THE CYBER COLLABORATION IMPERATIVE:

An Overview of Leading Government-Industry Collaboration Models and Practices in Cyber Defence

CADSI · AICDS
Canadian Association of Defence and Security Industries
Association des industries canadiennes de défense et de sécurité

TABLE OF
CONTENTS

EXECUTIVE
SUMMARY

The cyber domain is without historical precedent. It is a human construct, borderless, and ever changing. It is also growing in complexity and evolving in myriad new ways with extraordinary velocity, transforming the lives of individuals, dominating the global economy, and changing the rules of engagement for nation states. With revolutionary advancements now being made in artificial intelligence (AI), big data, 5th generation mobile communications, social networking, quantum computing and the Internet of Things (IoT), the cyber domain will continue to have an outsized impact at every level of society, including national security.

As cyber continues to evolve, malicious actors – a category which includes nation states, criminals, terrorists, hacktivists and opportunists – are harnessing each new capability and improvement in cyber technology to launch cyberattacks on individuals, businesses and states and are often able to obscure their tracks. At a national level, cyberattacks are already having measurable adverse economic effects. According to the Government of Canada, the total revenue at risk for Canada owing to cyber threats is estimated at $100B per year[1]. In the U.S., the economic impacts on the economy of a major cyberattack on the nation's critical infrastructure have been estimated to be between USD $243B and as much as USD one trillion in the most extreme scenario.

Unlike conventional interstate warfare, which takes meticulous planning and can cost billions of dollars to execute, devastating cyberattacks with far-reaching consequences can be launched against critical infrastructure with lightning speed by a small group of cyber experts armed with nothing more than internet-enabled personal computers and a few lines of malicious code. These attacks can be devised and unleashed with precision or indiscriminately from anywhere in the world over the course of a few minutes or seconds, and with the damage done, the perpetrators can quickly erase all traces of their activities, making attribution nearly impossible or plausibly deniable.

For governments, securing the state against cyberattacks is a challenge of significant magnitude that requires a commensurately big shift in thinking. For example, NATO now considers a cyberattack on one of its members an action that justifies invoking collective defense under Article 5 of the NATO Treaty. What starts in cyberspace, does not stay in cyberspace. Cyberattacks cannot be addressed using the strategies and methods designed to neutralize more conventional threats and adversaries because cyber is fundamentally different.

> Governments working in isolation will not be able to keep up with the escalating pace of threats presented by the cyber domain.

The unique characteristics of the cyber domain – accelerated pace of innovation, private sector ownership of the infrastructure, asymmetric threats, economics heavily favouring the attackers – will require new policies, decision-making processes, procurement approaches, and methods of integrating diverse public and private stakeholder resources and motivations around common objectives. However, these alone will not equip governments with the full range of tools and capabilities required to keep up with escalating threats from the cyber domain. In fact, no matter what improvements they make, governments working in isolation are unlikely to succeed.

Fortunately, the private sector brings many strengths to the table that governments can leverage to protect and defend national security through the cyber domain. Unlike the traditional domains of air, land, sea and space, over which governments have some measure of influence or control, cyber infrastructure is predominantly owned by the private sector. In Canada, for example, private firms own and operate 98 per cent of cyber infrastructure[2]. Cyber firms are also the engine driving the relentless pace of cyber innovation and the proliferation of the medium throughout society[3]. They develop the underlying technologies that allow the cyber domain to function and the commercial products and solutions designed to solve its biggest challenges. They provide access to a diverse array of product and service pipelines with development cycles that pace those of Canada's adversaries. They are perpetually on the front lines of cyberattacks and cyber aggression, regularly gaining insights into adversarial tactics, techniques and procedures. And unlike their public sector counterparts, they are not burdened by years-long or decades-long acquisition and deployment processes. Instead, they can field a new, fully functioning technology solution in months or weeks[4].

1 Dark Space (APT0) – A Comprehensive Report on Advanced Cyber Security Tradecraft and Issues Affecting Canada, Bell Canada, Department of National Defence, Communications Security Establishment , Apr 2011-Mar 2015

2 Cyber Interdependencies of Canada's Critical Infrastructures, Bell Canada, RAND Corporation, PSC, Apr-Mar 2007.

3 The Cyber Security Social Contact, Internet Security Alliance, Sept 2016.

4 From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence, Mar 2019.

Given the many areas in which private industry complements and augments government capabilities in the cyber domain, collaboration between the two groups is critical for keeping pace with rapid innovations in cyber; for developing effective policies, tools and strategies to ensure national security and defence; and for managing a deep skills gap. The scope, speed and complexities of the challenges presented by the cyber domain touch every aspect of society and require a unified response. Despite a common mission, mutual understanding and

> Canada's allies have recognized the benefits of a collaborative approach between government and industry in combating their cyber challenges.

trust remain elusive in Canada. CADSI's research, which involved an in-depth comparative study of global leading practices, models, and programs of government-industry collaboration in cyber defence and security, indicates that Canada's allies have recognized the many benefits of a collaborative approach in combating their own cyber security and defence challenges. They have experimented quickly and decisively with a range of approaches to government-industry collaboration at the strategic, policy and operational levels, and are forging new industry relationships to advance critical asset protection and rapid capability development. They have achieved notable successes in different areas of cyber as a result of their collaborative efforts and have learned tough lessons by failing quickly on occasion.

The U.S., for example, leads in cyber procurement, enabling its government (including the military and national security agencies) to rapidly acquire and iterate state-of-the-art cyber technologies and solutions from industry through an array of programs, constructs and supporting policies like the Defense Innovation Unit (DIU), Army Futures Commands (AFCs), and Other Transactional Authorities (OTAs). It realized that the traditional procurement balance between financial risk management and timely acquisition, if applied to cyber, would invariably lead to failures where a solution was available that could have prevented the impact of a cyberattack, but it could not be acquired in time. More realistic estimates (from an increasing sample size) of the resulting damages, lost operational effects and repairs imposed by cyberattacks and breaches, are forcing a recalculation of the cost of delay or inaction and creating a new dynamic that redefines traditional concepts of value for money when it comes to procuring cyber solutions.

On the talent development and knowledge sharing front, the U.K.'s National Cyber Security Center (NCSC) launched the "Industry 100" initiative to promote close collaborative working relationships between NCSC and 100 industry cyber defence experts. In cyber, where people are the endpoint of technological convergence, government and industry need to remove the administrative barriers that stop them from working together, wherever they exist. This is especially true given the growing cyber skills shortage faced by Canada and its allies.

