23 October 2023

CYBER HYGIENE WORKING GROUP – C&E WEEK 2023

References: A. New Vision for the Reserve Force (recent publication)
B Cybercapabilities - Canada.ca - https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/secd-april-24-2023/cybercapabilities.html
C. Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en &
D. An introduction to the cyber threat environment - Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment
E. JIMMY PADAWAN – Draft Network and Cyber Operations Training Plan v3
F. Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51 - Canada.ca - https://www.canada.ca/en/army/services/line-sight/articles/2022/02/offensive-cyber-in-the-canadian-armed-forces-opportunities-from-bill-c-51.html
G. Cyber operations - Communications Security Establishment (cse-cst.gc.ca) - https://www.cse-cst.gc.ca/en/mission/cyber-operations
H. Joint Capabilities - Canada.ca (2020/21) - https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/main-estimates-2020-2021/joint-capabilities.html
I. Evaluation of the Cyber Forces - Canada.ca (2021) - https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/eval-cyber-forces.html
J. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx

1. SITUATION

a. General: The digital domain is much like a dark forest. It is filled with wonder, natural resources, and exciting discoveries. Unfortunately, it is also home to many dangers. Much like the forest analogy, people (who explore, live, and make their living in the digital domain) possess a normal range of knowledge, skill and awareness to said dangers. The rate of technical evolution over the past 20 years has created a significant gap between risk and awareness. This working group will attempt to close this gap with a formalized framework, action items, and other tools to better defend against digital threats.

b. Background: *Significant material has been produced relating to the "cyber problem". Participants can review references above if they do not have sufficient background knowledge.*

2. OBJECTIVE

a. Introduction: This working group will explore a range of battlefield effects that the CA (Ares) may be able to perform with the understanding that the Reserve Force is not (presently) tooled to provide CFNOC and D Cyber FD with direct cyber task support. The purpose of these sub-cyber effects will be to enhance a Unit CO or CBG Comds garrison and field cyber-hygiene and create resilient soldiers and officers.

a. In Scope:

(1) Measurable tasks in support of units in the field.

(2) Education programs and products

(3) Cyber Hygiene Unit Standing Orders, SOPs and FSOPs

(4) Enhancing ISSO tasks/roles

(5) Cyber ROEs and "Actions On" a detected attack

(6) Defining new roles within the CA organization.

(7) Defensive battlefield effects.

b. Out of Scope:

(1) Direct Cyber-Network Tasks

(2) Offensive Operations Training

(3) Tasks that have a high risk of negative impact to the public domain.

3. EXECUTION - DISCUSSION

a. Initial Threat-Risk Assessment

(1) Device Threats:

i. Location Tracking: As seen in Ukraine with the active tracking and targeting of cellular signals. Can we replicate this in a limited capacity, (geo restricted) for field deployments?

ii. Hardware requirements?

iii. Legal considerations?

iv. Training model?

(2) Wireless Hygiene: Leaving wireless devices "on" which can lead to detection/identification.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Hardware for sniffing wireless signals? – use data to support education products.

(3) Device Dependence: Using a digital device as a flashlight, alarm clock, navigation tool…etc

i. Education Program – Briefs, soldier cards, SOPs?

ii. Field Audit – site check for personal equipment? Surrender personal phones in the field?

(4) Multi-Function Device Risk: Similar to the above risk, but also includes the need for backup equipment in case of loss.

i. Business Continuity Planning?

ii. Equipment Redundancy Exercises?

iii. EXCON scenarios – removal (notional) of equipment to test redundancy SOPs

(5) Threat Vectors: Device as a threat vector (ie: microphone and camera exploit)

i. Hardware/software to do this in a controlled environment?

ii. Educate through demonstration?

b. <u>Tech Dependence Threats:</u>

(1) Over-reliance Risk: Behavioral risk, where someone becomes dependent on certain technologies for normal function.

i. Business Continuity Exercises?

(2) Skill Fade (analogue skills): Example of digital maps overtaking paper maps in common use. (also navigation)

i. Business Continuity Exercises?

ii. Drills, drills, drills.

iii. IBTS reviews (ensure old training is brought forward more frequently)?

