Cybersecurity

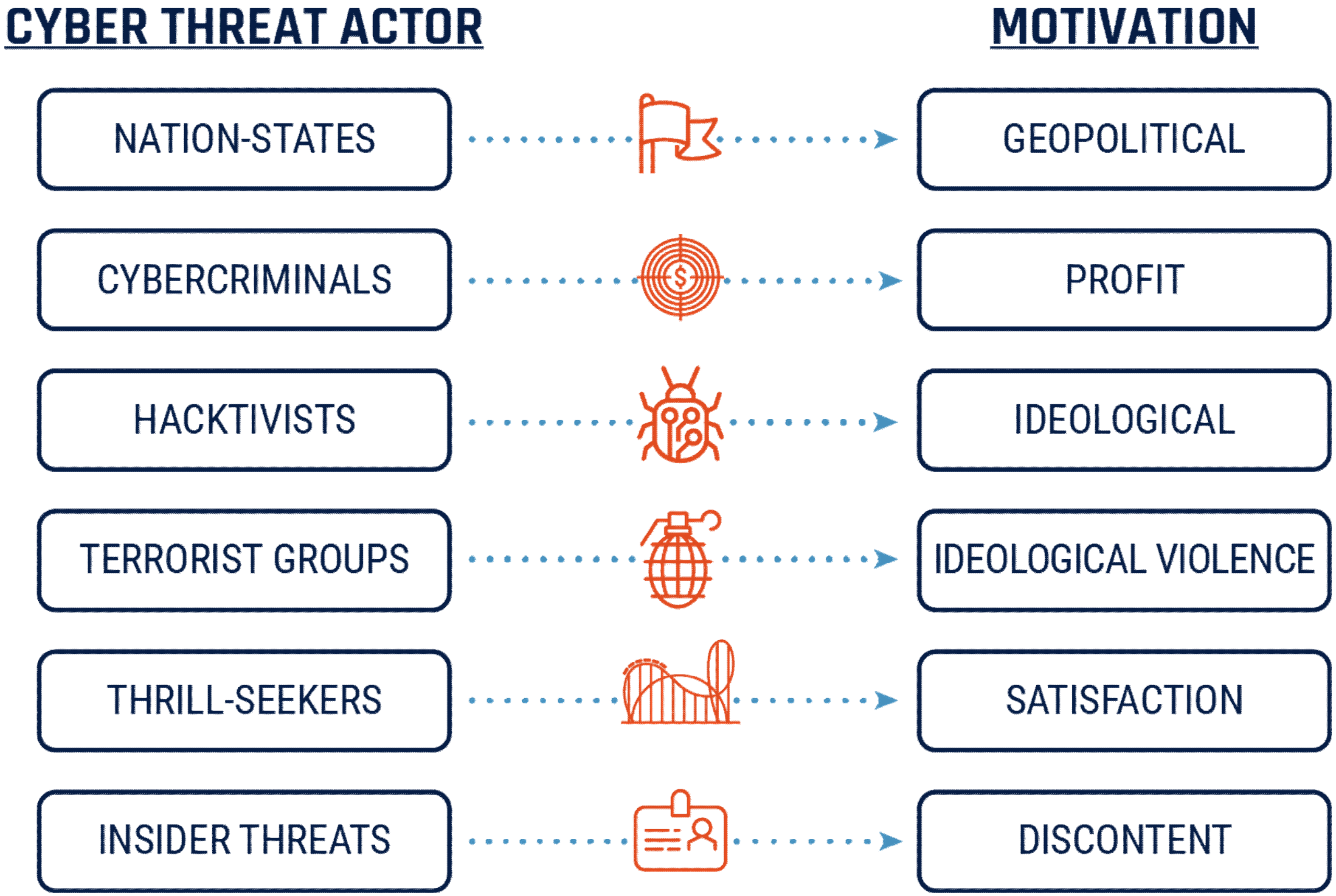
Presented by Marc Baril

Director Marine Chartering and Strategic Initiatives

The Cyber Threat Surface

- All the available endpoints that a threat actor may attempt to exploit in Internet-connected devices within the cyber threat environment.

