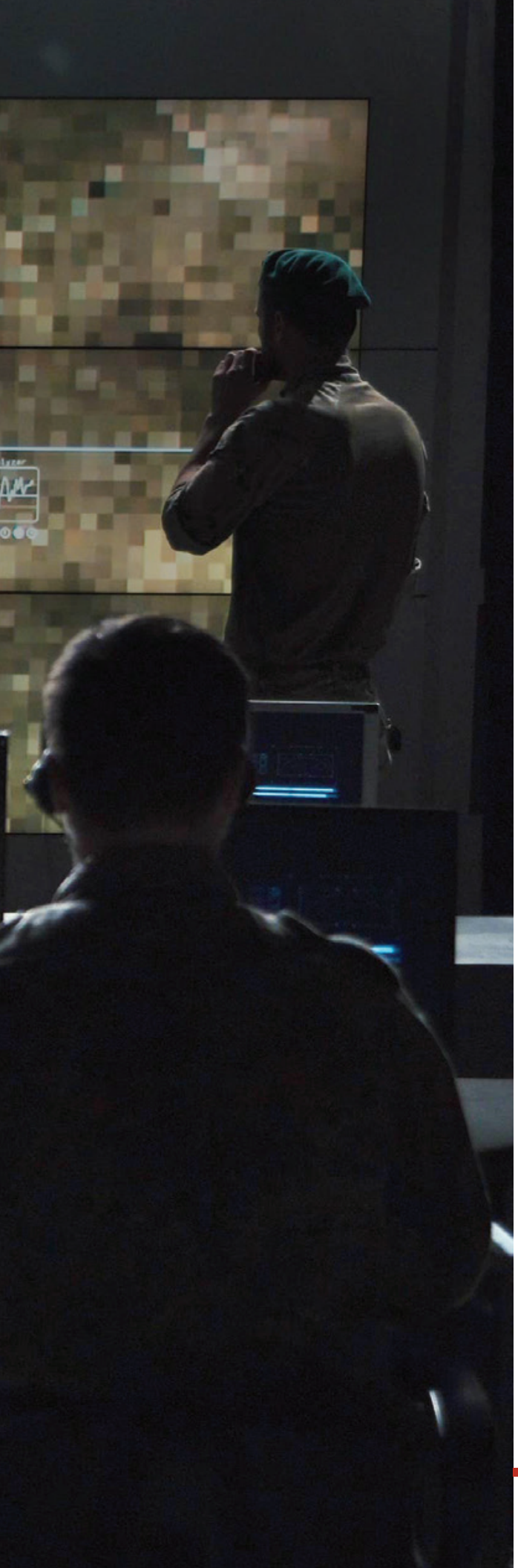
2019 REPORT

Canadian Association of Defence and Security Industries

FROM BULLETS TO BYTES: INDUSTRY'S ROLE IN PREPARING CANADA FOR THE FUTURE OF CYBER DEFENCE

TABLE OF **CONTENTS**



EXECUTIVE **SUMMARY**

Cyberwarfare will erase the distinction between home front and battlefront for Canadians and the Canadian Armed Forces (CAF). Both will be increasingly exposed to risks from the cyber domain in a way that will challenge our conceptions of domestic safety and international security. The rapid and growing rates of technological convergence and diffusion will empower criminal and state actors with capabilities to achieve military outcomes previously only possible by advanced nation states. Consequently, there is urgent need for the CAF to operate, defend and project power in the cyber domain.

CADSI's research – an extensive review of existing literature and policy frameworks in Canada and among allies, supplemented by 70 interviews with government, military and industry leaders in the field – suggests an overemphasis on resiliency, emergency management and disaster recovery, at the possible expense of defensive and offensive cyber operations, has left the CAF trailing allies and adversaries in certain cyber defence capabilities. While China and

For Canada to win on the cyber-enabled battlefield, government and industry must collaborate intentionally.

Russia have proven their ability to launch attacks that cripple critical systems in seconds or quietly collect intelligence for years, the CAF has only recently received approval to engage in active and offensive operations at scale (though specialized activity has been present for years). Adversaries and allies have also demonstrated their ability to deploy new cyber capabilities in months or weeks, while the CAF remains burdened by a years-long and sometimes decades-long procurement cycle. Leading cyber

nations have also developed intentionally porous boundaries between government and industry; their domestic industrial bases are highly mobilized and integral to countering cyber threats.

The government's new defence policy, Strong Secure Engaged (SSE), could pave the way to a better cyber future. SSE commits billions of dollars for cyber infrastructure and programming. These investments, properly directed, could bolster a core of domestic cyber defence firms who possess the talent and capabilities the CAF requires to deliver on its cyber defence mandate.

For Canada to win on the cyber-enabled battlefield, government and industry must collaborate intentionally, as our allies do. CADSI's research suggests the most advanced cyber defence strategies employed by western nations have a component that is industry-led, academic-supported and government-funded to permit the incubation of next-generation ideas at the speed of cyber without the limitations of bureaucracy. A similar approach for Canada could mobilize a strong sovereign line of defence against rapidly evolving cyber threats.

A full report methodology including research and analytical approach can be found in Annex A.

INTRODUCTION

The connective powers of cyberspace appear to have transformed the nature of warfare. Cyber is now a consequential element impacting military operations and a contested domain in which countries must protect and defend themselves. The cyber threat to the Canadian Armed Forces permeates domestically through vulnerabilities in critical infrastructure, combat systems and equipment, and extends to where the military is deployed abroad.

In industry's view, the CAF's existing cyber capabilities require bolstering, and new proficiencies spanning the full spectrum of defensive and offensive cyber operations must continue to be developed and matured.

To help fortify Canada's line of cyber defence and support the CAF's transition to cyber-enabled warfare, this report attempts to reconcile divergent government and industry viewpoints. A key finding from CADSI's research was that government and industry lack the mutual trust required to effectively collaborate in the cyber defence of Canada. This distrust has been sown over time through a history of unproductive engagements, limited communications, and inadequate mutual understanding of each other's capabilities.

> **Government and industry appear to lack the mutual trust required to effectively collaborate in the cyber defence of Canada.**

This report responds to these issues by establishing a common language; defining and differentiating key cyber defence terms and concepts; mapping the Canadian cyber defence ecosystem and industrial capabilities; identifying key growth and innovation challenges; discussing opportunities to improve government-industry collaboration; and exploring policy options that could better mobilize the domestic industrial base to meet the CAF's defence objectives.

Although this report represents a balance of viewpoints reflecting government, industry and academia, it has been developed by Canadian industry, and its conclusions are weighted in favour of positioning domestic firms as core contributors to Canada's cyber defence future.

