Cybersécurité

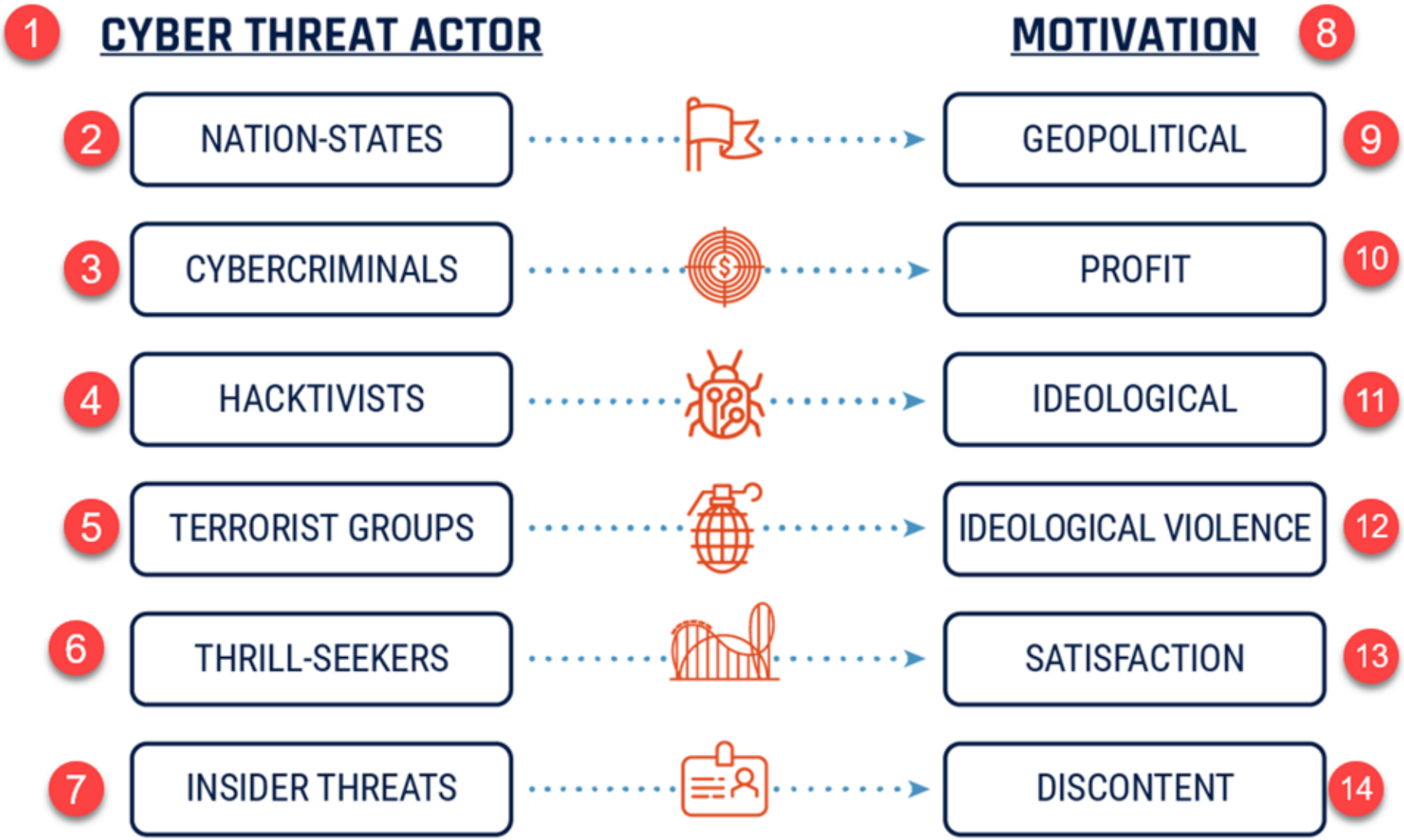
Présenté par Marc Baril

Directeur, Services d’affrètement maritime et d’initiatives stratégiques

Surface de cybermenace

- Tous les points d’extrémité accessibles qu’un auteur de menace peut tenter d’exploiter dans les appareils connectés à Internet dans l’environnement de cybermenace.