Cyber Threats



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

From the Canadian Centre for Cyber Security (CCCS)

CANADIAN CENTRE FOR CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2020

Communications Security Establishment

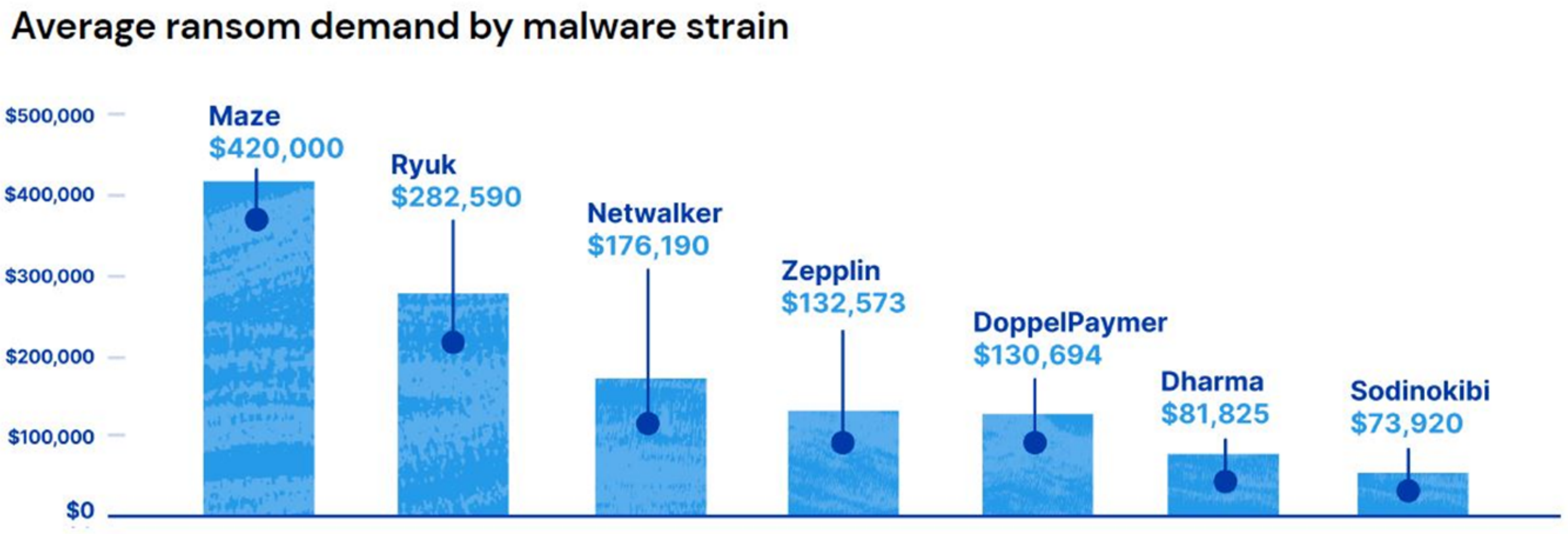
Centre de la sécurité des télécommunications

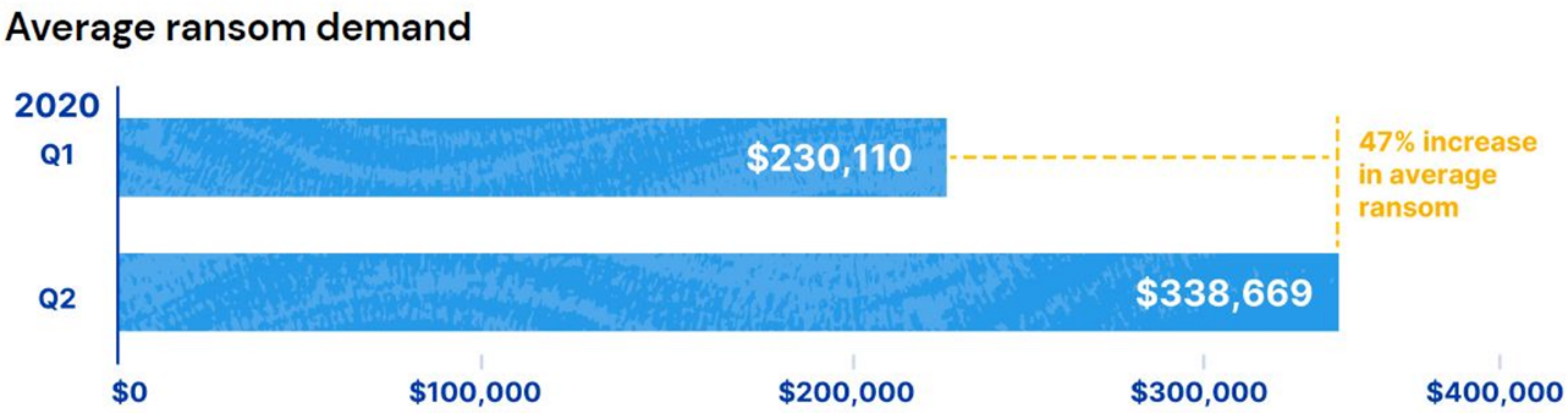
Canada

- The number of **cyber threat actors** is rising/more sophisticated.
- **Cybercrime** is the cyber threat that is most likely to affect Canadians
- **Ransomware** directed against Canada will almost certainly continue to target critical infrastructure providers.
- While cybercrime is the most likely threat, the **state-sponsored programs** of China, Russia, Iran, and North Korea pose the greatest strategic threats to Canada.
- State-sponsored actors are very likely attempting to develop cyber capabilities to **disrupt Canadian critical infrastructure**.
- State-sponsored actors will almost certainly continue to conduct **commercial espionage** against Canadian businesses, academia, and governments.