At a governance and international engagement level, Australia's efforts to coordinate across government and to actively engage South East Asian countries around critical cyber issues brought government and industry together to jointly develop Australia's International Cyber Engagement Strategy, released in October 2017. The benefits of a shared mission advanced through public-private collaboration, and engaging international allies, can have reinforcing benefits at home and abroad. International cyber norms are still in their infancy and subject to much multilateral negotiations, led in Australia's case by their Ambassador for Cyber Affairs.

Collaboration between industry and government takes many forms. It exists along a spectrum, ranging from traditional stakeholder management to highly integrated partnerships involving the co-creation of complex solutions. The countries studied have explored, experimented and implemented various programs and initiatives along this spectrum with varying degrees of success. While Canada's allies continue to make measurable progress in this area, CADSI's research suggests that Canada, despite having initiated some collaborative programs with industry, has been slow to move beyond basic forms of collaboration. A conceptual collaboration model is further described in the section Towards a Comprehensive Public-Private Collaboration Model for Cyber.

> Canada, despite having initiated some collaborative programs, has been slow to move beyond the most basic forms of collaboration.

By studying the collaborative practices of Canada's allies, CADSI has uncovered which ones have proven to be most effective for addressing specific cyber security challenges and has identified a set of common leading practices that are most likely to result in mutually beneficial collaboration between private industry and government. While recognizing that each country is different and has unique public governance and institutional contexts, this report proposes a comprehensive cyber security collaboration model. The Government of Canada can use this model to initiate a coordinated discussion around the best forms of collaboration to address their specific cyber challenges. It should also be noted that national cyber strategies in general are still emergent and while Canada's allies have each contributed to the composition of leading practices, none have yet integrated them together into a comprehensive framework. As such, the model and leading practices continue to evolve.

Finally, the report details specific recommendations to help Canada close the collaboration gap with its allies:

1. Innovation Science and Economic Development should create a Cyber Defence and Security Economic Strategy Table.

   • The Economic Strategy Tables are a new public-private collaboration approach launched by the Federal Government in 2017 that have already demonstrated early successes and contributed to important policy and regulatory changes by pairing industry executives with senior-level government officials to jointly develop strategies to tackle the most pressing challenges facing a sector.

2. The Federal Government should pilot a talent sharing mechanism with industry to respond to Canada's acute cyber talent shortage. Departments and agencies engaged in the pilot could include Public Safety Canada, the Canadian Centre for Cyber Security, and the Department of National Defence.

   • This program could be modeled after the U.K. Industry 100, a talent exchange framework administered by the National Cyber Security Centre that permits government and industry to jointly engage around emerging policy, innovation and operational challenges through short-term, embedded, corporate secondments.

3. Innovation Science and Economic Development (ISED) should compete one of the three cyber networks announced in Budget 2019 to permit proposals for the creation of an operational network focused on government-industry threat sharing, analysis, response, and solution testing.

   • One network could be competed to deliver an operational environment with a backbone, secure, physical and digital platform that is optimized to permit two-way threat information sharing, joint analysis and response, and the testing of solutions to live/real world problems.

NEW CHALLENGES
PRESENTED BY THE CYBER DOMAIN

Given the critical importance of the cyber domain to the safety and security of Canadian citizens, the success of industry and Canada's economic prosperity, securing cyberspace is a matter of urgency for the Government of Canada. At a national level, cyber defence and security entails providing protection from a wide range of malicious activities perpetrated by a combination of state and non-state actors looking to achieve various criminal, political or economic objectives. However, the unique characteristics of the cyber domain – outlined below – make defending against attacks of this kind a challenge unprecedented in scope.

1. **Cyber innovation is fast** – Major leaps in cyber innovation occur with relentless speed, making it extremely difficult for governments to keep pace and to mitigate the impact of new types of threats and malicious attacks in a timely fashion.

2. **Cyber infrastructure is owned by the private sector** – While governments share responsibility with industry for securing cyberspace, the private sector largely owns the infrastructure of cyberspace both nationally and internationally, making public-private collaboration an imperative.

3. **Threats from cyberspace are asymmetrical** – In the cyber realm, individuals and small groups of people have the capability to develop malicious technology quickly and cheaply and can use it to launch devastating cyberattacks on nation states quickly and with minimal cost. The economics of cyberspace favour the attacker.

> In Canada, 15 departments and agencies have direct cyber responsibilities, yet no central coordinating function to align mandates exists.

4. **Cyber pervades the other domains** – The cyber domain is unique in that it "pervades the other domains in the sense that warfighters in each of the prior domains would be severely handicapped if their access to cyberspace were successfully challenged." This has led some to believe that cyberspace is the new high ground of warfare, "the one domain to rule them all and in the ether bind them[5]."

5. **Cyberspace is human-made and highly malleable** – Cyberspace is different from the other domains in that it is human-made, but its malleability holds the potential to make it truly unique. As Martin Libicki notes, "the task in defending the network is not so much to maneuver better or apply more firepower in cyberspace but to change the particular features of one's own portion of cyberspace itself so that it is less tolerant of attack.[6]"

6. **Cyberspace was not designed with security in mind** – The architecture of cyberspace was "driven more by considerations of interoperability and efficiency than of security.[7]"

Not only is the cyber domain itself unique, governments tasked with securing it are not structured to address the many security problems it presents. Within the U.S. government, for example, "responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way[8]." In Canada, there are at least 15 different departments and agencies with direct cyber responsibilities, and no central coordinating function to align mandates – we are equally poorly structured to respond.

---

5 Cyberspace Is Not a Warfighting Domain, Journal of Law and Policy for the Information Society, Martin C. Libicki, Jan 2012.

6 Ibid.

7 Cyberspace Policy Review, United States Executive Office of the President, Apr 2014.

8 Ibid.

A SHIFT IN
COLLABORATIVE THINKING

Defining Collaboration

Collaboration is not a complex concept. It can, in fact, be summarized in ten words: "two or more people working together to achieve shared goals." At the most basic level, this could mean two people working together to replace a flat tire on a car. As larger groups of people work together to solve more difficult, multi-faceted problems, the collaborative process grows in complexity, and definitions of what constitutes collaboration begin to multiply and diverge. When these groups come from different organizational backgrounds with unique cultures, policies, assumptions, and priorities, effective collaboration can become quite challenging to define in concept and deliver in practice.

