Remarks to the Standing Committee on National Defence
Study on Cybersecurity and Cyberwarfare
Committee Appearance

March 10th, 2023 08:45, Ottawa (in person)

Check Against Delivery

(FRENCH FOLLOWS BELOW)

Good morning. Thank you for the invitation to appear before this committee.
Today, I will provide you with the perspective of the Canadian defence and security industry and the subset of companies that make up Canada's cybersecurity industry.
Canada's cybersecurity industry is world-class. According to studies carried out by ISED and Statistics Canada, between 2018 and 2020 the sector grew over 30% in terms of employment, R&D activity, and revenue. It is a fast-growing, global sector expected to quickly outpace traditional IT in spending.
However, only 8% of the sector's revenue is derived from Canadian government contracts. Eight percent.
The sector sells three times as much to our Five Eyes allies as it does to the Canadian government. Those numbers speak to a central challenge we face in this country when it comes to cyber: our allies see more value in Canada's cybersecurity sector than Canada does. Something is wrong with that picture.
So, one side of the coin is Canada needs to acquire more from our own industrial base, using procurement as a policy lever to drive innovation and build scale in Canadian businesses. The other side of the coin is Canada needs to procure at the "speed of cyber." A slow procurement process is a recipe for buying out of date or even obsolete cyber technology. Innovation cycles in this domain are measured in months, or even weeks.
Resolving these issues boils down to one word: collaboration. Canada requires a much greater degree of co-operation, knowledge sharing, and co-development between government and the private sector.
Some positive steps have been taken toward this, but we're nowhere near where we need to be. While agencies like CSE are very capable, CADSI's research has shown our government falling behind our allies when it comes to working with the sector in an institutionalized way. Our allies are collaborating with industry in real-time right now in Ukraine.
The Canadian government needs to establish a recurring forum for dialogue and discussion on cyber issues with all the key players - industry; DND /CAF; CSE; CCCS; GAC; and Public Safety Canada - at the table.
Canada also needs improved systems for threat-sharing that combine open sources with government and industry sources of information about breaches, indicators, and potential responses. This will mean rationalizing what is unclassified and what remains classified and who has access to what. Again, our allies are on the forefront of this type of activity.
We should consider sandboxes and collaborative lab spaces to test new technologies and capabilities together at scale and talent exchanges between the public and private sectors like the UK's Industry 100 program and a new talent exchange just launched by CSE. That could start to address the cyber talent shortages that we're all facing because cannibalizing each other isn't going to work. Reservists with cyber

and computing skills that are employed by companies could be an attractive way to support re-constitution of the CAF, so long as the government does not claim the IP and patents that reservists create while employed in the private sector.
It is also important to note that the broader defence industrial base or DIB - which includes companies making everything from satellites to ships - has become a prime target for cyber threat actors. Companies are increasingly incorporating technologies like artificial intelligence into their products; we know that countries like China and Russia will pursue Canada's AI through all available vectors.
Canada's DIB is closely integrated with the CAF and the American DIB. What we do in this sector is highly valuable and that makes us vulnerable given that ninety percent of Canadian defence companies are SMEs. Many lack the ability to defend themselves against a state-sponsored cyberattack.
There is a growing requirement to secure Canadian defence companies large and small. The Americans are not surprisingly ahead of us. Very soon, a demanding and mandatory cybersecurity standard will start appearing in Pentagon defence contracts. This is known as the Cybersecurity Maturity Model Certification, or CMMC.
CADSI has argued that Canada should adopt this standard by reference. CMMC will likely become a de facto Five Eyes, if not global, standard for defence firms. Taking time to contemplate a separate standard in Canada could become a competitive disadvantage for us and a non-tariff trade barrier. And while CMMC is new, other regulations need modernization for cyber and that needs to be done with industry at the table since we're at the technological bleeding-edge.
In conclusion, effective cyber defence at national levels is a team sport. If our allies can get this, why can't we?
Thank you. I will be pleased to take your questions.