https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2020

The Cost of Ransomware (From Coalition Insurance Inc, H1 2020 Claims report)





Maritime Supply Chains

Supply Chains Threats: Cybercriminals and State-sponsored actors

- Conduct commercial espionage on maritime organizations for:
  - illegal reproduction of technology;
  - for intimidation (profit etc.); and/or
  - Other reasons.

Examples:

2019 state-sponsored events targeted universities in Canada to acquire maritime technology;

Numerous ransomware examples affecting maritime companies such as Maersk Line shipping

Maritime Supply Chains

<u>Supply chain</u> - Software and hardware are at risk of malicious tampering before they are integrated in operational systems

<u>Sensitive Information</u> – Your intellectual property and information that may impact national security is targeted in your networks

What we are doing

- Developing Emergency Operations Procedures, Cybersecurity Incident Response Plans to meet IMO Resolution MSC. 428 (98) on Maritime Cyber Risk (2017)

- Collaborating with other Canadian and American federal partners on common maritime cybersecurity approaches
  - Developing alerts to pass on maritime cyber security information to mariners in emergency situations to ensure safety and security of waterways

- Assessing the needs for a Cyber certification program

What is the US doing? –
Cybersecurity Maturity Model Certification program (CMMC)

- **Cyber certification program for US Department of Defense (DoD) Contracts**
  - January 2020 – Maturity Model details v1.0 released and Accreditation Body announced
  - November 2020 – New Defense Federal Acquisition Regulation Supplement (DFARS) rule officially launches, CMMC in legislation
  - Jan 2021 - Industry actors - regardless of country of origin must be cybersecurity certified to be eligible to win any DoD contract (includes sub-contractors)
    - Phased rollout – All new DoD contracts will contain CMMC requirements by FY2026
    - 15 pilot contracts will apply CMMC in 2021 (US state that there are no foreign companies in these supply chains), 75 contracts in 2022.

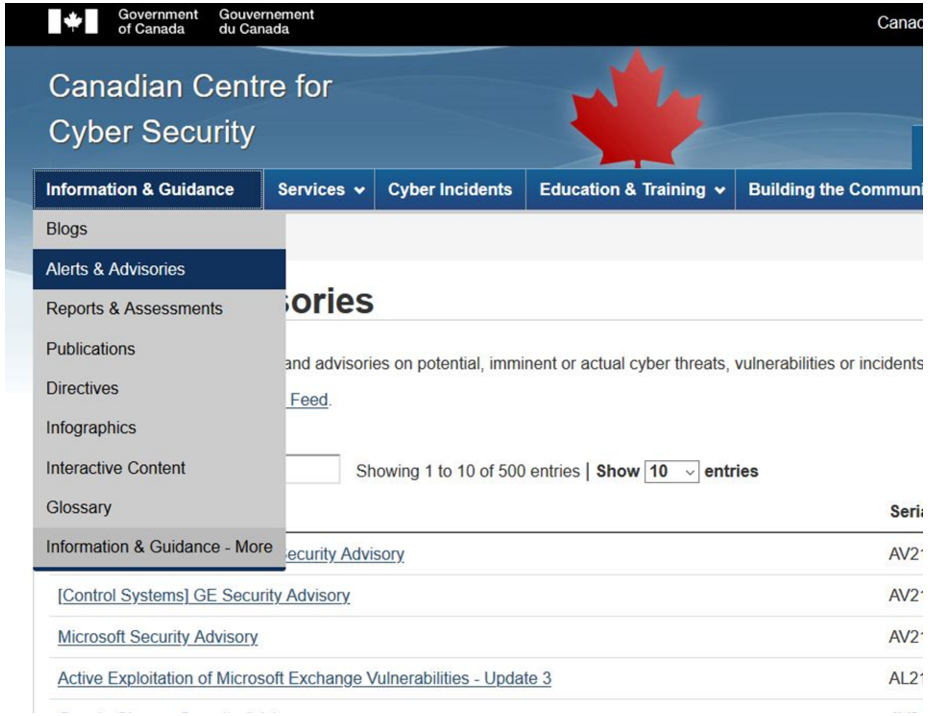
- Government of Canada is assessing options for how to address supply chain cybersecurity requirements in the context of CMMC

What can you do?