Cybermenaces

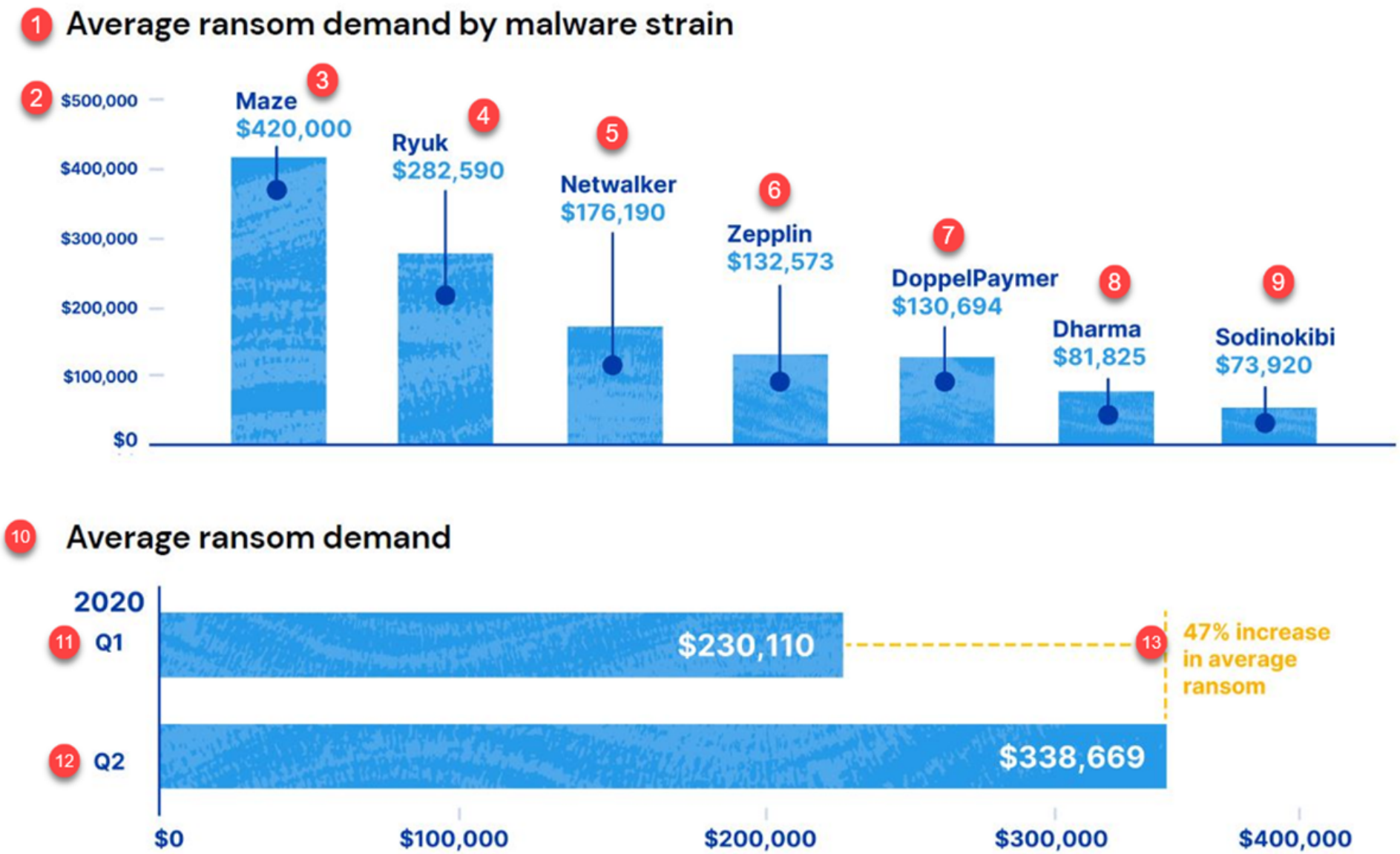


Information du Centre canadien pour la cybersécurité (CCC)

