CYBERTERRORISME ET PDMC

Brigadier-général (ret.) Gaston Côté
V-P Groupe DA
5 avril 2018

SUJETS COUVERTS

- La menace et vocabulaire militaire
- Préoccupations communes
- Conclusion

LA MENACE

LE **CYBERTERRORISME** PEUT SE DÉFINIR COMME L'ENSEMBLE DES ATTAQUES GRAVES (VIRUS, PIRATAGE, ETC.) ET À GRANDE ÉCHELLE, DES ORDINATEURS, DES RÉSEAUX ET DES SYSTÈMES INFORMATIQUES D'UNE ENTREPRISE, D'UNE INSTITUTION OU D'UN ÉTAT, COMMISES DANS LE BUT D'ENTRAÎNER UNE DÉSORGANISATION GÉNÉRALE SUSCEPTIBLE DE CRÉER LA PANIQUE.

UN VOCABULAIRE AGRESSIF

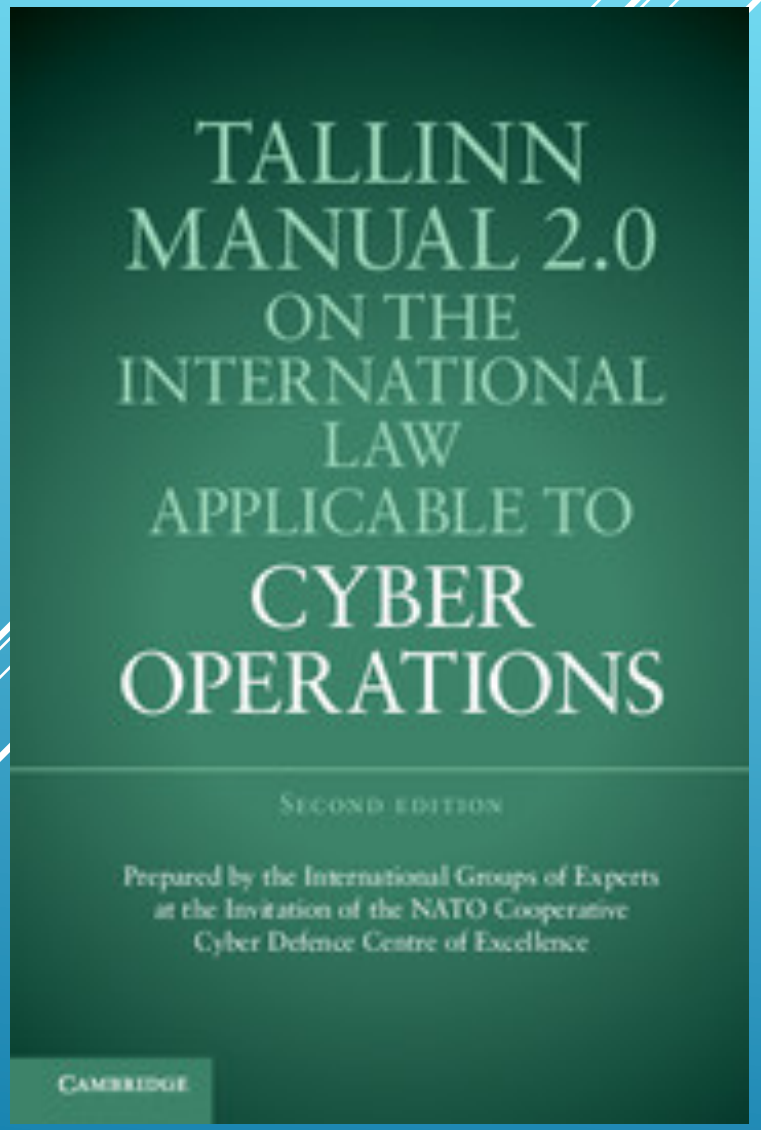
- Cyberespace
- Cyberguerre
- Cyberattaque
- Cyberterrorisme
- Des domaines réservées aux forces armées ?