- Internal Governance
  - Is cyber security a maintained priority? Is someone definitely responsible?
  - IMO Resolution MSC. 428 (98) on Maritime Cyber Risk (2017) - ensures cyber risks are appropriately addressed in safety management systems by companies
  - Consider security and risk management practices of standards like NIST 800-161,
- Investment
  - How much are you focusing resources on cyber security?
- Resilience
  - How prepared are you for a cyber attack? Do you have a cyber incident response plan?
- Supply Chain
  - Do all components of your supply chain have adequate cyber protection? Do they have access to your network?
  - Consider Supply Chain Risk Management, NIST 800-171
- Collaboration
  - Work with commercial cyber experts and leverage GC advice and guidance

Services the Cyber Centre can provide

- Alerts & Advisories
- Cyber incident intake
- Malware analysis
- Publications – Advice and Guidance
- Courses
- GetCyberSafe awareness campaign
- Community Calls like the "Transport Sector Cyber Community Call" (TSC3)
- Cyber security posture surveys
- Tools – Threat info, malware analysis, vulnerability notifications



Government of Canada Gouvernement du Canada Canad

Canadian Centre for Cyber Security

Information & Guidance | Services | Cyber Incidents | Education & Training | Building the Communi

- Blogs
- Alerts & Advisories
- Reports & Assessments
- Publications
- Directives
- Infographics
- Interactive Content
- Glossary
- Information & Guidance - More

ories

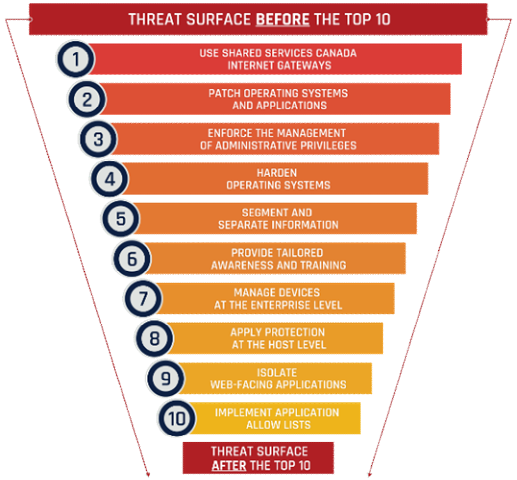
and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents

Feed.

Showing 1 to 10 of 500 entries | Show 10 entries

	Seri
ecurity Advisory	AV2
[Control Systems] GE Security Advisory	AV2
Microsoft Security Advisory	AV2
Active Exploitation of Microsoft Exchange Vulnerabilities - Update 3	AL2

Way Forward – Preparing for an Inevitable Cyber Attack



THREAT SURFACE **BEFORE** THE TOP 10

1 USE SHARED SERVICES CANADA INTERNET GATEWAYS

2 PATCH OPERATING SYSTEMS AND APPLICATIONS

3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

4 HARDEN OPERATING SYSTEMS

5 SEGMENT AND SEPARATE INFORMATION

6 PROVIDE TAILORED AWARENESS AND TRAINING

7 MANAGE DEVICES AT THE ENTERPRISE LEVEL

8 APPLY PROTECTION AT THE HOST LEVEL

9 ISOLATE WEB-FACING APPLICATIONS

10 IMPLEMENT APPLICATION ALLOW LISTS

THREAT SURFACE **AFTER** THE TOP 10

- *Top 10 IT Security Actions* by the Canadian Centre for Cybersecurity
  - E.g. harden operating systems, patch systems and apps, cyber-hygiene
  https://cyber.gc.ca/en/top-10-it-security-actions

- *Understanding Maritime Cyber Risk* by Transport Canada
http://publications.gc.ca/collections/collection_2016/tc/T86-21-2016-eng.pdf

- Create a Cybersecurity Incident Response Plan based off of the *National Institute of Standards and Technology's* Cybersecurity Framework
  - E.g. identify, protect, detect, response, recover

- Obtain Cybersecurity Certification offered by Private Companies

- Report events promptly to the Canadian Centre for Cybersecurity and to the Marine Commodity Management Office

Cyber Security contacts

- Canadian Centre for Cyber Security
  - For help with cyber-triage, access to services, general questions
  - 1-833-CYBER-88
  - contact@cyber.gc.ca
  - www.cyber.gc.ca
- To report a cybercrime:
  - RCMP: www.rcmp-grc.gc.ca (or your police-of-jurisdiction)
- To report Fraud:
  - Canadian Anti-Fraud Centre
  - 1-888-495-8501
  - www.antifraudcentre-centreantifraude.ca

- Marine Commodity Management Office:
  - marc.baril@tpsgc-pwgsc.gc.ca