DEFINING CYBER DEFENCE

Cyber security and cyber defence are distinct and need to be defined as such. An ambiguous lexicon of terms has prevented industry and government from mutual understanding of key terms, concepts and definitions. CAF doctrine, the Canadian Criminal Code, the Communications Security Establishment Act, US DOD doctrine, and accepted industry usage all vary to some degree. CADSI's research suggests the following terms require unambiguous definition to permit effective communication and collaboration between government and industry.

Cyber Security focuses on network assurance and is driven by standards and practices rather than military tactics or engagement with an adversary. It comprises the body of technologies, processes, practices, in addition to response and mitigation measures designed to protect networks, computers, programs, and data from damage and unauthorized access, and to ensure the confidentiality, integrity and availability of these resources.

Cyber Defence requires a shift from network assurance to mission assurance and is driven by the need to sense, detect, orient and engage adversaries in the cyber domain to ensure mission success. Cyber defence activities and operations are conducted in the cyber domain in support of mission objectives, and are fully integrated into operational and planning activities across the Joint Functions (Army, Navy, Airforce, and Space domains). Cyber defence activities and operations represent a spectrum of escalating response and engagement measures with the adversary. These measures are detailed below.

Defensive Cyber Operations refer to activities and operations conducted on or through the global information infrastructure to protect an institution's electronic information and information infrastructures as a matter of mission assurance. Defensive cyber operations do not normally involve direct engagement with the adversary.

Active Cyber Operations refer to response activities and operations conducted on or through the global information infrastructure to influence, interfere, degrade or disrupt the capabilities, intentions or

activities of an adversary. Active cyber operations decisively respond to the provocations of an adversary and can include hunt and adversarial pursuit activities.

Proactive Cyber Operations refer to activities and operations conducted on or through the global information infrastructure to aggressively interdict anticipated attacks or that engage in advanced preparation of the anticipated cyber battlespace. Proactive cyber strategies can improve information collection by stimulating early threat responses, mapping attack vectors, identifying sources, and providing strike/first strike options.

Offensive Cyber Operations manipulate and disrupt adversarial networks and systems to limit or eliminate their operational capability. Although offensive cyber capabilities and cyber weapons can be developed by the private sector independently or in partnership with government, operations that utilize these capabilities are often led by nation states, and require legislative or ministerial-equivalent approvals.

Cyber defence operations are distinct from traditional defence operations in several ways:

- The pace of change is significantly faster to develop and deploy new capabilities;
- Geography is rendered irrelevant, erasing the distinction between home front and battlefront;
- Determining attribution and intent is more challenging than for conventional warfare, making it more difficult to direct the national response to responsible actors in a way that is appropriate, proportional and clearly signals intent back (e.g. allows for de-escalation by the aggressor);
- It is difficult to establish the boundaries within the cyber domain where an operational commander has the authority to take military decisions, as opposed to those that require civil and political authorities;

- The costs of deploying operations and achieving military outcomes have the potential to be substantially reduced;
- It can often times prove difficult to determine the actual impacts of cyber attacks, and cyber attack outcomes are not always immediately detectable;
- Cyberspace responses lack measures of effectiveness, have yet to be proven through extensive use in exercises and operations, and lack clear rules of engagement.

Cyber Defence is driven by the need to sense, detect, orient and engage adversaries in the cyber domain to ensure mission success.

OPPORTUNITIES FOR **COLLABORATION**
IN THE CYBER DEFENCE OF CANADA

In the face of growing cyber threats, CADSI believes the Canadian cyber defence ecosystem should act swiftly, and in concert, to strengthen domestic cyber capabilities. To analyze key areas for collaboration, CADSI deconstructed the ecosystem by industry, government and academia. Analysis suggests that industry leads cyber defence capabilities in many areas, although there are important exceptions.

Strong Secure Engaged repositions the CAF towards a more active stance on cyber defence. Domestic industry has active and offensive cyber capabilities that can help the CAF deliver on its cyber mission.

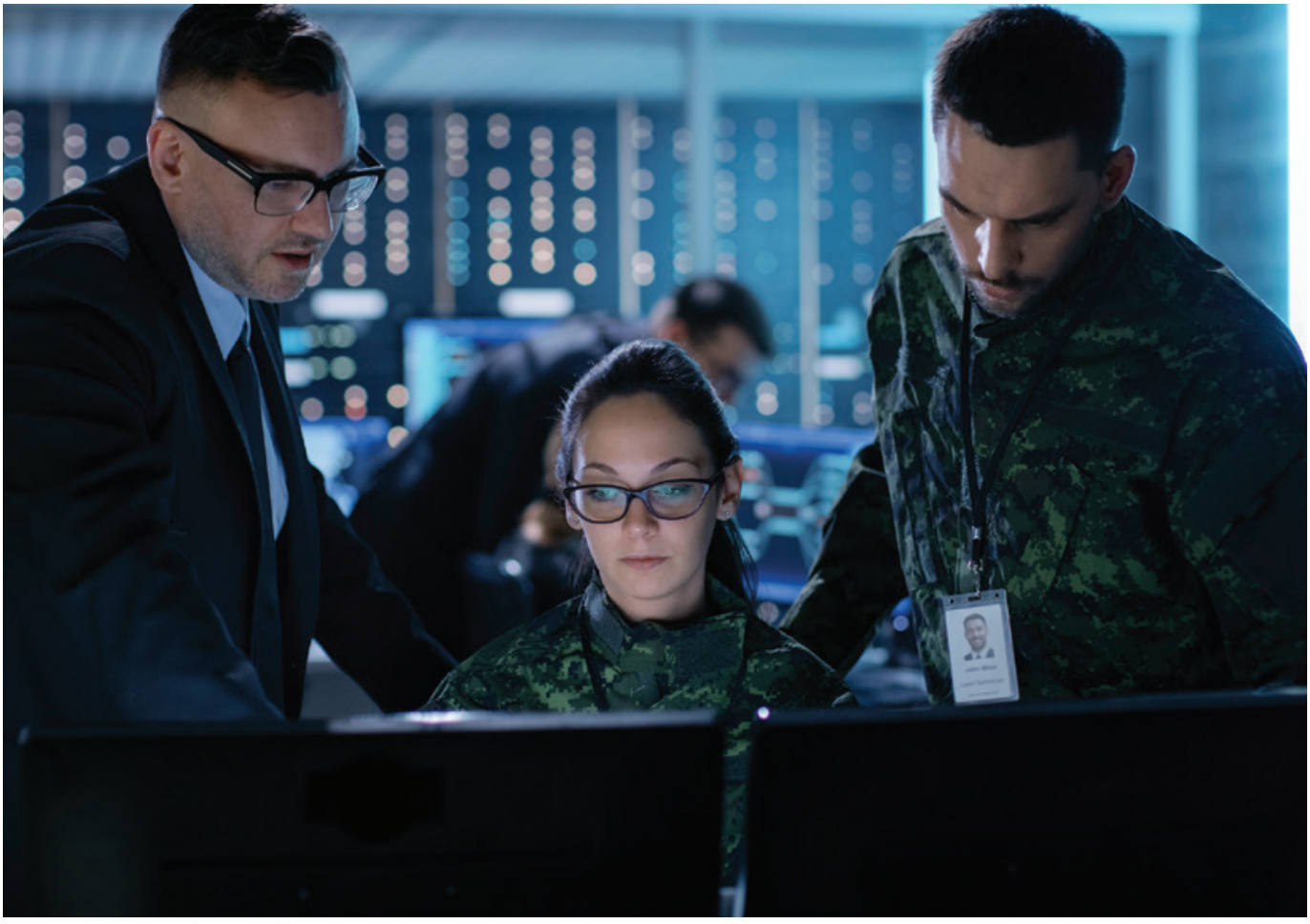
The Canadian private sector has a well-developed ability to identify and mitigate threats proactively, with precision and agility, at cyber speed. The government has expertise in cyber oversight, threat intelligence, investigation, quantum cryptography, reactive cyber, and has made significant investments in traditional IT security.[1] However, industry believes government has not fully exercised its unique mandate for active, proactive and offensive operations and CADSI research suggests these areas remain underserved markets compared with allies. The legislative framework in Canada is currently evolving in this area. Canada has produced world class academic research in areas of artificial intelligence, quantum computing, deterrence, and complex systems theory, but it is not fully exploited or connected to government and industry. Stronger collaboration between industry, government, and academia is key to scaling Canada's cyber defence capabilities.