LE CAS DE L'ESTONIE

- 2007 : attaques massives de déni de service (DDoS)
- Provenance des attaques : plus de 178 endroits différents avec l'aide des botnets
- Pas capable de confirmer si l'attaque provenait d'un état
- Pas de victimes sauf que effondrement des moyens de communication gouvernement/citoyens, accès aux guichets bancaires, etc.
- Pertes de dossiers des banques

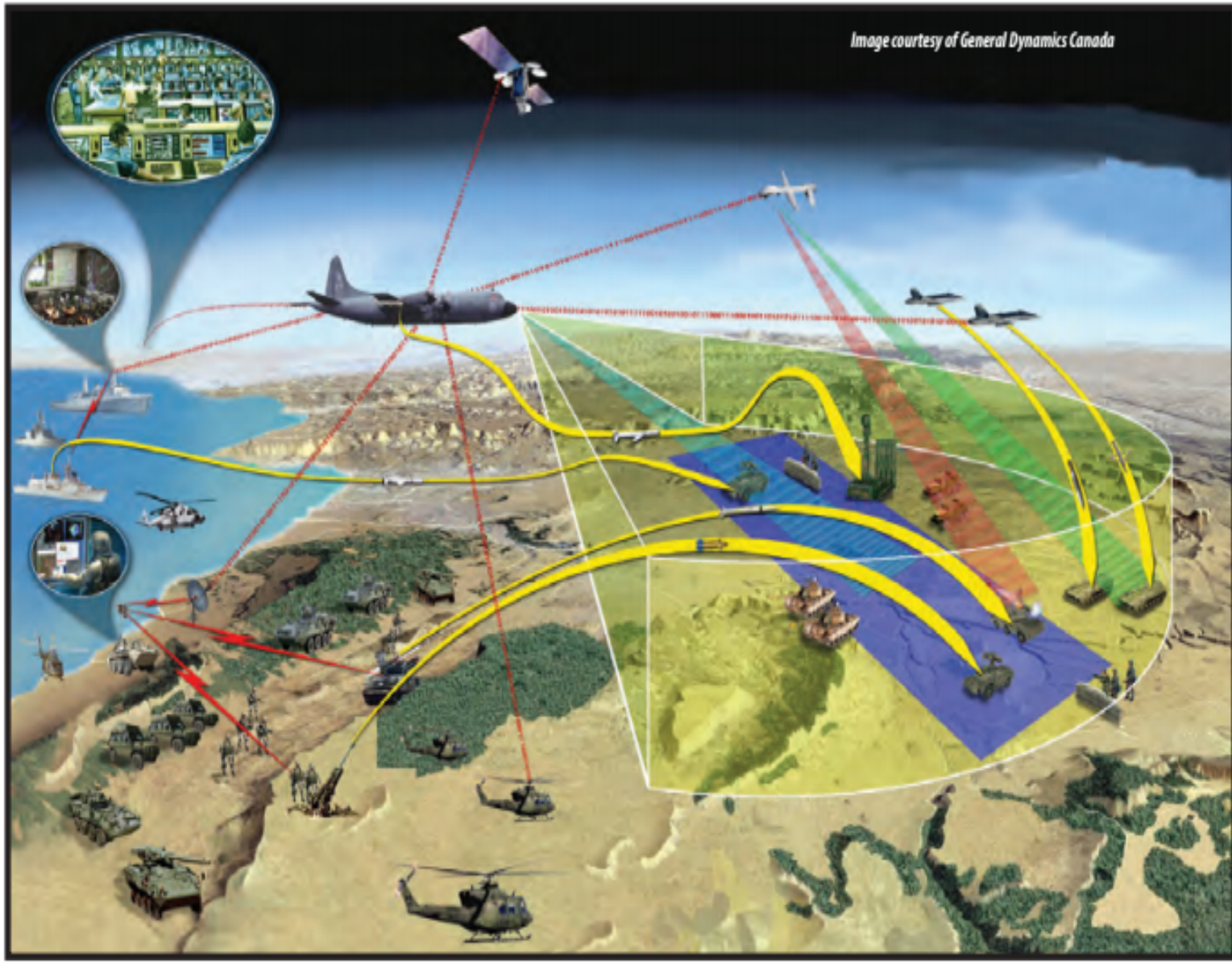
RÉACTIONS

- OTAN : article 5 de la Charte de l'OTAN
- La cyberdéfense fait partie de cette tâche fondamentale de l'OTAN qu'est la défense collective.
- 2016, afin de faire de l'amélioration des moyens de cyberdéfense une priorité.
- Tallinn 2,0