> Resolving the disconnect between government and industry in terms of what each wants and expects to gain from the other through collaboration is critical to success.

Collaboration between the public and private sectors is a prime example. This form of collaboration has been defined in many ways. Examined through the lens of "collaborative governance," it has been defined as "a governing arrangement where one or more public agencies directly engage non-state stakeholders in a collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets[9]." Alternatively, when examined through the "public-private-partnership" (P3) construct it has been defined as "an agreement between public and private actors to deliver certain services or perform certain tasks" and which may be "more focused around coordination rather than formal and consensus oriented decision-making[10]."

Within these definitions – and many others[11] – there is a broad spectrum of viewpoints on what constitutes collaboration between public and private sectors. It ranges from straightforward stakeholder information sharing and management activities, to highly cooperative partnerships in which government and its industry partners are engaged in the co-creation and delivery of solutions (see Figure 1 below). Resolving the disconnect between industry and government in terms of what each wants and expects to gain from the other through collaboration is critical to success.

---

9 Collaborative Governance in Theory and Practice, Journal of Public Administration Research and Theory, Chris Ansell and Alison Gash, Oct 2008.

10 Ibid.

11 For more information, see Freeman, 1997; Smith, 1998; Reilly, 1998; Padilla and Daigle, 1998; Beierle and Long, 1999; Walter and Petr, 2000; Seidenfeld, 2000; Prahalad and Ramaswamy, 2000; Connick and Innes, 2003; Porter and Kramer, 2011.

The New Collaboration Spectrum

Figure 1
The Public-Private Collaboration Spectrum
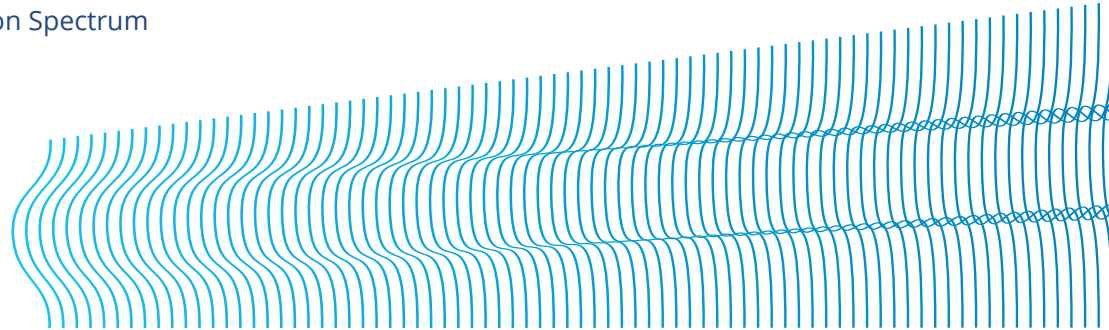
|	Level 1 **Inform**	Level 2 **Consult**
Primary Goal of Collaboration at this Level	To provide the private sector with balanced and objective information to assist them in understanding the problem, alternatives and/or solutions.	To obtain constructive feedback from the private sector on the analysis of the problem, or on solutions and alternatives developed by government to respond.
How it Plays Out in Practice	Government keeps the private sector informed on critical issues, but two-way communication is limited.	Government listens to the views of the private sector, and provides feedback on how this input influenced the decision-making process.

Fortunately, new research has begun to rationalize these divergent viewpoints. By positioning collaborative activities along a progressive spectrum where increasing responsibility and trust is placed in the private sector to identify and deliver solutions, a new model has emerged that sequences the previously disconnected collaboration activities (see Figure 1). Collaborative approaches situated on the left of the spectrum require minimal levels of two-way engagement between government and industry. They are therefore suitable to activities like awareness raising, communications campaigns, or traditional stakeholder management. Approaches situated on the right of the spectrum require more tightly integrated working relationships between government and industry, and a greater sharing of responsibility and accountability in the delivery of solutions. They are therefore more suitable to initiatives like the creation of talent exchange programs or rapid capability development centres. It is also worth noting that implicit "trust gates" must be passed to progress along the spectrum. Accountability for the creation of outcomes becomes increasingly shared, with the government divesting more of its responsibilities to non-state actors. (Figure 1, above, highlights this new collaboration spectrum.)
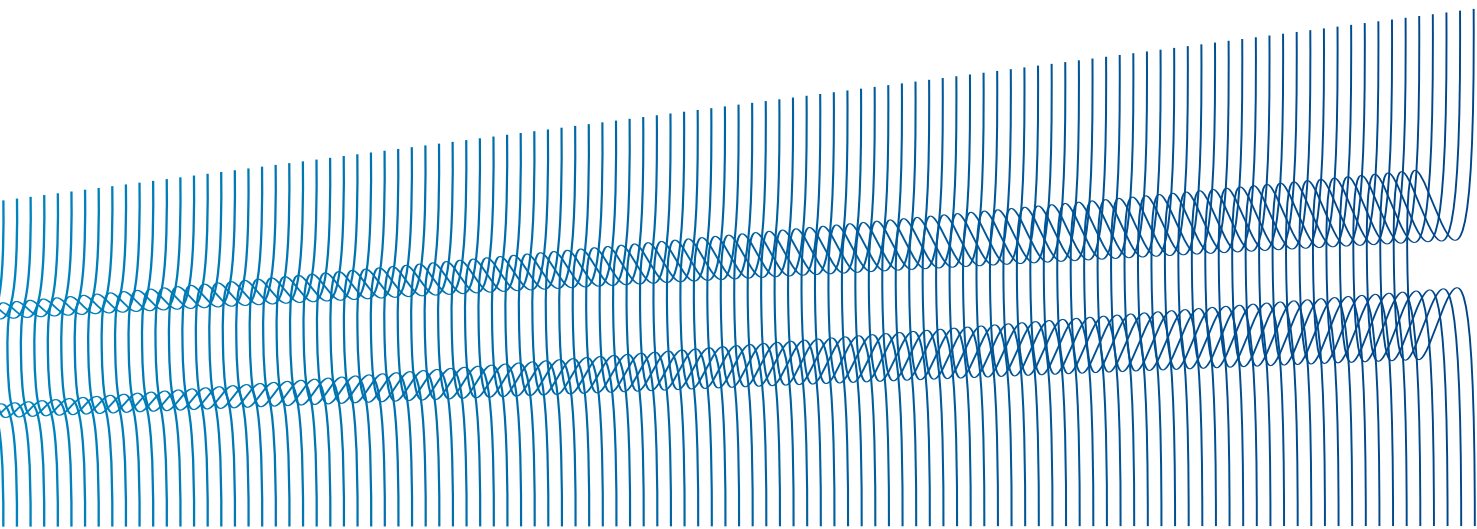
Level 3
Engage

To work directly and consistently with the private sector throughout the problem identification and analysis process, and in the formulation of solutions.