(3) Cognitive Fade Risk: Inability to store short term memory into long term recall due to cell phone pictures, digital note taking apps … etc.

i. Unit SOPs or Standing Orders to force soldiers/officers to take physical notes,

ii. Surrender devices during parade nights?

(4) Reality Truncating Risk: Whereby people start to view their environment through the lens of their digital app use.

i. Risk Mitigated as a result of less device use in other interventions?

(5) Addiction/Withdrawal Risks: The loss of access to a device may cause an anxiety response.

i. SrNCO role in coaching and mentoring?

c. Behavioral Threats:

(1) Location Tracking – Profiling: A threat actor may be able to track someone through social media. This can be used to create targeting data.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Volunteer personal threat assessment?

iii. Do we have skillsets to do this?

iv. Is it ethical to teach these skills?

v. Does this lead to a measurable reduction of risk?

(2) Habit Tracking: Similar to the above, tracking social media activity (online, posting frequency etc) can also be leveraged.

i. Same questions/points as above.

(3) Reckless Online Behavior Risk: Engaging in online arguments, visiting questionable websites and other risks.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Greylist/Blacklist Website List…Mobile Apps?

iii. Do/Do Not: "defined" online behaviors?

(4) App Activity Risks: Connecting to unknown WiFi access points for banking and other account access.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Do/Do Not: "defined" online behaviors?

(5) Behavioral Threat Awareness: "Ignorance is Bliss" or "Security by Obscurity" are dangerous personal attitudes to an organization.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Unit Level Threat Briefs (ISSO task?)

d. Targeting Threats:

(1) Social Engineering: Social Media risks are numerous.

i. Unit Level Threat Briefs (ISSO task?)

(2) Extortion & Fraud: A need to define activities that may expose people to this, and how to prevent risk.

i. Unit Level Threat Briefs (ISSO task?)

(3) Spoofing & Reputational Threats: This is a risk to people already targeted and may infer a more significant threat.

i. Unit Level Threat Briefs (ISSO task?)

ii. Demonstrating – Use real examples?

(4) Online Hygiene: Establish online best practices to ensure the minimization of exposure across the online space.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Unit Level Threat Briefs (ISSO task?)

iii. Volunteer personal threat assessment? Do we have skillsets to do this? Is it ethical to teach these skills? Does this lead to a measurable reduction of risk?

(5) Incident Management: Actions on being hacked or targeted. How to secure online resources and minimize damage.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Unit Level Brief – ACTION ON HACK (ISSO task?)

iii. Chain of Command involvement? What scenario does a personal hack cause a knock-on effect to unit effectiveness? What happens if a Sgt loses their life savings in a banking attack?

e. Cognitive Threats

(1) Dependence on technology: Education or Professional Development Program to minimize the chance of this risk.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Personal Assessments?

(2) Assorted Biases: A series of cognitive biases that may lead to unintended behaviors or choices that can be targeted by online activity. https://en.wikipedia.org/wiki/Cognitive_bias#/media/File:Cognitive_Bias_Codex_-_180+_biases,_designed_by_John_Manoogian_III_(jm3).jpg

i. Education Program – Briefs, soldier cards, SOPs?

ii. Mentorship and Coaching (CSM/RSM task?)

(3) Reality Distortion: A result of online echo-chambers. This threat may profoundly impact decision-making.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Mentorship and Coaching (CSM/RSM task?)

(4) Radicalization: This threat vector often comes from online.

i. Will need to explore a few options to mitigate. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx

ii. Education Program – Briefs, soldier cards, SOPs?

iii. Mentorship and Coaching (CSM/RSM task?)

(5) Attitude and Mood Attacks: Doom scrolling, and echo-chambers can have a profound mood effect that can lead to a number of undesirable outcomes.

i. Education Program – Briefs, soldier cards, SOPs?

ii. Mentorship and Coaching (CSM/RSM task?)