DÉPLOIEMENT MILITAIRE

- Développement technologique de tous les systèmes d'armes
- Utilisation du cyberespace
- *Guerre réseau-centrique*
- Multiplicateur de force
- Expérience récente
- Vulnérables même si ces systèmes ne sont pas sur l'internet ('air-gap')



GROUPE DA INTERNATIONAL

SECURISATION
INVESTIGATION
PROTECTION

EN GARNISON

RÉACTIONS - CANADA

- Le projet d'architecture de cybersécurité
  - infrastructure générale en matière de technologie de l'information
  - l'exécution d'opérations automatisées dans l'ensemble du cyber terrain
  - systèmes d'armes des FAC, des systèmes de commandement et contrôle et des systèmes d'entreprise
  - $249M

RÉACTIONS – CANADA (2)

- Défense des réseaux informatiques
  - détection et l'analyse de tous les activités cybernétique suspectes
  - Support au processus de prise de décision pour les opérations de défense cybernétique
  - Intégration avec le projet Commandement et contrôle de réseau et capacité intégrée de connaissance de la situation
  - Temps de réaction plus rapide et automatisation de réponses prédéterminés
  - $99M

RÉACTIONS – CANADA (3)

- Création du métier de cyberopérateur
- Gestion de réseau
- Détection et protection contre les intrusions
- Protection lors de déploiements

PRÉOCCUPATIONS COMMUNES

- Le cyberterrorisme est une réalité et frappe autant les civils que les cibles militaires
- Les logiciels malveillants prolifèrent
- Besoins modestes, anonymat, localisation, monnaies numériques = pas nécessairement un état coupable!
- Peu importe le motif ou l'auteur de l'attaque, les dégâts et les coûts sont ÉNORMES

PRÉOCCUPATIONS COMMUNES MILITAIRE – CIVILE - 2

- Possibilité de faire des gains financiers FACILES (Ransomware)
- Cybercrime-as-a-service sert les groupes criminels, les groupes terroristes, les états voyous
- Alliance filière criminelle et groupes terroristes = facilite l'utilisation de la cyberespace

PRÉOCCUPATIONS COMMUNES MILITAIRE – CIVILE - 3

- Hésitation à rapporter les cyberattaques
- Le remboursement par l'assurance élimine ni le risque ni le problème de sécurité
- Barrières informatique (logiciels de protection, mots de passe, etc.) contournées par une seule intervention humaine!
- Défi de l'informatique quantique

QUELQUES CAS

- La technologie n'est pas le seul moyen
- Cyberattaque frappant le Pentagone = la pire attaque sur les systèmes informatiques de l'histoire. Quatorze mois pour nettoyer les réseaux militaires du logiciel malveillant (malware)
- STUXNET
- Avez-vous un plan pour contrer la menace la plus insidieuse : LA MENACE INTERNE

NOTE – BULLETIN DE SÉCURITÉ

- Le Canada se situe au deuxième rang!

”

Source : Global Cybersecurity Index 2017

NOTE – BULLETIN DE SÉCURITÉ

- Le Canada se situe au deuxième rang!
  - ….sur trois pays d'Amérique du Nord
- Mais il se situe au 20ième rang mondial
- Critères utilisés : législation, soutien technique, organisation, renforcement des capacités, coopération

Source : Global Cybersecurity Index 2017

CONCLUSION

- Cyberterrorisme est une réalité
- Les cyberterroristes sont très futés, très ingénieux et innovent sans cesse
- La menace touche toutes les facettes d'une société numérisée
- Le Canada doit promouvoir une meilleure concertation de tous les milieux afin de mieux se protéger
- Action canadienne un peu tardive
- N'oublions pas que derrière ces machines, il y a toujours un être humain avec toutes les forces …et les faiblesses
- Pour les militaires …il faut toujours se souvenir que notre équipement provient du plus bas soumissionnaire…

,,


QUESTIONS ?