FRENCH

Bonjour. Merci de m'avoir invitée.
Aujourd'hui, je vous donnerai le point de vue de l'industrie canadienne de la défense et de la sécurité, et du sous-ensemble des entreprises qui forment l'industrie canadienne de la cybersécurité.
L'industrie canadienne de la cybersécurité est de classe mondiale. Selon des études effectuées par ISDE est Statistique Canada, entre 2018 et 2020, le secteur a connu une croissance de plus de 30 % en ce qui a trait à l'emploi, à la recherche-développement et aux revenus. Il s'agit d'un secteur mondial qui croît rapidement et qui devrait dépasser rapidement les TI traditionnelles en termes de dépenses.
Toutefois, seuls 8 % des revenus du secteur de la cybersécurité dérivent des contrats du gouvernement. Huit pour cent.
Le secteur fait trois fois de vente auprès de nos alliés du Groupe des cinq qu'auprès du gouvernement du Canada. Ces chiffres montrent un défi central auquel notre pays est confronté en matière de cyberdéfense : nos alliés voient plus de valeur dans le secteur de la cybersécurité que le Canada. Quelque chose cloche dans cette image.
Donc, d'un côté, nous avons le Canada qui a besoin de faire plus d'acquisitions auprès de sa propre base de la cyberindustrie, en utilisant l'approvisionnement comme levier politique pour stimuler l'innovation et pour faire croître les entreprises canadiennes. De l'autre côté, le Canada a besoin de faire des acquisitions à une vitesse « cybernétique ». Un processus d'acquisition lent est le moyen parfait pour acheter des cybertechnologies désuètes, voire obsolètes. Les cycles d'innovation dans ce domaine se mesurent en mois et même en semaines.
La résolution de ces problèmes se résume en un mot : collaboration. Le Canada a besoin d'un plus grand degré de coopération, de partage de connaissances et de développement en collaboration entre le gouvernement et le secteur privé.
Nous avons pris des mesures concrètes en ce sens, mais nous ne sommes absolument pas rendus là où nous devrions l'être. Des agences comme le CST ont les capacités voulues, mais la recherche de CADSI a montré que notre gouvernement est loin derrière nos alliés lorsqu'il est question de collaboration avec le secteur

d'une manière institutionnalisée. Nous pouvons voir nos alliés collaborer avec l'industrie en temps réel avec la guerre en Ukraine.
Le gouvernement du Canada doit établir un forum permanent pour le dialogue et la discussion sur les questions cybernétiques avec tous les principaux intervenants : l'industrie, le ministère de la Défense nationale et les Forces armées canadiennes, le Centre de la sécurité des télécommunications du Canada, Affaires mondiales Canada, et Sécurité publique Canada.
Le Canada a aussi besoin de systèmes améliorés de partage des menaces qui combinent les sources de données ouvertes avec celles du gouvernement et de l'industrie à propos des effractions, des indicateurs et des réponses possibles. Il s'agira de rationaliser ce qui n'est pas classifié et ce qui reste classifié et qui a accès à quoi. Encore une fois, nos alliés sont à l'avant-garde de ce type d'activité.
Nous devrions envisager d'utiliser les bacs à sable et les laboratoires collaboratifs pour tester ensemble les nouvelles technologies et les capacités à l'échelle et l'échange de talents entre les secteurs public et privé comme le fait le programme Industry 100 au Royaume-Uni et le nouvel échange de talent qui vient d'être lancé par le CST. Cela pourrait permettre de remédier aux pénuries de cybertalents qui sévissent partout, parce que le fait de se cannibaliser mutuellement ne fonctionnera pas. Le recours aux réservistes ayant des compétences en cybernétique embauchés par des entreprises pourrait constituer un moyen attrayant de soutenir la reconstitution des Forces armées canadiennes, pour autant que le gouvernement ne réclame pas la propriété intellectuelle et les brevets des réservistes pour la période où ils étaient embauchés par le secteur privé.
Il est également important de souligner que l'infrastructure industrielle de défense en général, qui englobe les entreprises qui fabriquent tout, des satellites aux navires, est devenue une cible de choix pour les cybermenaces. De plus en plus, les entreprises intègrent des technologies comme l'intelligence artificielle dans leurs produits. On sait que la Chine et la Russie peuvent s'intéresser à l'intelligence artificielle du Canada par tous les moyens disponibles.
L'infrastructure industrielle de défense canadienne est étroitement intégrée dans les Forces armées canadiennes et l'infrastructure industrielle de défense américaine. Ce que nous faisons dans ce secteur revêt une grande valeur et nous sommes extrêmement vulnérables, étant donné que 90 % des entreprises de défense canadiennes sont des petites ou moyennes entreprises. Bon nombre d'entre elles n'ont pas la capacité de se défendre contre une cyberattaque parrainée par un État.
Le besoin de sécuriser les entreprises canadiennes de défense, petites et grandes. Les Américains sont, sans surprise, en avance sur nous. Très bientôt, une norme contraignante et obligatoire sera appliquée à tous les contrats de défense du Pentagone. Il s'agit du Cybersecurity Maturity Model Certification, la CMMC.
CADSI a déjà affirmé que le Canada devrait adopter cette norme en référence. La CMMC deviendra fort probablement de fait la norme de référence du Groupe des cinq, voire une norme mondiale, des entreprises de défense. Prendre le temps d'envisager d'adopter une autre norme au Canada pourrait s'avérer être un désavantage pour les entreprises canadiennes et un obstacle au commerce libre de tarifs douaniers.
Et bien que CMMC soit nouveau, d'autres réglementations doivent aussi être modernisées pour le cyber et cela doit être fait avec l'industrie à la table puisque nous sommes à la pointe de la technologie.
En conclusion, une cyberdéfense efficace au niveau national est un sport d'équipe. Si nos alliés peuvent le faire, pourquoi pas nous?
Merci. Je vais maintenant répondre à vos questions.