——————

Government works with private sector to ensure that industry input is directly reflected in the proper identification and analysis of the problem, and in the development of alternative solutions.

Level 4
Collaborate

To work with the private sector in each aspect of identification and resolution of the problem, placing reliance on the private sector in both the development and delivery of solutions.

——————

Government works hand-in-hand with the private sector at each stage of the problem's identification and the development of solutions, and trust's industry to play a defined role in delivering solutions.

Level 5
Lead

To place responsibility for the development and delivery of solutions in the hands of the private sector, supported by government where appropriate.

——————

Government divests its responsibility to resolve the problem to private sector counterparts, and puts in place controls to ensure appropriate implementation.

CADSI's research, which included interviews with cyber experts in government and industry, found that most forms of collaboration currently being employed by the Government of Canada operate between Stages 1 and 3. The new Cyber Security Cooperation Program recently launched by PSC, appears to be one of the few new mechanisms the government has formally employed to pierce into the fourth stage of collaboration. And although this program is new and unproven, it signals the government's intent to experiment with new arrangements where increasing trust and responsibility can be placed with industry to resolve some of Canada's most pressing cyber defence and national security challenges.

THE COLLABORATION IMPERATIVE IN
CYBER DEFENCE AND SECURITY

Why do governments value collaboration?

Governments are ill-equipped to tackle the challenges of cyber defence and security on their own. The nature of "cyber power" is changing and evolving at a pace that is too rapid for existing public sector governance models, procurement systems, and decision-making frameworks to respond. As one interview subject noted, "cyber represents a challenge well beyond the skill sets, resources, capabilities or knowledge of any one player."

New knowledge, technologies, tools and practices are radiating outwards in all directions at an increasing rate. Our allies have now openly acknowledged that keeping pace with the relentless expansion of the digital/cyber frontier has passed a tipping point – no longer can any single organization marshal the requisite intellectual capacity or operational footprint to encompass the task alone. Protecting the utility of the cyber domain requires partnerships with a broad set of stakeholders to remain knowledgeable of advancements at key inflection points along this new technological frontier, and to remain connected to the expertise and skillsets that can quickly operationalize new capabilities to counter adversarial innovations. (See Figure 2 on the next page.)

For democratic market economies like Canada, this issue is further compounded by the fact that key adversaries and rivals, including China and Russia, do not face the same administrative, legal or ethical burdens which hamper agility and reduce the speed of new technology acquisition. With their nationalized telecommunications and security industries, which closely collaborate with, assist, or are controlled by a combination of state intelligence services, the military, government research labs and (on occasion) organized crime, these adversaries are well equipped to innovate rapidly and operate offensively against Canada and its allies. These state actors recognize the porous interoperability within their cyber ecosystems as a primary strategic advantage and are maximizing their efforts to exploit it.

> Protecting the utility of the cyber domain requires partnerships with the broadest set of stakeholders to remain connected to rapidly emerging knowledge and skillsets along this new technological frontier.

What does the private sector have to offer?

Democratic market economies need not face their cyber adversaries alone. In Canada, and in the countries studied, the private sector offers a wealth of proven expertise and a diverse and powerful set of capabilities that governments alone do not possess.

Private sector firms own and manage the majority of the country's critical infrastructure and have unique insights into how the domain can be reshaped with security in mind. They are also the primary drivers of cyber innovation in technologies, tools and practices, and are persistently engaged in developing innovative new capabilities to solve real-world cyber challenges. They have also proven their ability to provide a range of critical cyber solutions and services to public and private organizations through a constantly evolving arsenal of defensive and offensive capabilities.

Increasingly, private sector firms are becoming the prime targets of the cyber domain's most advanced and persistent attackers, and this front line exposure gives them unique insights into how the cyber threat is morphing, enabling them to rapidly identify capability gaps, and close them through the development of new technologies, tools, and practices at cyber speed (in 10 months or less). The areas where Canadian cyber companies have proven capabilities are set out in CADSI's March 2019 report titled, "From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence."
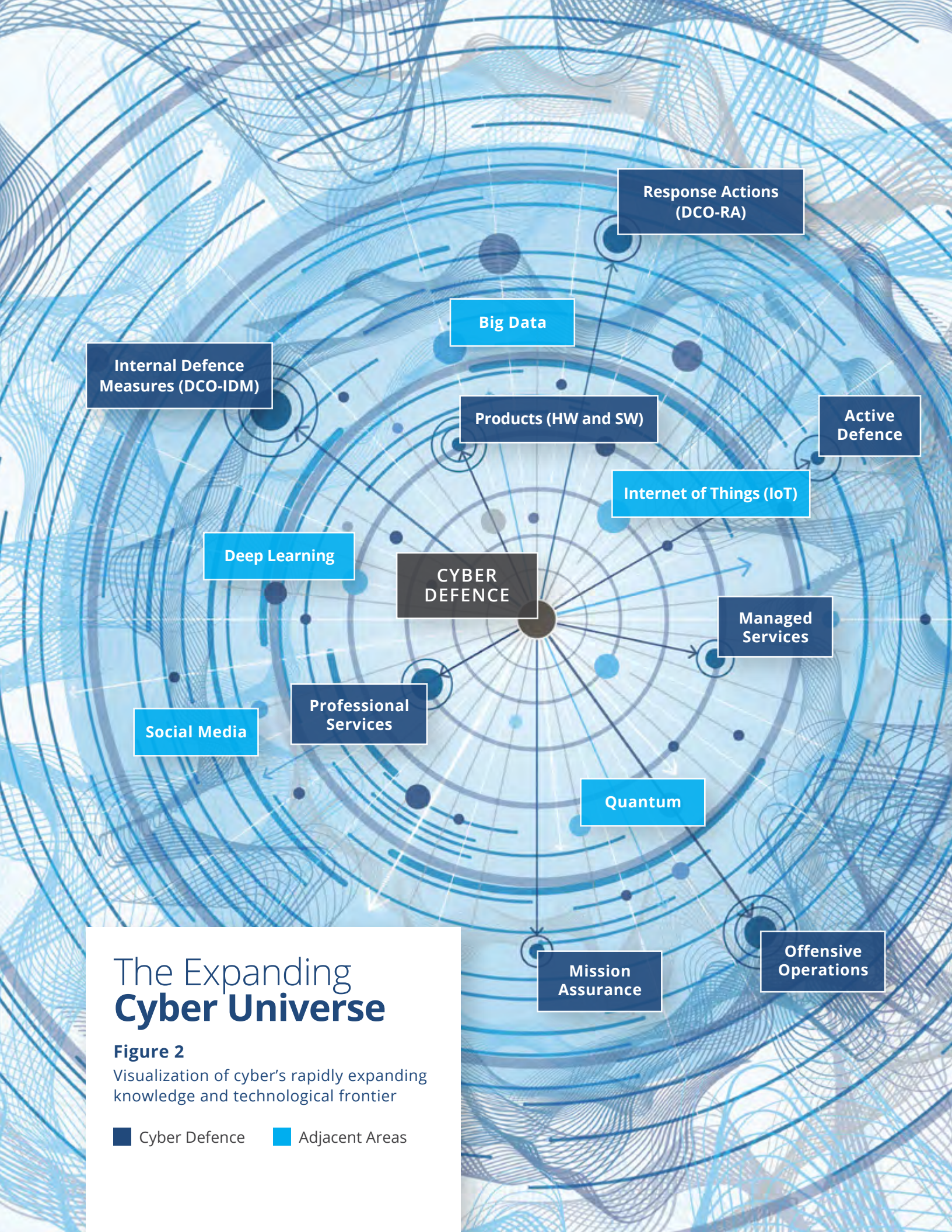
The Expanding Cyber Universe

