Guide de cybersécurité du MDN

Une perspective du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC)

Ce bref document vise à fournir des réflexions du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC) au min DN sur les domaines de discussion possibles au sein du gouvernement du Canada (GC) sur l'amélioration de notre résilience collective dans le cyberespace et la capacité de décourager les agressions, à offrir des options au gouvernement, à appuyer notre capacité de mener à bien toutes les missions autorisées et à demeurer un partenaire fiable de la coalition.

Il y a des indications que la Stratégie de cybersécurité du GC fera l'objet d'un examen dirigé par Sécurité publique Canada (SP). Ce travail devrait être appuyé en vue d'élaborer une mise à jour complète avec l'apport de l'ensemble des intervenants, y compris le MDN et les FAC. Publiée en 2010 et quelque peu modifiée en 2018 pour annoncer la *Loi sur le Centre de la sécurité des télécommunications* (CST) et le Centre canadien pour la cybersécurité (CCCS), la situation qui sous-tend la stratégie a considérablement évolué au cours des années suivantes et beaucoup a été appris. Une stratégie révisée pourrait actualiser la position, les plans et les priorités du GC dans le cyberespace.

Le MDN et les FAC travaillent à comprendre le domaine cybernétique et élaborent des plans d'intervention depuis une décennie. Un certain nombre de grands thèmes ont émergé et englobent bon nombre des observations et des tendances qui ont été notées au fil du temps. Les voici :

- La dissuasion par la résilience. Ce terme est emprunté aux États-Unis, mais la résilience est devenue un facteur important au Canada et avec nos alliés (référence au décret 14028 promulgué par les États-Unis et aux engagements sur le renforcement de la résilience de l'OTAN) qui pourrait se refléter dans les priorités canadiennes. Cela est beaucoup plus grand que le MDN et les FAC; notre préoccupation porte sur nos propres réseaux, plateformes et systèmes d'armes, mais la possibilité de réduire les demandes d'aide nationales (qui peuvent inclure ou non le MDN et les FAC) lorsque le paysage canadien en général souffre des répercussions négatives des cyberacteurs malveillants est importante. Cela pourrait comprendre des choses comme :
    - Comprendre et renforcer les chaînes d'approvisionnement
    - Protéger les infrastructures essentielles
    - Des programmes de sensibilisation contre la désinformation
    - Préciser les pouvoirs, responsabilités et obligations (PRO) fédéraux, provinciaux, territoriaux et municipaux
    - De la surveillance, de la conformité (axée sur les résultats) et l'application de la loi (cadres et lois)
    - Des cadres d'atténuation des risques, comme le cadre d'assurance des cybermissions du MDN et des FAC, qui visent à exposer les risques liés aux opérations (armes, plateformes, systèmes de technologie de l'information [TI], appareils personnels, etc.) dans le cyberespace et à accepter ou atténuer systématiquement ces risques pour assurer le succès des missions.

- Une meilleure compréhension par la collaboration. Le cyberespace est un domaine relativement nouveau, mais le min DN reconnaît clairement qu'il s'agit d'un domaine de guerre et d'opérations que nous devons comprendre. Les alliés sont allés jusqu'à déclarer le cyberespace comme un domaine de guerre traditionnel pour aider à cette compréhension. En plus de cette compréhension générale des répercussions du domaine, une plus grande capacité en matière de renseignement et des collaborations plus importantes seront essentielles au succès. L'acquisition, l'utilisation et le partage accrus de renseignements devraient comprendre :
    - Une collaboration interne au GC.
    - Une collaboration multilatérale le long des canaux existants et nouveaux du cyberrenseignement.
    - Des engagements auprès de l'industrie (fournisseurs d'accès à Internet [FAI], obligation/incitation à signaler les incidents) et du milieu universitaire (national et allié).
    - Des évaluations et des cadres des gains et des pertes du renseignement parmi tous les intervenants.
    - Une capacité accrue en matière de cyberrenseignement pour le MDN et les FAC intégrée au Renouvellement de l'entreprise du renseignement de défense (RERD).
    - Tirer davantage parti des capacités de renseignement électromagnétique (SIGINT) traditionnelles pour contribuer à notre compréhension du cyberdomaine.