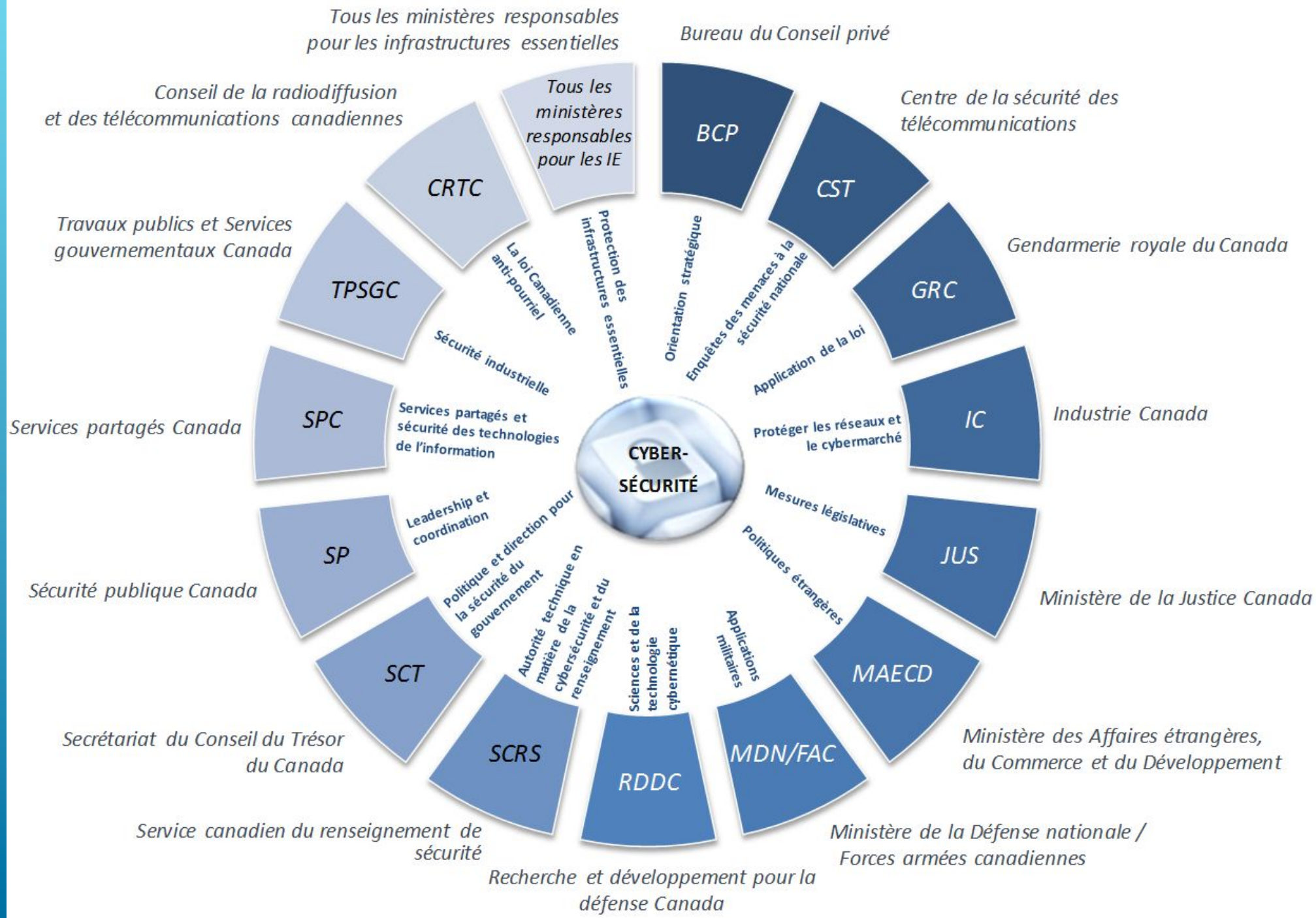
BREF RAPPEL HISTORIQUE

- 1988 : APPARITION DU VER MORRIS (du nom de son ‘inventeur’ Robert Morris)
- 2007 : Déni de service des réseaux gouvernementaux de l’Estonie
- 2014 : invasion de la Crimée, véritable laboratoire

GROUPE DA
INTERNATIONAL
SECURISATION
INVESTIGATION
PROTECTION

CONTRER LA MENACE INTERNE

- Restreindre les privilèges d'accès
- Contrôle des appareils vs BYOD
- Définition des données sensibles
- Contrôle des appareils de communication
- Entraînement et formation des employés
- Procédure d'urgence en cas de bris de sécurité accidentel
- Que faire avec les employés qui ont quitté récemment ? Les frustrés et les compétiteurs éventuels ?