[1] Government investment in traditional reactive IT security is estimated at $1 billion per year, compared with $30 million on what could be classified as cyber defence.

Defence Policy

In interviews with CADSI, members of Canada's cyber defence industry suggested that the federal government's emphasis on cyber resiliency, emergency management and disaster recovery has established a policy of reaction as a starting point for a strategy on cyber. However, the government's new Defence Policy, Strong, Secure, Engaged (SSE) signals a doctrinal shift. This policy repositions the CAF towards a more active stance on cyber defence with seven key cyber initiatives and investments to develop joint capabilities in advanced training, situational awareness, mission assurance, cyber threat intelligence, active response, offensive cyber operations, and to address existing talent gaps.

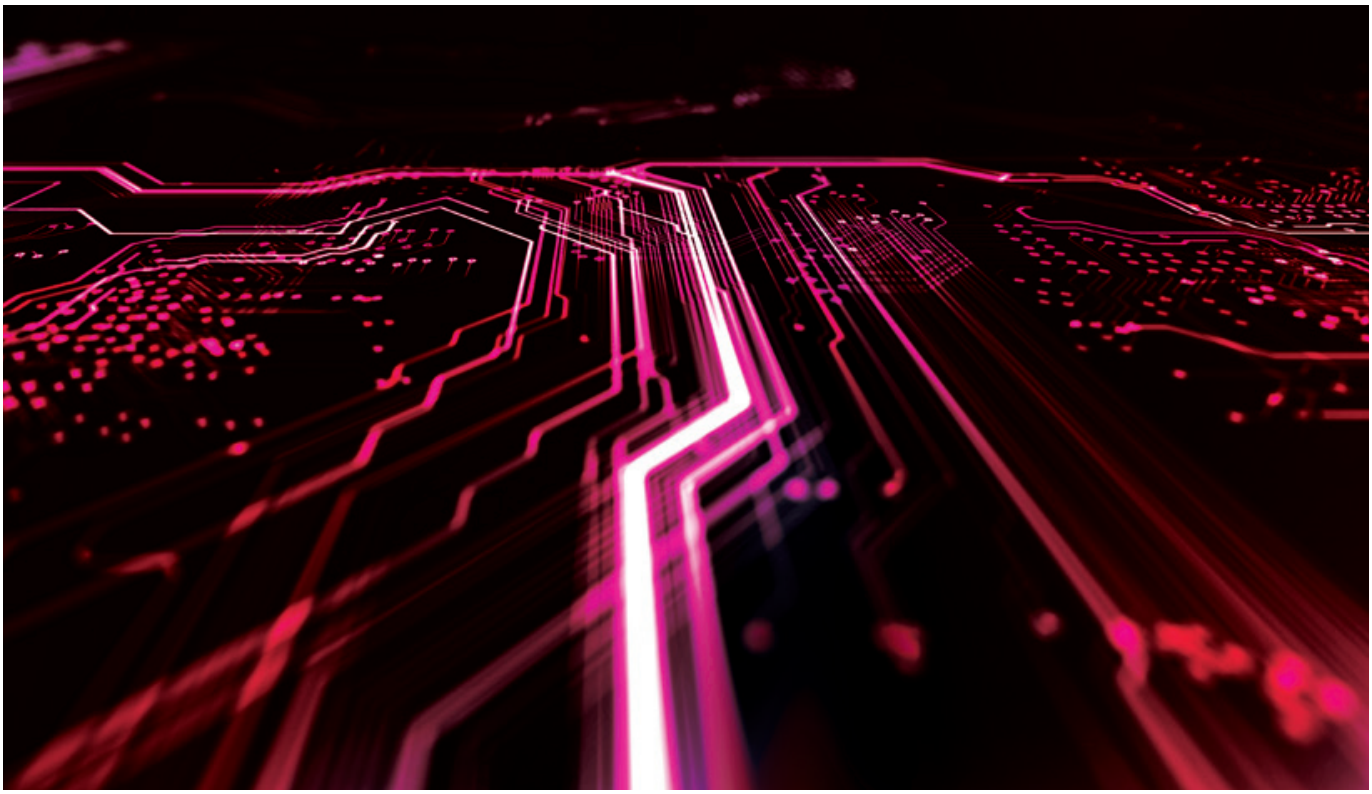
Under this policy, the IDEaS procurement program (a $1.6 billion investment over 20 years) has issued calls for proposals for multiple cyber-related challenges. Furthermore, the 2018 Federal Budget proposed spending more than half-a-billion dollars over the next five years to battle cybercrime and update Canada's aging digital security strategy ("Equality and Growth - A Strong Middle Class"). Included in these investments is the Canadian Centre for Cyber Security, which opened in October 2018 and is mandated to solve Canada's "most complex cyber issues" by working in partnership with private and public sectors (Canadian Centre for Cyber Security). The government's new policy position and investments are regarded by industry as positive indications of its willingness to collaborate to strengthen Canada's cyber defence capabilities.



CANADA'S CYBER DEFENCE **INDUSTRIAL BASE**

In North American and European markets, the private sector is largely responsible for developing the cyber networks upon which governments operate. Consequently, the private sector has intimate, specialized, and unique expertise in the cyber domain.