Figure 2

Visualization of cyber's rapidly expanding knowledge and technological frontier

- Cyber Defence
- Adjacent Areas

Response Actions (DCO-RA)

Big Data

Internal Defence Measures (DCO-IDM)

Products (HW and SW)

Active Defence

Internet of Things (IoT)

Deep Learning

CYBER DEFENCE

Managed Services

Social Media

Professional Services

Quantum

Mission Assurance

Offensive Operations

Consider the following heuristic. The growth of the digital domain in some ways has been like the Big Bang – we have created a new and expanding digital universe in what amounts to the blink of an eye. But as opposed to a violent explosion of matter through all directions of space, digital technologies have exploded through and interconnected nearly every facet of our society. A 2016 report by the Internet Security Alliance concluded that digital technologies "affect virtually every aspect of our lives from our physiology to our identity, how we develop and manage relationships, the meaning of core values such as privacy, and many of the assumptions we have long held about national issues such as economics and national defense." Most importantly, this universe is continuing to expand in all directions, at an ever increasing rate.

Keeping pace with the relentless expansion of cyber's technological frontier has passed a tipping point - no single organization can encompass this task alone. And this new reality presents one inevitable conclusion: protecting the utility of the cyber domain requires partnerships with the broadest set of stakeholders: to remain knowledgeable of advancements all along this new technological frontier; to remain connected to the expertise and emerging skillsets that can quickly operationalize new capabilities; and to counter adversarial innovations wherever they arise. Partnerships and collaborative relationships must be sought and secured with those at this new frontier to have any chance of success, and they must be pursued with a vigour and intensity that matches the underlying explosiveness of the domain.

TOWARDS A COMPREHENSIVE PUBLIC-PRIVATE **COLLABORATION MODEL FOR CYBER DEFENCE**

All of Canada's key allies are actively engaged in multiple forms of collaboration with the private sector to address challenges across the entire cyber security domain. Not only are they forging strong relationships with the private sector, which will be invaluable as they look to become increasingly agile in the face of rapid innovation in cyber; they are also improving their ability to defend government, businesses and citizens against current threats and laying the foundation for a united approach that will mitigate the impact of cyberattacks and cyber aggression by adversary states.

While CADSI's research makes clear the value that Canada's allies place on public-private collaboration in cyber defence, it has also yielded a list of success factors and leading practices they use. When examined in aggregate, these success factors and practices can be combined to lay the foundation for a comprehensive public-private collaboration model for cyber defence, one that can be flexibly tailored and selectively implemented to directly respond to a country's unique cyber environment and challenge set.

However, it is important to note that none of Canada's allies have yet developed, tested or implemented models or strategies that connect their full complement of collaborative activities into a unified framework. A few have begun to experiment and combine activities like rapid capability development with real or simulated operational testing environments. None have developed an overarching framework that aligns a concentration of collaborative resources and programs around a common set of objectives and shared outcomes between government and industry.

There are likely several reasons for this, one of the most obvious being that most collaborative activities have emerged within our allies' systems in response to urgent needs, rather than according to deliberate long term planning. It is also unlikely that any cyber expert would have been able to predict the ways in which

> Canada needs to develop more comprehensive strategies that connect overlapping areas of cyber influence and capability, and the means to anticipate how our adversaries will use these, in combination, against us.

cyber and digital technologies would begin to overlap with one another, producing unexpected results. For example, the combination of big data analytics, online psychological and voter profiling, social media influence campaigns, advanced behavior modification techniques, and weaponized communications algorithms used to influence voters and elections on a global scale (see Brexit and Cambridge Analytica). But now that the proverbial cat is out of the bag, countries will need to begin to develop more comprehensive strategies that connect more of these overlapping areas of cyber/ digital influence and capability together and develop the means to anticipate how various combinations could be used against Canada.

LEADING COLLABORATION FUNCTIONS, **POLICIES, AND PRACTICES FROM CANADA'S ALLIES**

Every country has unique geopolitical, economic, social and cultural realities, and when combined with different ecosystem structures, policy and operational environments, it is unlikely that a single, prescribed collaboration model would serve the needs of all. As one government interview subjected noted, "best practices are not always portable between nations or even departments, because you do have to recognize that governments are fundamentally different." Notwithstanding, Canada's allies have found success with a focused set of practices within their own environments. Some may have the potential to be applicable within the Canadian environment. All will provide useful insights to improve the effectiveness and adaptability of Canada's current approaches to public-private collaboration in cyber defence.