- Des options et des interventions coordonnées. Il sera essentiel à l'avenir d'offrir au GC des options solides au moyen d'une vaste capacité d'intervention. Le Canada doit être actif militairement dans le cyberespace pour être pertinent et interopérable avec nos alliés et nos partenaires. Les FAC ont déjà reçu l'orientation du GC pour s'affirmer davantage dans le cyberespace, renforcer nos défenses et développer et mener des cyberopérations actives (offensives). Il est à noter qu'un cyberincident ne justifie pas nécessairement une cyberréponse et vice versa. De plus, on a eu l'impression que les cyberactions des nations occidentales peuvent déclencher une escalade rapide;

  Cela est également étroitement lié à la dissuasion dans le cyberespace. Toutefois, jumelées à la dissuasion, la planification et la préparation délibérées (y compris le développement des capacités) avant que des hostilités surviennent sont une caractéristique clé du succès des cyberopérations à l'avenir. Compte tenu de ces facteurs, les éléments suivants pourraient être pris en considération :
    - Un cadre clairement compris et des PRO établis pour tous les intervenants afin de permettre une prise de décision rapide et des interventions coordonnées.
    - Normaliser la planification, la préparation, les opérations et les interventions grâce à une capacité, une collaboration et une communication accrues.
    - Des cadres opérationnels alignés sur les intérêts canadiens et les principaux alliés qui sont actifs dans le cyberdomaine. Les alliés demandent de plus en plus la coopération opérationnelle et recherchent des cadres opérationnels (missions désignées) qui comprennent des interventions cybernétiques robustes, qu'il s'agisse d'opérations propres à la cybernétique ou du soutien pour des opérations plus conventionnelles.

- Faire évoluer le concept de dissuasion comme un ensemble complet de mesures parmi tous les principaux intervenants. Le MDN et les FAC pourraient offrir un large éventail d'options de dissuasion dans tous les domaines qui contribueraient à la dissuasion générale dans le cyberespace et qui devraient être incluses dans des plans exhaustifs.
- Des cadres d'intervention nationaux qui placent le MDN et les FAC dans un rôle de soutien semblable à toutes les autres opérations nationales (OP NAT) (incendies, inondations, etc.).

- Développement des capacités et perfectionnement du personnel. Il faudra investir dans les gens, les capacités et les processus pour être en mesure d'en faire plus pour le Canada dans le cyberespace. De la résilience à la défense en passant par les capacités offensives, les intervenants, y compris le MDN et les FAC, devront recruter, former, employer et maintenir en poste des cyberprofessionnels. Le MDN et les FAC ont un plan de développement des forces qui s'étend jusqu'en 2035. Ce plan nécessitera des ressources au fil du temps pour bâtir une cyberforce militaire capable d'exécuter des opérations dans le cyberdomaine de la même manière (mais peut-être pas selon la même échelle) que les services traditionnels exécutent des opérations dans les domaines terrestre, aérien et maritime et se réunissent pour obtenir de meilleurs résultats à l'appui des missions autorisées du GC.

En conclusion, la cybernétique est un sport d'équipe. Qu'il s'agisse d'affaires internes au MDN ou aux FAC, au sein du GC ou de relations externes avec nos partenaires, aucune entité ne protège le Canada et ses intérêts dans le cyberespace. Nous devons tous en faire davantage, mettre en commun étroitement nos efforts et, grâce à ces mécanismes, obtenir les meilleurs résultats pour les ressources disponibles.

MND Cyber Playbook
A DND/CAF Perspective

This brief document aims to provide DND/CAF thoughts to the MND on potential areas of discussion within the GoC on improving our collective resilience in cyberspace and the ability to deter aggression, offer options to Government, support our ability to carry out all authorized missions, and remain a reliable coalition partner.

There are indications that the GoC Cyber Strategy will undergo a review led by PS. This work should be supported with a view to crafting a comprehensive update with input from across the stakeholders, including DND/CAF. Issued in 2010, and amended somewhat in 2018 to announce the CSE Act and CCCS, the situation that underpinned the strategy has evolved significantly in the intervening years and much has been learned. A revised strategy could refresh the GoC position, plans and priorities in cyberspace.