Throughout CADSI's interviews, industry consistently expressed its interest and willingness to share expertise, technologies, and talent with government, but has limited opportunities and fora in which to do so. This presents an opportunity to build upon the government's existing strengths in areas such as reactive cyber.



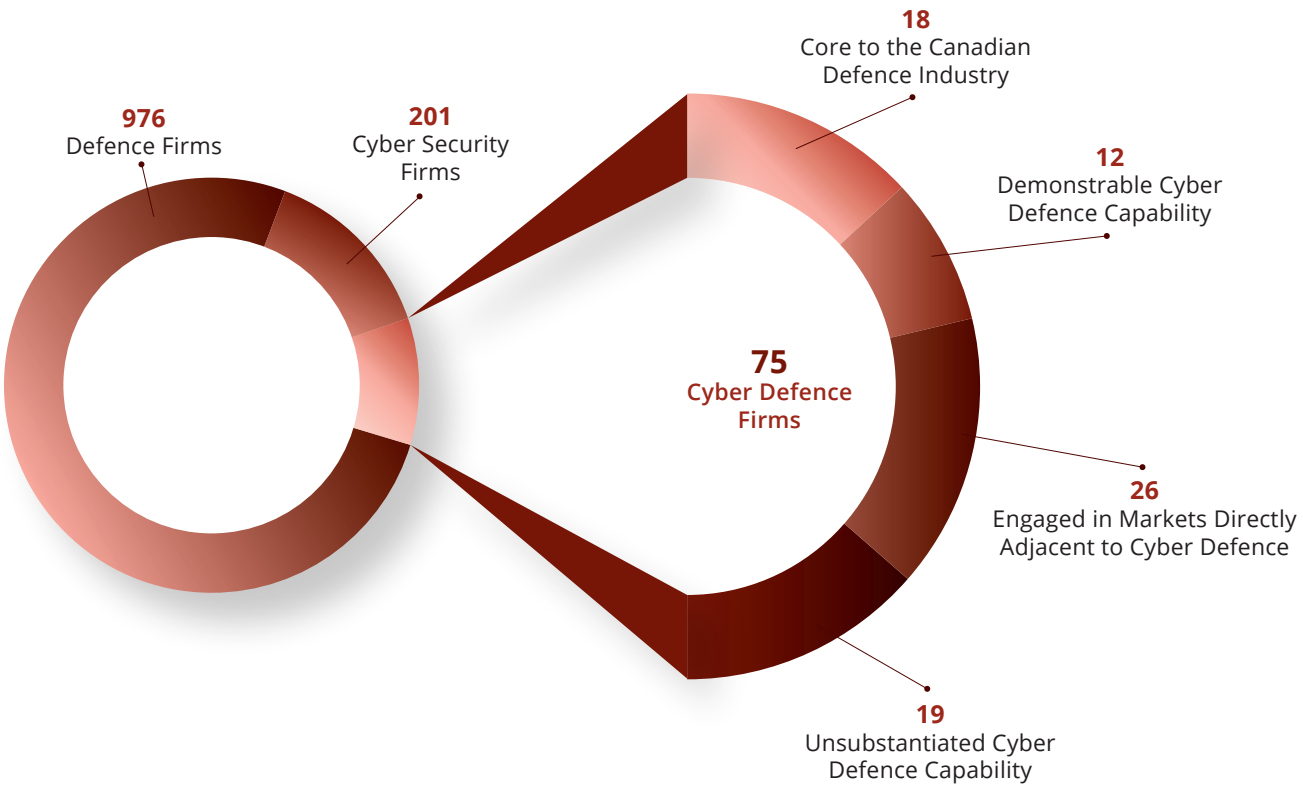
Industry is ready and willing to share expertise, technologies and talent with government, but has limited opportunities to do so.

At the outset of this study, CADSI identified 1,252 companies and organizations involved in defence, cyber security or cyber defence. From this list, 78 per cent identified as defence, 16 per cent identified as cyber security, and 6 per cent identified as cyber defence. A detailed analysis of those identifying as cyber defence revealed 26 companies with capabilities relevant or adjacent to cyber defence, 12 companies with demonstrable cyber defence capability, 18 companies at the core of the cyber defence industry with broad in-country strength, and 19 companies claiming cyber defence capability which could not be substantiated through available sources. Figure 1 illustrates an overview of Canada's defence, cyber security, and cyber defence industries. Figure 2 evaluates the cyber defence industry in greater detail.

Overall, the cyber defence ecosystem in Canada is made up of less than 30 companies and a dozen individuals with prerequisite top-tier expertise, most of whom are working for allied agencies, since the Canadian market has yet to demonstrate demand. These companies possess strong situational awareness and the means to mitigate threats proactively, with precision and agility, at cyber speed. They can develop and deploy new cyber technologies, training programs and services in ten months or less. Properly incentivized, they could help the Federal Government and the CAF keep pace with adversarial and allied innovation.

(Figure 1) *Overview of Canada's Defence, Cyber Security, and Cyber Defence Industries*

The following chart highlights cyber defence firm counts by level of capability development and domestic integration.



BUILDING UPON **CANADIAN CAPABILITIES**

A thorough analysis of Canadian defence, cyber security and cyber defence companies reveals 13 key capability areas that can be leveraged by government to fulfill Canada's growing and urgent need for defensive and offensive operations in cyberspace. These capabilities are assets to and complement the existing capabilities of the CAF.

Assessment Rating of Capabilities

To evaluate the cyber defence maturity of companies, this study used a scale (0-3) based upon evidence including but not limited to publications, project references, independent market analysis, interviews, intellectual property claims, and key performance metrics.

Building upon current government strengths in cyber oversight, threat intelligence, investigation, reactive cyber and traditional IT security, the CAF can benefit from industry efficiencies in the following areas to defend Canada in the cyber domain. ***(See Figure 2)***

See Annex B for a complete listing of cyber defence sub-capabilities by area.

Ranking

0

There is no evidence to substantiate that Canadian firms have expert knowledge of cyber defence concepts or the desire to develop cyber defence capabilities in this area.

1

There is some evidence to substantiate that Canadian firms have basic knowledge of cyber defence concepts and have considered the development of cyber defence capabilities in this area.