Viewed in aggregate, they can be grouped with relative accuracy into four focused areas of cyber collaboration:

1. Governance, strategy, policy, and programs

2. Missions and operations

3. Protection of critical assets

4. Technology development

New areas may be added in the future as new activities, enabling policies and leading practices emerge and are validated. For now, the 16 leading practices identified and validated through case study analysis and expert interviews, can be grouped logically into this structure.

Leading Activities,
Policies and Practices

Governance, Strategy, Policy and Programs

- Permanent National Level Coordination and Cooperation Structures

- Collaborative Governance Structures in Program Delivery

- Procurement Reform

- Other Transactional Authorities

- Urgent Operational Requirements

Missions and Operations

- Deep Contractor Integration into Government Operations

- Cyber Experimental Ranges and Capability Testing Environments

- Talent Exchange Programs

- Scenario Planning and Joint Exercises

Protection of Critical Assets

- Jointly Developed Critical Infrastructure Protection Frameworks

- Information Sharing and Analysis Centres

Technology Development

- Cyber Accelerators and Innovation Hubs

- Rapid Capability Development and Deployment Centres

- Collaborative Research and Development Agreements

- Technology Roadmaps

- Industry Managed Innovation and Collaboration Networks

1. Governance, Strategy, Policy and Programs

1.a. Permanent National Level Coordination and Cooperation Structures

The United States strives to maximize the consistency of cyber defence and security policy, strategy and operations among departments, agencies, and with the private sector – a significant coordination and governance effort. These investments have paid dividends.

In the spring of 2012, for example, the government successfully collaborated with industry partners to mitigate the impact of a major distributed denial of service (DDoS) attack on U.S. banks. Working with 120 countries across diplomatic, technological and operational levels, they were able cut off the brunt of the malicious traffic at nodes around the world. While these measures did not stop the attacks altogether, the adverse impact on the banks was significantly reduced[12], allowing them to gain a foothold and re-establish control of their systems. This outcome was made possible because of recurring discussions and scenario planning activities that were permanently housed within the supporting constructs of the National Infrastructure Protection Plan (NIPP), specifically its match-made Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). Through the NIPP framework, government and industry's key stakeholders had already had lengthy discussions focused on developing a joint response to a similar attack originating from within the U.S., and had already participated in exercises to this effect. When this multi-national attack was launched, the existing plan was scaled quickly. Everyone knew their part, knew what they needed to get their international counterparts to do, and knew the exact steps to guide them through, to successfully dismantle the attack. Most importantly, when other departments and agencies had to get engaged (e.g. the State Department) they were able to accept working with industry more quickly and directly – they were already vouched for by existing government partners and had built longstanding relationships that engendered trust.

This example demonstrated that these collaborative constructs, traditionally constrained to a narrower and more defensive view of critical infrastructure protection, could be used to support a broader suite of strategic, operational, and coordination activities. This trend has taken flight with various SSCs contributing to high level policy, programming, operational and economic discussions and engaging their GCC counterparts.

1.b. Collaborative Governance Structures in Program Delivery

An overarching theme that emerged from both the research and interview phases of this report is the critical importance of well-defined and clearly communicated roles for all players in a public-private collaboration. Many interview subjects noted that without a clear and equitable division of responsibilities and tasks, with shared accountabilities, successful collaboration is not possible. In the U.S., the development of the IT Sector Baseline Risk Assessment was a successful collaborative initiative undertaken by government and industry. Among the success factors praised by both industry and government participants was the designation of co-chairs from industry and government, which "ensured joint accountability and authority, with defined roles and responsibilities for each co-chair[13]." The NIPP example noted above also derives much of its success from the paired SSC / GCC construct, which ensures an equivalent level of joint government-industry control over activity planning and delivery, and equally emphasizes a shared accountability for the creation of outcomes.

1.c. Procurement Reform

The interview subjects consulted for this research project repeatedly cited the need for the Government of Canada to adopt leading practices for the procurement of cyber products and services. Private sector executives interviewed for the study suggested that when compared to existing government procurement practices, which focus on meeting detailed requirements and lowest-cost compliance, capability-based approaches to procurement provide the benefits of being simpler, faster, more precise and more efficient. Canadian industries have a genuine

interest in helping ensure cyber security. Outcome-focused, capability-based approaches are important and there is significant upside value in establishing independent contract authorities. The importance of procurement to successful long-term collaboration cannot be understated. One senior government interviewee noted, "if we can't then acquire the fruits of our joint labour, no one is going to be happy, and the will to collaborate will disappear." Significantly, Canada lacks a recurring government-industry mechanism to discuss these and other regulatory and economic issues impacting the cyber security environment. Constructs like the Economic Strategy Tables seem tailor-made to address this cadre of issues, and have achieved some success in Canada to date.

> "If we can't then acquire the fruits of our joint labour, no one is going to be happy, and the will to collaborate will disappear."

1.d. Other Transactional Authorities

A leading collaboration enabler cited throughout the project interviews were the Other Transactional Authorities (OTAs). Employed by the U.S. Department of Defense's (DoD) Defense Innovation Unit (DIU), among many others, OTAs are a mechanism intended to simplify defence acquisitions in specific areas and exist in parallel to procurement rules used for traditional defence systems. The U.S. DoD has permanent authority to award "Other Transactions" for research, prototype development and production purposes, which gives it the "flexibility necessary to adopt and incorporate business practices that reflect commercial industry standards and leading practices into its award instruments[14]." The turning point for OTAs, which have been in existence for quite some time, but only recently gained more wide-spread recognition and use, was when procurement officers were mandated to use them unless they could come up with a compelling and defensible reason not to – a necessary shift in emphasis, which was viewed as critical to their rise to prominence. Currently, they sit at the core of many U.S. programs that aim to create environments where government and industry can jointly work together to identify, develop, test, and field solutions to emerging problems.

1.e. Urgent Operational Requirements

The U.S. defence procurement system was improved through the adoption of another leading enabler, Urgent Operational Requirements (UORs). Since standard DoD processes were not leading to swift fielding in the early 2000s[15], the U.S. widely recognized the importance of responding coherently and rapidly in the complex security environment of the 21st century. The U.S. has applied UORs to the area of cyber defence as well. Among the family of U.S. procurements instruments, UORs are akin to cousins of the OTAs, permitting DoD (and others) to activate special procurement channels, that by-pass more cumbersome and traditional vehicles, though not restricted to R&D/rapid prototyping activities.

