?". *Royal Canadian Air Force Journal* 5, no. 3 (2016).

Rockwell, Wayne. "Leverage System Security Engineering for Cyber Defense – Information Brief." Ottawa: Air Cyber Mission Assurance Workshop, 2018. Last accessed 30 January 2018. https://acmaw.segfaults.net/.

"Zeros and ones: tackling cyber at the tactical edge". *International Defence Review* 46, no. 12 (2013).