4. POTENTIAL FRAMEWORKS

a. Proposed Frameworks for Discussion:

(1) **Perimeter Defense – Wireless Defense Framework (OODA loop)**

i. Task: **SENSE**

(a) Human: Analyst or Operator (any trade, Jr NCM/2Lt)

(b) Hardware: COTS Laptop & Sensor (Wi-Fi pineapple or another device)

(c) Actions: Passive Scan for wireless signals in a defined range in the defined geolocation.

ii. Task: **DEFINE**

(a) Human: Analyst or Operator (any trade, Jr NCM/2Lt)

(b) Hardware/Software: COTS Laptop w/ Logging System/Chat/Database & Knowledge Base (threat directory?)

(c) Actions: Log detected signals in database, check against known records, report as per SOPs.

ii. Task: **MANAGE**

(a) Human: SrNCO or Officer with basic or advanced domain knowledge.

(b) Hardware: COTS Laptop, Chat program

(c) Actions: View reports and logs, receive reports and follow SOPs and ROEs, Report to higher, and be prepared to issue orders.

iv. Task: **ACT**

(a) Human: SrNCO or Officer with Analyst or Operator.

(b) Hardware: COTS Laptop & ????

(c) Actions: ????

(2) **Perimeter Defense: Online Presence & Personal Defense Framework**

i. **EDUCATE**

(a) Human: Instructor and Students (all members at the earliest training opportunity)

(b) Hardware: DLN3.0 and/or classroom, computer, projector, handouts and lesson plans.

(c) Actions: Use tools to educate on threats and SOPs

ii. **SANITIZE**

(a) Human: Instructor/Student 1:1 scenario

(b) Hardware: Civilian (unrestricted) computer with (open) internet access, VPN.

(c) Actions: Step-by-step sanitization of the student's online presence. Detect and identify risks and mitigation strategies.

iii. **SHAPE**

(a) Human: Instructor/Student 1:1 scenario

(b) Hardware: Civilian (unrestricted) computer with (open) internet access, VPN.

(c) Actions: Step-by-step design and build of an obfuscated online persona. Identify risks and mitigation strategies.

iv. **TEST**

(a) Human: 2nd Instructor (not witness to the SHAPE actions)

(b) Hardware: Civilian (unrestricted) computer with (open) internet access, VPN.

(c) Actions: Search for and test the security of the student's SANITIZE actions.

v. **ITERATE**

(a) Human: Instructors/Students

(b) Hardware: Same as above

(c) Actions: Review All previous actions, improve where needed, update techniques if needed.

5. ADDITIONAL QUESTIONS:

a. Do we have a methodology to identify vulnerabilities, define threats/risks, harden(protect) against attacks and monitor/detect when they occur?

b. Do we have the technology/tools to do the initial functions indicated above?

c. What practical technical support roles (sub-cyber ops) that can be used as the lowest rung of the cyber-skills ladder?

d. What kind of tasks/effects is the current force employer looking for? (Capability enhancement)

e. What is the minimum knowledge threshold for entry? (Define a train-up-to-level# approach)

f. Is there an appetite for targeted recruitment?

g. Is there an appetite for a joint-civil-military mentorship program?

h. Is there hardware available that can be used in such activities?

i. What is the cost (to our Units/Brigades and the CAF) if we do not succeed?

6. SERVICE SUPPORT

a. Working Group Sessions – CFB Kingston

(1) Thu 26 Oct 0800-1200: WGs Session 1

(2) Thu 26 Oct 1300-1600: WGs Session 2

b. MS TEAMS dial-in details - *TBD*

c. Physical Location: *TBD*

d. WG Website: https://cmcen-rcmce.ca/events/ce-working-group-2023/

7. COMMAND AND SIGNALS

a. WG Chair: CWO Peter G Nordstrom – 306-216-1962 - peter.nordstrom@forces.gc.ca

b. WG Vice Chair: WO Ben Morrison – 613-945-6455 Ext 7437 – Benjamin.morrison@forces.gc.ca

c. 2023 C&E Week WG Coordinator: Maj (OF-3) Jack Shen - Tel: 613-541-5010 ext 5064 / Cell: 343-548-7029 --- Jianan.Shen@forces.gc.ca

Potential Models

Perimeter Defense – Wireless Defense Framework (OODA loop)