---

12 U.S. Rallied Multinational Response to 2012 Cyberattack on American Banks, Washington Post, Ellen Nakashima, Apr 2014.

13 Best Practices for Operating Government-Industry Partnerships in Cyber Security, Journal of Strategic Security, Larry Clinton, Winter 2015.

14 Other Transaction Authority Guide, Defense Acquisition University, Dec 2018.

15 Fulfillment of Urgent Operational Needs, University of Maryland, Jacques Gansler, Apr 2010.

2. Missions and Operations

2.a. Deep Contractor Integration into Government Operations

Building on the successful joint response to the U.S. Banking System's 2012 DDoS attack, in its National Security Strategy (2018), the U.S. Department of Defense (DoD) further emphasized the need for collaboration with industry partners in both the physical and cyber domains. To carry out its cyber priorities, the U.S. government reaffirmed its commitment, and its intended mechanisms, to collaborate extensively with private industry, including using industry knowledge, tools, and expert resources to augment government efforts. Across the board, Canada's allies encourage and rely on far greater civilian/contractor integration into sensitive networks and operational environments (reaching a 50/50 balance according to those interviewed with extensive experience in allied operations). Canadian national security agencies seem exceptionally reticent to accept and adopt this practice, on occasion going so far as to view this reliance on civilian/contractor integration as an internal deficiency as opposed to a strategic asset.

> Canada's allies encourage and rely on far greater civilian/contractor integration into sensitive networks and operational environments, sometimes achieving as much as a 50/50 balance.

2.b. Cyber Experimental Ranges and Capability Testing Environments

Many interview subjects raised the concept and value of a Cyber Experimental Range, which is an experimental or virtual proving ground where industry and government can assess potential and emerging technologies and de-risk solutions using unique government and military generated, controlled or owned data and networks where they exist. For example, in some countries studied, only the military has the real-world data of how a complex weapons system operates and interacts with other such systems in a battlefield environment. Transposing this data into a Cyber Experimental Range allows qualified firms to test and develop improved solutions to mission assurance and resiliency in these systems and to identify possible inter-dependencies between systems and adversarial tactics. For smaller innovators, who may not be able to afford full-scale test and evaluation, a Cyber Experimental Range offers an environment where emerging solutions can be tested against known challenges and combined with their own data from the systems they have developed. For government, it provides an opportunity to assess solutions and get a better understanding of state-of-the-art developments. For industry participants, the government provides access to unique datasets and modelled networks along with requirements and challenges they are unlikely to encounter in the private sector, and an opportunity to receive feedback from the military or national security end-users.

2.c. Talent Exchanges

In the U.K., the Industry 100 program enables industry experts to work directly with the National Cyber Security Center (NCSC). These experts are assigned bespoke short-term placements at the NCSC, typically on a part-time basis, which gives them an opportunity to understand and challenge the way government thinks and tests innovative ideas inside the government environment. Overall, Industry 100 promotes greater mutual understanding of cyber security, better cyber policy, improves delivery of programs, helps both government and industry identify systemic vulnerabilities, and reduces the future impact of cyberattacks.

3. Collaboration in the Protection of Critical Assets

3.a. Critical Infrastructure Protection Frameworks

In the U.S., the development of the National Infrastructure Protection Plan (NIPP) was held up by both government and industry participants as a successful collaboration leading to the creation of an effective framework for protecting the U.S.'s suite of critical infrastructure assets. The government engaged CI owners and operators throughout the development of the NIPP, reflecting industry language and recommendation at each stage of the plan's development. Government also demonstrated, at senior levels, a strong commitment to, and stewardship of, the development of the plan, and in leading the outreach and engagement to a broad base of CI stakeholders. Most importantly, the ongoing delivery of the plan is overseen by paired government and industry coordinating councils for each CI sector, ensuring that permanent government-industry collaboration drives the plan's delivery.

3.b. Information Sharing and Analysis Centres (ISACS)

Most allied countries pursue some level of government-industry collaboration in the sharing of cyber threat information, vulnerabilities and breaches. Debates rage as to whether participation in these types of constructs should be voluntary or regulated, with industry and a majority of academics favouring a voluntary and incentivized approach. The concept of sharing threat information across a diverse array of trusted actors to gain dramatically improved situational awareness is recognized as a critical component to an effective national cyber defence. It remains one of the forms of collaboration most highly prized by government and industry, although for somewhat different (and sometimes conflicting) reasons. The governments that have created these networks hope to gain access to private sensors, networks and data, and to be notified immediately of breaches into critical private systems. Private sector participants want equal access to sensitive government intelligence and operational knowledge that will often be classified, or may belong to competitors that have provided it to the government, as well as guidance on what kind of information governments finds most useful as a consumer of threat intelligence.

4. Technology Development

4.a. Cyber Accelerators and Innovation Hubs

The U.K.'s NCSC Cyber Accelerator supports the growth of start-up cyber companies working to bring better, faster and cheaper cyber security products to market. Launched in 2017, the program has since helped 16 start-ups with technical, leadership and advisory support. In addition, the country's CyberInvest program brings together key players from government and industry to invest and support the development of cutting-edge cyber security research across the U.K.'s academic sector. Twenty-four companies that are the members of CyberInvest have committed to invest a minimum of £8M over the next five years.

In Australia, AustCyber acts as a multiplier and connector to establish Australia as a recognized leader in the global cyber marketplace. Cyber Security Innovation Nodes have been set up throughout the country to serve as hubs for start-ups, corporations, universities, and government agencies to share information and drive innovation. Australia has also founded the Cooperative Research Centre for Cyber Security (CSCRC) to facilitate industry-led commercialization and R&D for cyber security.

4.b. Rapid Capability Development and Deployment Centres

Among the collaborative initiatives studied, those designed to accelerate the co-creation of technology solutions for cyber defense and security are perhaps most highly valued by both industry and government. The U.S. Army Futures Command (ACF) is one such program that is emerging as a leading method for government collaboration with industry and for procuring solutions at the "speed of cyber." Starting with the foundational questions, "what technology is necessary to complete our mission?" and "who are the innovators in the space?", U.S. AFC aims to modernize the Army's capability through direct R&D collaboration and acquisition from small-medium enterprises (SMEs) and academia, and aims to deliver these collaborative outcomes by co-locating facilities in innovation hubs throughout the U.S. to get the best and brightest minds focused on the Army's biggest challenges.