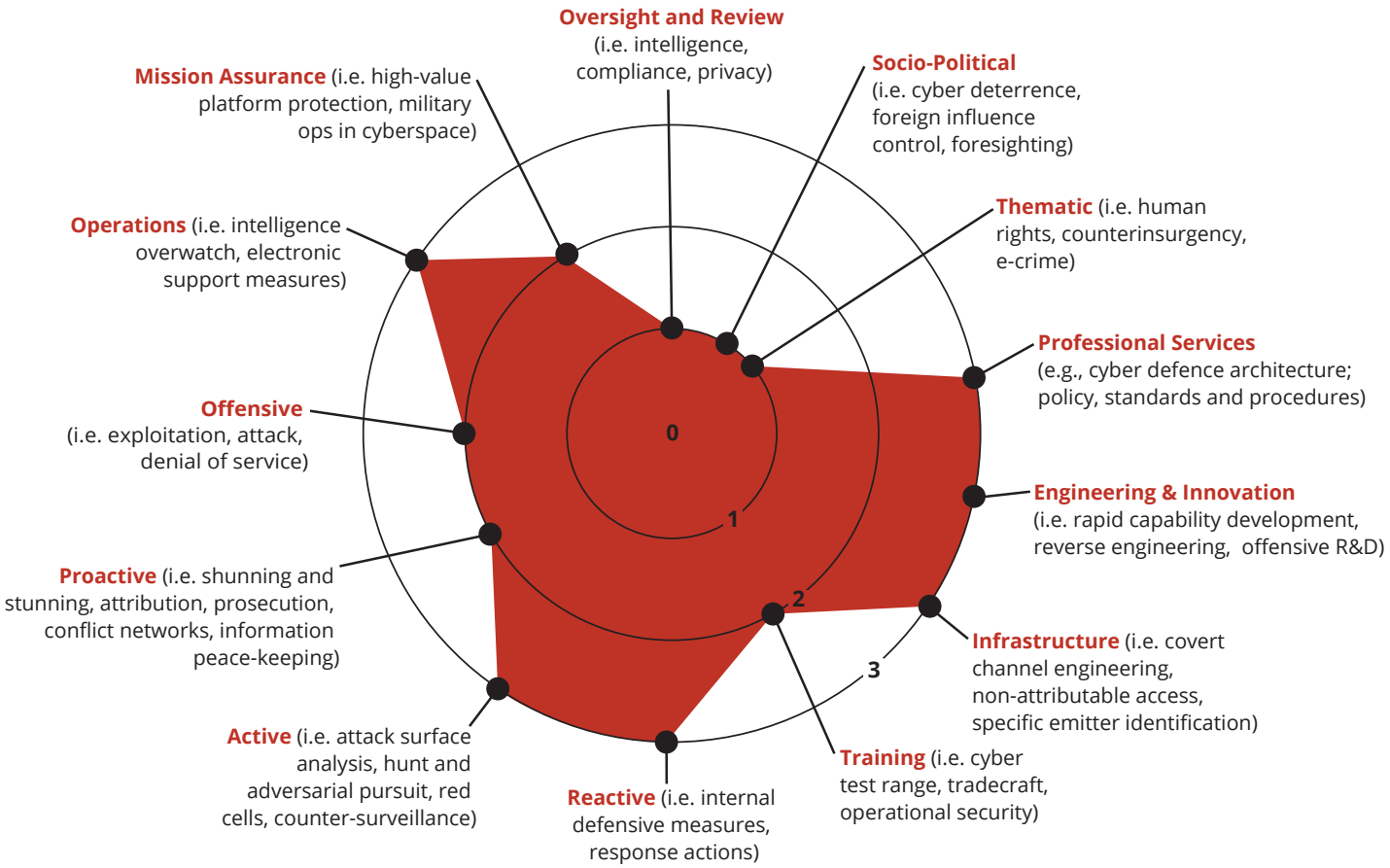
2

There is evidence to substantiate that Canadian firmshave working knowledge of cyber defence concepts and have developed emerging cyber defence capabilities in this area.

3

There is evidence to substantiate that Canadian firms have in-depth cyber defence knowledge, demonstrable capabilites, mature products/ services and measurable successes in this area.

(Figure 2) *Canada's Cyber Defence Capabilities*



ROADBLOCKS TO GROWTH

The speed of cyber, consequences of convergence, and growing exposure of defence firms and the CAF to adjacent cyber threats are key concerns for Canada's cyber defence future. To address these concerns, however, Canada must first break down the silos that prevent cyber defence actors from collaboration and capacity-building.

The CADSI research team tried to register a cyber defence company to do business with the Government of Canada. This process required engagement with multiple groups including PWGSC, BuyAndSell, ISED, and Revenue Canada, in addition to an array of classification systems including SIC, NAICS, and GSIN*. None of these classification systems have dedicated categories for cyber security or cyber defence.

*SIC: Standard Industrial Classification System. NAICS: North American Industry Classification System; GSIN: Goods and Services Identification Numbers.

Cyber Defence Silos in an Era of Convergence

Interviews with government and industry experts suggest that silos are preventing key cyber defence actors – including government departments, industry associations, companies, and academia – from meaningful collaboration and capacity building. An analysis of adjacent policies and programs spanning defence, national security, critical infrastructure protection, public safety, foreign relations, and industrial development reveals little cyber-harmonization. Though elements of a functional ecosystem are present in Canada, no organization or group has yet assumed the mantle of responsibility for aligning currently dissociated resources around a common set of objectives or outcomes.

Though elements of a functional ecosystem are present in Canada, no organization has taken responsibility for aligning Canada's significant cyber defence resources around a common set of objectives.

The existing procurement system, designed for the acquisition of more traditional goods and services, is another limiting factor contributing to industry frustration and preventing engagement with the public sector. The standard definition of cyber used globally,

compared to that used by the CAF does not align. Nearly all modern militaries have collapsed the definitions of C4ISR/EW/SIGINT/C5I[2] under cyber, though the Government of Canada's industry classification system does not include any dedicated categories for cyber security or defence.

In addition to communication challenges, industry does not perceive government to be a strong adopter of Canadian cyber defence technologies. Canadian cyber defence companies have developed proven expertise working with allies on active defence for decades. Despite this, available evidence suggests the Department of National Defence procures predominantly from foreign companies – as much as 94 per cent in ICT security.

The Canadian cyber defence industry finds it challenging to navigate, sell and partner across boundaries in an environment where government client groups are working in silos, policies and programs are discordant, industry and government do not speak the same language, and where government has made limited investment in Canadian companies. Despite these frustrations, industry is willing to share its expertise with the CAF to strengthen sovereign capabilities that will work in the best interests of Canadians.

[2] Acronyms for military systems. C4ISR is an acronym for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Systems; EW is an acronym for Electronic Warfare; SIGINT is an acronym for Signals Intelligence; and C5I is an acronym for Command, Control, Communications, Computers, Collaboration, and Information Systems.

The CADSI research team analysed 5 years worth of DND transactions* in cyber and adjacent areas (90,839 transactions accounting for $17.7B in product and service purchases) and discovered that 60% of purchases went to foreign suppliers, which rose to 94% foreign purchases in ICT security.