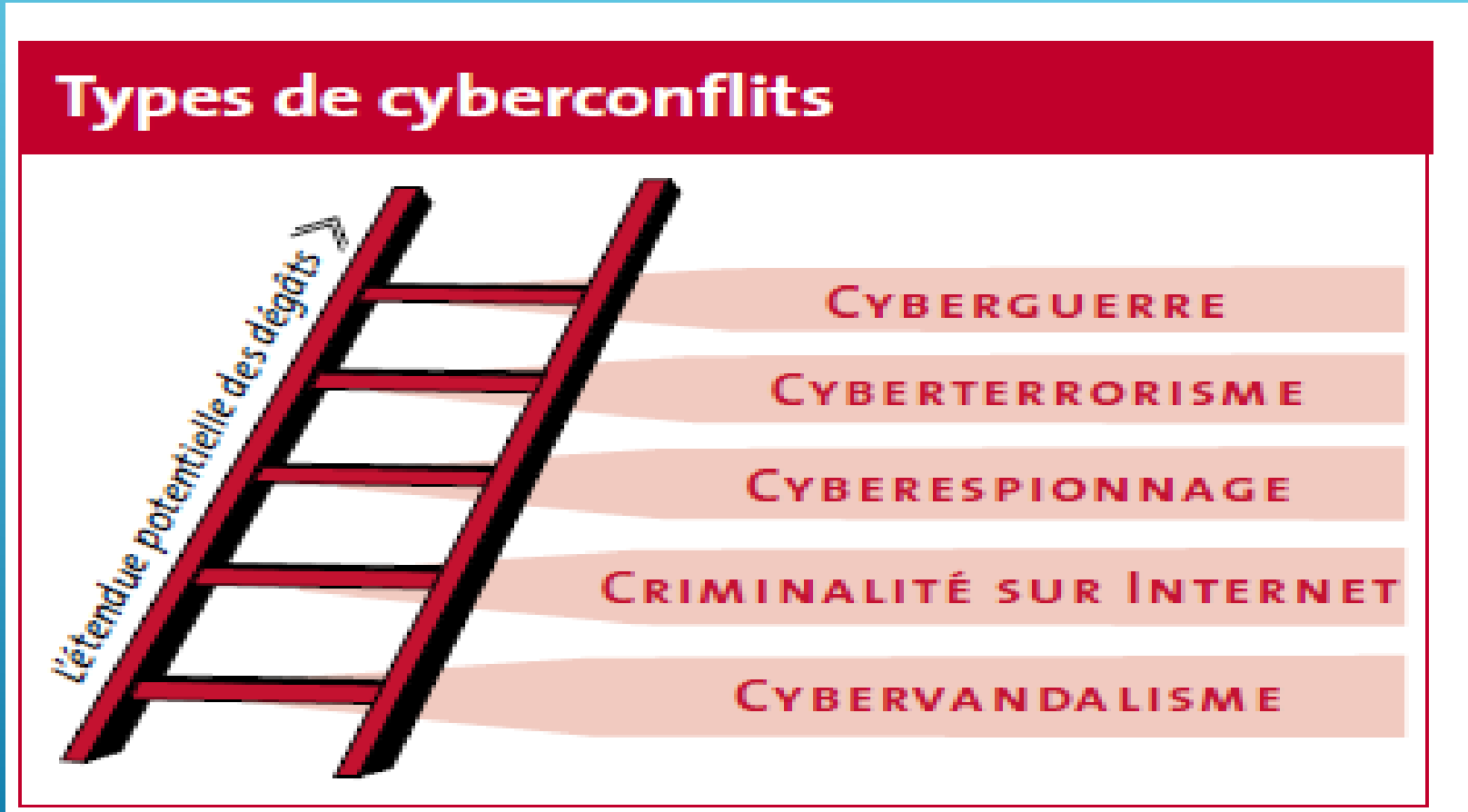

Tous les ministères responsables pour les infrastructures essentielles
Bureau du Conseil privé
Conseil de la radiodiffusion et des télécommunications canadiennes
Centre de la sécurité des télécommunications
Travaux publics et Services gouvernementaux Canada
Gendarmerie royale du Canada
Services partagés Canada
Industrie Canada
Sécurité publique Canada
Ministère de la Justice Canada
Secrétariat du Conseil du Trésor du Canada
Ministère des Affaires étrangères, du Commerce et du Développement
Service canadien du renseignement de sécurité
Ministère de la Défense nationale / Forces armées canadiennes
Recherche et développement pour la défense Canada
Tous les ministères responsables pour les IE
BCP
CST
GRC
IC
JUS
MAECD
MDN/FAC
RDDC
SCRS
SCT
SP
SPC
TPSGC
CRTC
Protection des infrastructures essentielles
Orientation stratégique
Enquêtes des menaces à la sécurité nationale
Application de la loi
Protéger les réseaux et le cybermarché
Mesures législatives
Politiques étrangères
Applications militaires
Sciences et de la technologie cybernétique
Autorité technique en matière de la cybersécurité et du renseignement
Politique et direction pour la sécurité du gouvernement
Leadership et coordination
Services partagés et sécurité des technologies de l'information
Sécurité industrielle
La loi Canadienne anti-pourriel
CYBER-SÉCURITÉ

Centre canadien de réponse aux incidents cybernétiques (CCRIC)

- Principes de prévention contre les menaces sophistiquées et persistantes : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-002-fr.aspx
- Formation, orientation et conseils techniques en matière de cybersécurité : http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-fr.aspx