- Le nombre d'**auteurs de cybermenaces** augmente et les auteurs deviennent de plus en plus « sophistiqués ».
- La **cybercriminalité** est la cybermenace la plus susceptible de toucher les Canadiens.
- Les **rançongiciels** dirigés contre le Canada continueront presque certainement de cibler les fournisseurs d'infrastructures essentielles.
- Bien que la cybercriminalité soit la menace la plus probable, les **programmes parrainés par l'État** en Chine, en Russie, en Iran et en Corée du Nord constituent les plus grandes menaces stratégiques pour le Canada.
- Les auteurs de cybermenaces parrainés par l'État sont fort susceptibles de mettre au point des cybercapacités permettant de **perturber l'infrastructure essentielle canadienne**.
- Les auteurs de cybermenaces parrainés par l'État continueront presque certainement de faire de l'**espionnage commercial** au sein des entreprises, des universités et des gouvernements du Canada.

https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020

Le coût des rançongiciels (de Coalition Insurance Inc., Rapport des réclamations au 1er semestre de 2020)



Chaînes d’approvisionnement maritime

Menaces sur les chaînes d'approvisionnement : Cybercriminels et auteurs de cybermenaces parrainés par l’État

- Espionnage commercial visant les organisations maritimes aux fins suivantes :
  - reproduction illégale de la technologie;
  - intimidation (profit, etc.); et/ou
  - autres motifs.

Exemples :

En 2019, des événements parrainés par l’État ont ciblé des universités du Canada pour acquérir des technologies maritimes;

Nombreux exemples de rançongiciels affectant des compagnies maritimes, comme la société de transport maritime Maersk Line

Chaînes d’approvisionnement maritime

<u>Chaîne d’approvisionnement</u> – Les logiciels et le matériel risquent de faire l’objet de manipulations malveillantes avant d’être intégrés dans les systèmes opérationnels

<u>Renseignements sensibles</u> – Votre propriété intellectuelle et les informations susceptibles d’avoir un impact sur la sécurité nationale sont ciblées dans vos réseaux

Ce que nous faisons

- Élaboration de procédures d’opérations d'urgence et de plans d’intervention en cas d’incident de cybersécurité, conformément à la résolution MSC.428 (98) de l’OMI sur les cyberrisques maritimes (2017)

- Collaboration avec d’autres partenaires fédéraux canadiens et américains à des approches communes en matière de cybersécurité maritime
  - Élaboration d’alertes pour transmettre des informations sur la cybersécurité maritime aux navigateurs dans des situations d’urgence afin d’assurer la sécurité et la sûreté des voies navigables

- Évaluation des besoins d’un programme de cybercertification

Que font les États-Unis? – Programme « Cybersecurity Maturity Model Certification » (CMMC) [Certification du modèle de maturité de la cybersécurité]

- **<u>Programme de cybercertification pour les contrats du département de la Défense des États-Unis</u>**
  - Janvier 2020 – Publication des détails du modèle de maturité v1.0 et annonce de l'organisme d'accréditation
  - Novembre 2020 – Lancement officiel du nouveau règlement « Defense Federal Acquisition Regulation Supplement » (DFARS), introduction de la certification CMMC dans la législation
  - Janvier 2021 – Les acteurs de l'industrie - quel que soit leur pays d'origine - doivent être certifiés en matière de cybersécurité pour pouvoir obtenir un contrat du département de la Défense (y compris les sous-traitants).
    - Mise en œuvre progressive – Tous les nouveaux contrats du département de la Défense contiendront des exigences de CMMC d'ici à l'année financière 2026.
    - 15 contrats pilotes appliqueront le programme CMMC en 2021 (les États-Unis indiquent qu'il n'y a pas d'entreprises étrangères dans ces chaînes d'approvisionnement), 75 contrats en 2022.