*Analysis of all transactions through Government of Canada cyber security categories in supply arrangements and standing offers over the past five years as well Buy and Sell related to DND over the past five years.

The Pace of Decision-Making in the Civil Service

The urgency of cyber defence is rooted in the reality that cyber threats propagate faster than the government decision-making process enables action. As this report has already discussed, the lifecycle of major CAF cyber programs ranges from five to 20 years, whereas CADSI research suggests that Canada's adversaries can innovate within months and attack within minutes. Government must adapt its policies and decision making processes to the speed of cyber.

Government must adapt its policies and decision making processes to the speed of cyber.

While the new Defence Policy is a positive step for Canada, current CAF projects moving through the procurement pipeline for fielding post-2020 are wed to the old doctrine. As cyberwarfare is highly sensitive to the speed of procurement, defence procurement reform stands at the centre of success or failure for cyber defence initiatives in the CAF, a viable industry, and the national security of Canada.

CADSI's research also suggests the CAF's current procurement approach may overemphasize acquisition of highly customized and inflexible cyber solutions. Industry would prefer to offer the CAF overarching solution architectures that comprise combinations of existing and emerging technologies and services, capable of delivering the desired outcome, while preserving the flexibility to evolve alongside current cyber innovations.

The defence industrial base is a network of importance to Canada. The government should declare it as such, and help to protect it from cyber threats.

Preparing the Domestic Industrial Base to Manage Adjacent Threats

CADSI believes the CAF will increasingly become a priority target for cyber attacks from adversaries, and defence companies supporting the CAF will be drawn into cyber conflicts. Firms supporting critical Canadian military networks, platforms and technologies could be subjected to attacks that aim to reduce or eliminate the ability of the affected network, platform or technology to meet the needs of the CAF. Given the consequences of such an attack, CADSI believes that the Government of Canada should declare the defence industrial base as a network of importance to Canada, and ensure that organization including CSE and PSC are mandated to work with the defence industry to secure defence supply chains and the goods and services they produce.

THE WAY **FORWARD**

An analysis of global cyber security and defence organizations, domestic and international associations, national and international cyber strategies, the Canadian cyber defence ecosystem, interviews with subject matter experts, and additional independent research, has led to several observations and policy options that can support the fortification of Canada's cyber defence capabilities.

The most effective cyber defence programs have, at their core, a secure and trusted goverment-industry network, real-time threat intelligence sharing, and joint threat reduction activities.

Global Best Practices

CADSI research suggests that amongst allies, the United States, the United Kingdom, and Australia have the most evolved cyber security strategies, and these can be adapted to the Canadian context. In these countries, government and industry have a collaborative relationship. Effective government participation includes the sharing of actionable intelligence, threat reduction measures on behalf of industry, the creation of innovation centres, targeted investment towards industry-led initiatives, securing defence supply chains, and promoting and practicing supply chain sovereignty as a first-buyer of national technologies.

In the U.S., U.K., and Australia, programs foster free discussion amongst subject matter experts at different classification levels. In the United States, InfraGard is a program that partners the FBI and members of the private sector to provide timely exchange of threat information and mutual learning opportunities to protect critical infrastructure.

Additional features of national programs in these countries include exploitation of research, rapid and agile engineering, and the commercialization and operationalization of ideas. All of these programs, at their core, have a secure network, real-time cyber threat intelligence sharing, and coordinated threat-reduction activities. Fundamentally, they are based upon trusted partnerships between industry and government and represent what is possible within Canada to advance domestic cyber defence capabilities.

A Model for Canada

For Canada to win on the cyber battlefield, the Canadian cyber defence ecosystem must collaborate intentionally, as our allies do. CADSI's research suggests the most advanced cyber defence strategies employed by western nations have a component that is industry-led, academic-supported and government-funded to permit the incubation of next-generation ideas at the speed of cyber without the limitations of bureaucracy. A similar approach for Canada would empower and mobilize a strong line of defence against rapidly evolving cyber threats.

Figure 4 draws upon global best practices, Canadian capabilities, and an ecosystem needs analysis to provide an overview of recommended actions and initiatives that could contribute to the development of an effective government-industry collaboration and engagement strategy. Validated over the course of this study's seventy (70) interviews, and refined through subsequent discussions with cyber defence experts from government, industry and academia, CADSI has identified eight (8) priority actions and initiatives that represent critical first steps along the path toward better government-industry collaboration and mobilization of the defence industrial base. They are summarized below, and grouped thematically.

The most advanced cyber defence strategies have a component that is industry-led, academic-supported, and government-funded to incubate next-generation ideas at the speed of cyber.

(Figure 3)
The Way Forward:
A Model for Canada

Share Knowledge and Build Trust

Improve Sector Operations and Governance

Bridge the Talent Gap

Modernize Cyber Procurement

Align Industry Capabilities to Global Market Demands

Recommendation 1: Share Knowledge and Build Trust

Government-Industry Dialogue: Engage industry, provincial and federal departments and agencies, and other cyber mandated organizations to harmonize agendas and sustain an ongoing dialogue on cyber issues and policies challenges. Develop formalized structures to locate this dialogue, and ensure that specialized considerations including defence policy, national security, critical infrastructure protection, procurement and innovation policy are addressed.

Cyber Communities of Trust: Create recurring fora to host top-tier speakers, expert panel discussions and workshops on critical cyber defence issues within classified venues. Attract government, military, academic and industry subject-matter-experts to these intimate engagements to facilitate undistorted discussions of cyber threats, joint response measures, and to establish communities of trust.

Recommendation 2: Improve Sector Operations and Governance

Secure Cyber Network: Establish a secure (trusted) Canadian cyber defence network to facilitate collaboration and knowledge sharing between government and industry partners, while providing a platform for secure communications. This network could serve multiple purposes including the generation of situational understanding within the cyber domain, joint detection and deterrence of attacks, a collaboration and testing space to tackle emerging cyber threats, and a platform for joint R&D.

Secure the Canadian Defence Industrial Base: Connect defence associations and their members, particularly SMEs, with relevant departments and organizations including the Communications Security Establishment, Department of National Defence, Public Safety Canada, Innovation, Science and Economic Development Canada, and the Canadian Centre for Cyber Security to increase the security of the defence industrial base at scale. This could include, for example, the joint development and publication of cyber vulnerability and threat assessments.

Recommendation 3: Bridge the Talent Gap

Cyber Corporate Reserves and Expert Exchanges: Increase the pool of available cyber talent to be used as cyber reservists by developing expert exchanges and talent sharing agreements between government and industry in multiple areas, including offensive and defensive cyber operations, information peacekeeping, education and training, programming, procurement, and policy development.