DND/CAF has been working to understand the cyber domain and develop plans to respond for a decade. A number of broad themes have emerged that encompass many of the observations and trends that have been noted over time. They are:

- Deterrence through Resilience. This term is borrowed from the US but resilience has become a major thrust within Canada and with our allies (reference US Executive Order 14028 and NATO Strengthened Resilience commitments) that could be reflected in Canadian priorities. This is much larger than DND/CAF; our concern centers on our own networks, platforms and weapons systems but the potential to reduce domestic requests for assistance (which may or may not include DND/CAF) when the broader Canadian landscape suffers negative impacts from malicious cyber actors is important. This could include things like:
    - Understanding and strengthening Supply Chains
    - Protecting Critical Infrastructure
    - Misinformation Awareness Programs
    - Clarifying F/P/T/Municipal ARAs
    - Monitoring, Compliance (outcome based) and Enforcement (frameworks and legislation)
    - Risk mitigation frameworks such as the DND/CAF Cyber Mission Assurance framework that seeks to expose the risks of operating (weapons, platforms, IT systems, personal devices, etc.) in cyberspace and systematically accepting or mitigating these risks to ensure mission success.

- Better Understanding through Collaboration. Cyberspace is a relatively new domain but the MND clearly recognizes that it is a domain of warfare and operations that we need to understand. Allies have gone as far as declaring cyberspace a traditional domain of warfare to help with this understanding. As well as this broad understanding of the impacts of the domain, greater intelligence capacity and collaborations will be key to success. Greater intelligence acquisition, use and sharing should include:
    - Collaboration internal to the GoC.
    - Multi-lateral collaboration along existing and new cyber intelligence channels.
    - Engagements with industry (ISPs, duty/incentive to report incidents) and academia (domestic and allied).
    - Intelligence gain/loss assessments and frameworks across all stakeholders.

- Increased cyber intelligence capacity for DND/CAF integrated with DIER.
- Greater leveraging of traditional SIGINT capabilities to contribute to our understanding of the cyber domain.

- Coordinated Options and Responses. Providing the GoC with robust options through a broad capacity to respond will be essential moving forward. Canada needs to be active militarily in cyberspace to be relevant and interoperable with our allies and partners. The CAF has extant GoC direction to be more assertive in cyberspace, harden our defences, and to develop and conduct active (offensive) cyber operations. It should be noted that a cyber incident does not necessarily warrant a cyber response and vice versa. As well, there has been a perception that cyber actions by Western nations can spark rapid escalation;

  However, coupled with deterrence, deliberate planning and preparation (including capability development) in advance of hostilities is a key characteristic of successful cyber operations in the future. Given these factors, the following elements might be considered:
  - A clearly understood framework and established ARAs across all stakeholders to allow rapid decision-making and coordinated responses.
  - Normalizing planning, preparation, operations and responses through increased capacity, collaboration and communication.
  - Operational frameworks aligned with Canadian interests and key allies that include the cyber domain. Allies are increasingly calling for operational cooperation and seeking operational frameworks (Named Missions) that include robust cyber responses whether they are cyber-specific operations or supporting more conventional operations.
  - Maturing the concept of deterrence as a comprehensive set of actions across the key stakeholders. DND/CAF could provide a broad spectrum of deterrence options across all domains that would contribute to general deterrence in cyberspace that should be included in comprehensive plans.
  - Domestic response frameworks that place DND/CAF in a similar supporting role as all other DOMOPs (fires, floods, etc.).

- Capacity and Workforce Development. There will be a need to invest in the people, capabilities and processes to be able to do more for Canada in cyberspace. From resilience to defence to offensive capabilities, stakeholders, including DND/CAF will need to recruit, train, employ and retain cyber professionals. DND/CAF has a force development plan that extends outs to 2035. This plan will require resources over time to build a military Cyber Force capable of executing operations in the cyber domain in the same manner (but perhaps not scale) that traditional services execute operations in the land, air, and maritime domains and come together jointly to achieve greater outcomes in support of GoC authorized missions.

Final Thought: Cyber is a team sport. Whether we are looking internal to DND/CAF, within the GoC or externally with our partners, no one entity protects Canada and Canadian interests in cyberspace. We all need to be doing more, collaborating our efforts closely and, through these mechanisms, delivering the greatest outcomes for the available resources.