- Principes de prévention contre les attaques par déni de service : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-fr.aspx
- Guide Pensez cybersécurité pour les petites et moyennes entreprises : http://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx
- Guide de rétablissement à la suite d'une infection par un logiciel malveillant : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2011/tr11-001-fr.aspx
- Systèmes SCADA et SCI : http://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-fr.aspx

PRÉOCCUPATIONS COMMUNES

MILITAIRE - CIVILE



SOURCE : CENTER FOR SECURITY STUDIES (CSS),ZURICH

GROUPE DA
INTERNATIONAL
SECURISATION
INVESTIGATION
PROTECTION

LEGAL

Cybercriminal Legislation, Substantive law,
Procedural cybercriminal law,
Cybersecurity Regulation.

TECHNICAL

National CIRT, Government CIRT, Sectoral CIRT,
Standards for organisations,
Standardisation body.

ORGANIZATIONAL

Strategy,
Responsible agency,
Cybersecurity metrics.

CAPACITY BUILDING

Public awareness, Professional training,
National education programmes, R&D programmes,
Incentive mechanisms, Home-grown industry.

COOPERATION

Intra-state cooperation, Multilateral agreements,
International fora, Public-Private partnerships,
Inter-agency partnerships.

“

ID SGPM 00378 CYBEROPÉRATEUR (CYBEROP)
FONCTIONS GÉNÉRALES :

UN CYBEROPÉRATEUR RÉUNIT ET ANALYSE DES DONNÉES PROVENANT DE SYSTÈMES INFORMATIQUES RÉSEAUTÉS DES FAC POUR APPUYER DES OPÉRATIONS RÉSEAUTÉES DE DÉFENSE, AUSSI BIEN LORS D’UN DÉPLOIEMENT QUE NON. IL SURVEILLE UN RÉSEAU À L’AFFÛT DE TOUTE INTRUSION OU ANOMALIE ÉVENTUELLE ET EXAMINE LA VULNÉRABILITÉ D’UN RÉSEAU TANT EN POSITION DÉFENSIVE QU’OFFENSIVE. IL SOUMET CERTAINS INCIDENTS À UNE ENQUÊTE CYBERCRIMINALITÉ ET ASSURE LA MAINTENANCE DE CYBEROUTILS SPÉCIALISÉS PROPRES À CE GPM.

”