Recommendation 4: Modernize Cyber Procurement

Procurement at the Speed of Cyber: Create different authorities for cyber defence procurements capable of keeping pace with the shorter innovation cycles of adversaries. This could include redesigning Standing Offers and Supply Arrangements, developing new contracting vehicles capable of responding to convergence, IoT/IoE, open system design, etc., and encompassing both goods and services task-based authorizations.

Recommendation 5: Align Industry Capabilities to Global Market Demands

Classification System and Capabilities Database Overhaul: Update industry classification systems, including Standard Industrial Classification (SIC), North American Industry Classification System (NAICS), and the Government of Canada's Goods and Services Identification Numbers (GSIN), to accurately represent the cyber defence domain. Changes should reflect a common taxonomy of terms and capability areas acceptable to government, military and industry and that can be mapped to the taxonomy of allies and partners. Develop a database of firms reflecting the updated classification systems and providing accessible information on product and service offerings by capability.

Global Market Analysis and Export Support: Engage relevant departments and agencies including Global Affairs Canada and the Trade Commissioner Service to develop or acquire market assessments for priority

cyber defence markets. Particular attention should be focused on Eastern European and Southeast Asian Markets. Engage industry to align market opportunities to Canadian capabilities and provide export guidance and support.

Government and industry working together is the way forward to build digital sovereignty, secure the defence industrial base, and effectively defend Canada and the CAF in the cyber domain. This report's recommendations provide the means to connect industry talent and capability to operational and mission support requirements, foster ongoing dialogue and information sharing through trusted networks, and support the growth and resiliency of domestic firms.

CONCLUSION

Cyber threats hit at the core of a government's responsibility – to keep its citizens safe – and cut across multiple sectors that impact on prosperity, quality of life and national security. The Government of Canada faces many challenges and hard choices as it adapts to a world that has become increasingly cyber-enabled and dependent. Whereas nations used to be able to protect and defend their citizens buffered by geography, cyber erases distinction between home front and battle front. The tools we rely on to communicate and connect, to share knowledge and ideas, to conduct business, to manage the day to day activities of our lives have become increasingly exposed to the cyber domain and we are more vulnerable as a result.

When it comes to the operations of the Canadian Armed Forces (CAF), the risks imposed by an increasingly cyber-enabled world are significant. The platforms and systems on which the military depends are poised to enter a new battlespace where the physical and digital are seamlessly merged. Although the CAF is intimately familiar and capable to defend itself against physical threats, those born of the cyber domain and subject to its relentless pace of technological innovation and convergence, are unlike anything the CAF has faced before.

Fortunately for Canada, our allies face the same disruptive shifts, and have recognized the magnitude of the challenge, and the futility of addressing it in silos. They have aligned government, industry and academic resources to respond collaboratively, and have broken down the barriers that would otherwise limit the sharing of knowledge, ideas and talent essential to countering the cyber threat. Canada should quickly learn from and adopt the relevant practices our allies.

Now is the time, as the mouse proves equally mighty to the missile in modern warfare, to repatriate Canada's cyber defence expertise and overhaul the ecosystem and procurement processes to work at cyber-speed. Canadian firms are ready and willing to support the CAF to defend and protect Canada in the cyber domain. Intentional collaboration between industry and government is the way forward. Similarly, the government should recognize the defence industrial base as a network of importance to Canada. By sharing innovative ideas, talent, and capabilities related to cyber defence across government, industry and academic boundaries, Canada will be better equipped to protect and defend its citizens, critical infrastructures, and military against threats from the cyber domain.

REFERENCES

Barysevich, Andrei. "Military Reaper Drone Documents Leaked on the Dark Web". Recorded Future. July 10, 2018.
https://www.recordedfuture.com/reaper-drone-documents-leaked/

Brewster, Murray. "Civilian oversight key to offensive cyber operations, says expert". CBC. June 18, 2017.
https://www.cbc.ca/news/politics/cyber-weapons-canada-1.4164696

Brewster, Murray. "Old Russian fighters and smartphone hacking: What the Canadian military learned in 2017". CBC. January 3, 2018.
https://www.cbc.ca/news/politics/canada-fighters-hacking-nato-1.4470361

Boutilier, Alex. "Canada's military seeks major cyber defence upgrade". Toronto Star. December 27, 2107
www.thestar.com/news/canada/2017/12/27/canadas-military-seeks-major-cyber-defence-upgrade.html

Canadian Centre for Cyber Security, Government of Canada. October 30, 2018.
https://www.cyber.gc.ca/en/about-cyber-centre

Communications Security Establishment, Government of Canada. August 8, 2014.
https://www.cse-cst.gc.ca/en/about-apropos/vision-mission

"Equality and Growth - A Strong Middle Class". Department of Finance Canada. Government of Canada. February 27, 2018.
https://www.budget.gc.ca/2018/docs/themes/advancement-advancement-en.html

Greenberg, Andy. "The Untold Story of Notpetya, the Most Devastating Cyber Attack in History". Wired. August 22, 2018.
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Howell, Jenalea. "Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says". IHS Markit. October 24, 2017.
www.technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says

"Internet Organised Crime Threat Assessment 2018". Europol's European Cybercrime Centre. 2018.
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

Mlot, Stephanie. "70 Percent of Population Will Have Smartphones by 2020". June 3, 2015. PC Mag.
https://www.pcmag.com/artcle2/0,2817,2485277,00.asp

"Strong, Secure, Engaged: Canada's Defence Policy". Department of National Defence. Government of Canada. 2017.
http://dgpaapp.forces.gc.ca/en/canada-defence-policy/docs/canada-defence-policy-report.pdf

ANNEX A - **REPORT METHODOLOGY**

The methodology for this report included analysis of existing cyber and militarydoctrine, corporate and departmental strategic and operational plans, program activity architectures, innovation, defence and security policies, Canadian Armed Forces outlooks, security science and academic literature, international standards and cyber norms, and the global threat landscape.

The Canadian cyber security and defence industrial ecosystems were mapped by correlating quantitative data across several sources, including the Industry Canada Company Capabilities Database, CADSI's membership database, econometrics from BuyandSell.gc.ca, proactive disclosures involving all transactions in the past five years by the Government of Canada, and independent industry market analysis.

Research was further enriched through open source and business intelligence methods including keyword searches of corporate websites and industry publications and an in-depth review of cyber security R&D conducted in Canada over the past decade. An intersecting view of the market was completed through an assessment of partnership channels.

To ensure proper contextualization of key findings and to develop the SWOT analysis, subject matter experts were identified through market research, existing client relationship management systems, staff augmentation databases, and supplemented with social network analysis and relationship power mapping. Seventy (70) subject matter experts were identified and interviewed reflecting a balance of inputs across private (55%), public (40%) and academic (5%) domains. Their insights helped to refine and validate the ecosystem maps, identify areas for additional research, prioritize opportunities and challenges, and develop recommendations.