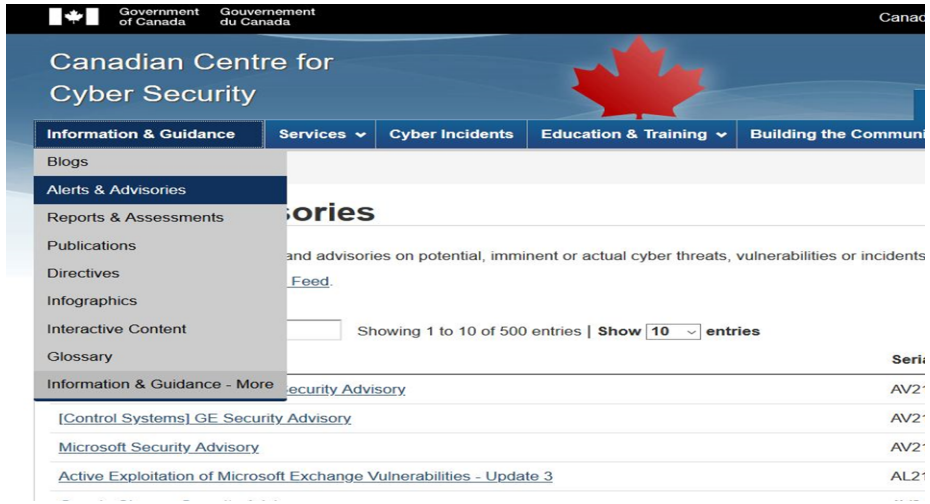
- Le gouvernement du Canada évalue les options pour répondre aux exigences de cybersécurité de la chaîne d'approvisionnement dans le contexte du programme CMMC.

Que pouvez-vous faire?

- Gouvernance interne
  - La cybersécurité est-elle une priorité maintenue? Quelqu'un est-il vraiment responsable?
  - Résolution MSC.428 (98) de l'OMI sur les cyberrisques maritimes (2017) – veiller à ce que les cyberrisques soient pris en compte de manière appropriée dans les systèmes de gestion de la sécurité des entreprises
  - Tenir compte des pratiques de sécurité et de gestion des risques des normes telles que la norme NIST 800-161
- Investissement
  - Dans quelle mesure consacrez-vous des ressources à la cybersécurité?
- Résilience
  - À quel point êtes-vous préparé à une cyberattaque? Avez-vous un plan d'intervention en cas de cyberincident?
- Chaîne d'approvisionnement
  - Toutes les composantes de votre chaîne d'approvisionnement disposent-elles d'une cyberprotection adéquate? Ont-elles accès à votre réseau?
  - Envisagez la Gestion des risques de la chaîne d'approvisionnement (NIST 800-171)
- Collaboration
  - Collaborez avec des experts en cybersécurité dans le domaine commercial et tirez parti des conseils et des directives du GC

Les services que le Centre pour la cybersécurité peut fournir

- Alertes et avis
- Prise en charge des cyberincidents
- Analyse des logiciels malveillants
- Publications - Conseils et directives
- Cours
- Campagne de sensibilisation « Pensez cybersécurité »
- Appels communautaires comme le « Transport Sector Cyber Community Call » (TSC3) (Appel à la cybercommunauté du secteur des transports)
- Enquêtes sur la posture de cybersécurité
- Outils – Renseignements sur les menaces, analyse des logiciels malveillants, avis de vulnérabilité



La voie à suivre - Se préparer à une cyberattaque inévitable

- Les *10 meilleures mesures de sécurité des TI* du Centre canadien pour la cyberse
  - Par exemple, renforcer les systèmes d'exploitation, appliquer des correctifs aux systèm applications, cyberhygiène.

  https://cyber.gc.ca/fr/10-meilleures-mesures-de-securite-des-ti-0

- *Comprendre les cyber-risques* par Transports Canada

http://publications.gc.ca/collections/collection_2016/tc/T86-21-2016-eng.pdf

- Créer un plan d'intervention en cas d'incidents de cybersécurité basé sur le cadre de cybersécurité du National Institute of Standards and Technology (NIST)
  - Par exemple, identifier, protéger, détecter, intervenir, récupérer.

- Obtenir une certification en matière de cybersécurité offerte par des entreprises privées

- Signaler rapidement les événements au Centre canadien pour la cybersécurité et au Bureau de gestion des biens et services maritimes

Contacts pour la cybersécurité

- Centre canadien pour la cybersécurité
  - Pour obtenir de l'aide concernant le tri des cyberincidents, l'accès aux services ou des questions générales
  - 1-833-CYBER-88
  - contact@cyber.gc.ca
  - https://www.cyber.gc.ca/fr/
- Pour signaler un cybercrime :
  - GRC : www.rcmp-grc.gc.ca (ou votre service de police)
- Pour signaler une fraude :
  - Centre antifraude du Canada
  - 1-888-495-8501
  - https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

- Bureau de gestion des biens et services maritimes
  - marc.baril@tpsgc-pwgsc.gc.ca