ANNEX B – **CANADIAN CYBER DEFENCE**

SUB-CAPABILITIES BY AREA

Oversight and Review

- Intelligence
- Compliance
- Privacy
- Legal

Socio-Political

- Cyber Deterrence]
- Direct Diplomacy
- Cyber Norms and Standards
- Human Rights
- Foreign Influence Control
- Foresighting and Over-the-Horizon (OTH) Scanning
- Informationized Warfare
- International Legal and Privacy Law
- Operational Research
- Strategic Analysis

Thematic

- Civilian-Military Cooperation (CIMIC)
- Counterinsurgency (COIN)
- Counter Electronic Espionage
- Gamification
- Electronic Crime
- Irregular / Unconventional Warfare Influence and Information Activities
- Joint Interagency Multination and Public (JIMP) Environments
- Cyber Warcrimes
- Cyber Weapons of Mass Destruction

Professional Consulting Services

- Cyber Defence Strategy
- Cyber Defence Architecture
- Project Management and Engineering Support Services
- Policy, Standards and Procedure Development
- Program Development
- Cyber Defence Futures and Foresighting
- Cyber Defence Planning
- Security Orchestration and Automation

Engineering & Innovation

- Over-the-Horizon (OTH) Offensive Cyber Threat Capability Research and Development
- Rapid Engineering Capability Development
- Special Programs
- Reverse Engineering
- Next Generation Lawful Access

Infrastructure

- Big Data Analytics
- Botnets
- Bullet-Proof Hosting
- C5ISR
- Circumvention Technology
- Clandestine Networks
- Command and Control (C&C)
- Conflict Networks
- Counter e-Surveillance and Censorship
- Covert Channel Engineering
- Cyber Collection Systems
- Cyber Intelligence, Situational Awareness and Decision Support
- Cyber Test Range
- Delivery Networks
- Non-Attribution Networks
- Overwatch
- Trusted Internet Access
- Ultra Secure Facilities Architecture Design
- Specific Emitter Identification (SEI)

Training

- Cyber Test Range and Staging Environment
- Cyber Operator / Warrior Training
- Tradecraft

Reactive

- Cyber Security Awareness (CSA)
- Defensive Cyber Operations Decision Support (DCO-DS)
- Internal Defensive Measures (IDM)
- Defensive Cyber Operations Response Actions (DCO-RA)

Active

- Advanced Open Source Intelligence (A-OSINT)
- Adversarial Modelling
- Airborne Intelligence, Surveillance and Reconnaissance (ISR), and Drones

- Analytic Tradecraft
- Area Handbooks
- Attack Surface Analysis
- Attribution
- Attribution Independent Verification and Validation (IV&V)
- Backstopping and Persona Management
- Big Data Fusion / Multi-Level Data Fusion Modelling
- Critical Infrastructure Protection (CIP)
- Communications Electronic Warfare (EW) Electronic Counter-Counter Measures (ECCM)
- Counter-Advanced Persistent Threat (APT)
- Cyber Intelligence Surveillance and Reconnaissance (ISR)
- Cyber Intelligence Preparation of the Battlefield (IPB)
- Cryptanalysis
- Cyber Threat Intelligence
- Dark Net Analysis
- Dark Space Analysis
- Dark Web
- Deep Field Sensor Array
- Semantic Botnet Defence
- Digital Currency Financial Intelligence
- Electronic Deception
- Enhanced Situational Awareness (SA) and Activities of Interest (AOI)
- Game Theory
- High Value Targeting
- Human Terrain Mapping
- Hunt and Adversarial Pursuit
- Intelligence Software Agents
- Multiplayer Online Role-Playing Games (MMORPG) and Persistent Virtual Worlds (PVW)
- Online Source Recruiting and Handling
- Operations Security (OPSEC)
- Over-the-Horizon (OTH) Thinking
- Recursive Domain Name System (DNS) Analytics
- Red Cells
- Radio Frequency (RF) / Electro Magnetic (EM) Sensors
- Semantic Weapons
- Signals Intelligence (SIGINT)
- Communications Intelligence (COMINT)
- Electronic Intelligence (ELINT)
- SIGINT/COMINT/ELINT Support
- Social Media Exploitation
- Social Network Analysis
- Social Media Intelligence (SOCMINT)
- Space Exploitation
- Security Intelligence Operations Centre
- Special Operations Security
- Tactics, Techniques and Procedures (TTPs)
- Target Templating
- Targeting Methodology
- Upstream Security and Intelligence

Proactive

- Adaptive Dispersed Operations
- Computer Network Exploitation (CNE) and Access
- Counter-Influence
- Cyber Operations & Influence Activities
- Deep Field Research
- Exploit Development
- Exploitation of Internet of Things (IoT) / Internet of Everything (IoE)
- Cyber Find, Fix, Finish, Exploit, Analyze, Disseminate (F3AED)
- Foreign Military Technology Acquisition
- Human Intelligence (HUMINT)
- Influence Activities and Counter Influence
- Information Peace Keeping (IPK)
- Computer Network Operations (CNO)
- Online Countering Violent Extremism (CVE) and
- Counter-Radicalization
- Systems Security Engineering (SSE)
- Technical Elicitation
- Tradecraft

Offensive

- Blocking, Stunning and Shunning
- Computer Network Attack (CNA)
- Communications Electronic Warfare (EW) Electronic Counter Measures (ECM)
- Critical Infrastructure Interference
- Denial of Service
- Internet of Things (IoT) / Internet of Everything (IoE) Distributed Denial of Service (DDoS) Attacks
- High Energy Weapons (Directed Energy [DE], Electromagnetic Pulse [EMP])
- Preemptive Operations

Operations

- Attack Surface Analysis
- Defensive Cyber Operations Decision Support (DCO-DS)
- Defensive Cyber Operations Response Actions (DCO-RA)
- Close Access Cyber Operation
- Communications Electronic Warfare (EW) Electronic Support Measures (ESM)
- Cyber Intelligence Preparation of the Battlefield (IPB)
- Electronic Enemy Order of Battle (EEoB)
- Intelligence Oversight and Overwatch
- Intelligence Production
- Sensitive Site Exploitation
- Special Operations Security
- Target Templating
- Threat Reduction Measures
- Lawful Access

Mission Assurance

- High-Value Platform Protection
- Critical Capability and Asset Protection
- Military Operations in Cyberspace
- Rapid Response Orchestration
- Effective Operations Under Constrained Cyberspace Conditions

Canadian Association Of Defence And Security Industries

300-251 Laurier Avenue West
Ottawa, ON K1P 5J6

defenceandsecurity.ca | @cadsicanada