4.c. Cooperative Research and Development Agreements (CRADAs)

Similar in some respects to the Cyber Experimental Range, Cooperative Research and Development Agreements (CRADAs) are a written agreement between a government agency (often a defence lab) and a private party or university to work together on the research and development of new technologies. The CRADA model is highly valuable for small tech firms, as it facilitates technology transfer and offers a low-risk opportunity to collaborate and build relationships with defence labs. While CRADAs do not provide funding, they allow defence labs to provide staff, access to facilities, equipment, data, and other resources to private firms with or without repayment.

> The policies, tools and practices outlined herein have the potential, in combination, to lay the foundation for an exceptionally strong whole-of-nation cyber defence framework.

4.d. Technology Road Maps

Technology Road Maps (TRMs) for cyber security and defence were another leading practice cited by interview subjects. TRMs support strategic, long-term planning of product and service developments, forecast against a predicted technology horizon and resulting set of government procurement requirements, and are sustained through structured and meaningful dialogue between government and industry participants. For TRMs to be effective, it is critical that long-term goals are supported and aligned to short and medium-term deliveries of specific technology solutions. This can serve as a capability development process where industry and government work together to define the technological horizon and related challenges; produce a market analysis of the anticipated market demand and resulting developments in technology supply; develop a list of preferred solutions; assess and address challenges presented by existing policy and program instruments; and, ultimately, connect the sequence of proposed solutions to an evolution of upcoming government procurements. Niteworks in the U.K. and the Australian Rapid Prototyping, Development and Evaluation (RPDE) program, that has since been fully integrated into their Defence Innovation Hub, are examples of this.

4.e. Industry Managed Innovation and Collaboration Networks

In some cases, leading prime contractors with well-established government client relationships and proven track records in complex systems integration are experienced at navigating the procurement landscape while remaining flexible enough to incorporate new technologies and practices into their supply chains. In large part, this is because they create and manage their own innovation ecosystems. Opening these ecosystems to SMEs with leading capabilities that lack the resources to respond to detailed technical RFP requirements is one way to produce greater value-add in terms of commercializing the most cutting-edge innovations in cyber defence. In this model, the government only needs to maintain relationships with a few primes, who develop a detailed knowledge of their evolving requirements, and can tailor their supply chains to flexibly respond and deliver. In other cases, large primes and integrators can develop in-house venture capital funds or accelerators, or can form teams and joint ventures to promote more collaborative engagement with their supply chains, and deliver resulting benefits to government, while not simply adding cost premiums through layering of suppliers. These new approaches seek to:

- Lower the barriers to SME participation;

- Foster greater competition;

- Connect government with a wider array of leading-edge technologies tailored to their unique needs;

- Position the collaborative activity largely on the industry side; and

- Focus on a few higher-level public-private relationships that set the tone for the downstream engagements.

This concept is still emerging. It is favoured by larger OEMs/integrators and some government officials. The impact on SMEs and the long-term, sustained health of the industrial base is not clear.

More than the Sum of their Parts

The current slate of leading cyber collaboration practices has arisen at different times, in different jurisdictions, and in response to different but equally urgent crises, which is to say in no way in an organized or strategic fashion. However, viewed in aggregate they present a surprisingly powerful cyber defence construct. They offer a menu of collaborative activities, enabling policies and emerging practices that countries can review to identify and select custom solutions tailored to their unique cyber environment. Implemented through collaborative partnerships with a broad range of industry, academic, and other government stakeholders, they have the potential, in combination, to lay the foundation for an exceptionally strong whole-of-nation cyber defence.

CORE FACTORS
LEADING TO SUCCESSFUL COLLABORATION

A review of six case studies of cyber-focused collaboration projects released by the U.S. Department of Homeland Security, and further supported by academic research into new concepts like "collective impact[16]" (Stanford) and "shared value creation[17]" (Harvard), 15 core principles and collaboration success factors have been identified that "consistently generate successful partnership programs on both a substantive and operational maintenance level.[18]"

These success factors are different from the 16 leading allied activities, policies and practices noted above, and are more geared towards managing a healthy and productive relationship between government and industry throughout the collaborative process.

> "Solving problems is about substance and relationships, and most people ignore the relationships." Doing so in cyber will surely lead to failure.

As noted by one interview participant, "solving any problem is about substance and relationships, and most people ignore the relationships." While the activities, policies, and practices noted above address the substantive elements of what must be done to respond to select cyber challenges, the success factors outlined below should be regarded as a combination of model principles and behaviours that, if held to, present the best chance to build successful collaborative relationships between government and industry from which successful activities can flow unimpeded. Fifteen core success factors are outlined below:

1. Government should seek private sector insight early, ideally at the initial priority, goal and objective setting phase of any collaborative project, not just at implementation.

2. A common agenda should be developed that drives participants to reach a shared vision for what must be done, and establishes clarity around what each participant is willing to commit to the development and delivery of solutions.

3. Senior government and industry executives must commit to the collaboration and this commitment must be consistently communicated and demonstrated to engaged and supporting staff and stakeholders.

4. A recognized model or process, that has already gained the confidence of government and industry stakeholders, should be used wherever possible to structure collaborative activities. Ideally this would be a model that itself has been developed with industry input (e.g. U.S. NIPP, Canada's NCSF and Economic Strategy Tables).

5. Stakeholder outreach should be broad, and begin early, ideally at the "blank page" stage.

6. Continuous interaction and communication must be maintained between government and industry stakeholders. This can occur through permanent and recurring fora, or through regular interactions, emailing, and commitments and deliveries against joint project work. This communication and interaction is vital to coordinating joint activities, building trust and maintaining project momentum.

7. Government must provide adequate time for stakeholders to review and respond to materials, requests for decision, etc. (equivalent to the time required for the government to review and respond to similar issues).

8. Co-leadership or mutually acceptable shared-leadership roles should be created across programs and activities (government and industry can each take the lead in areas that best suit them, but the overarching collaboration requires a sense of equitable leadership).

9. Decision making should be consensus-based by default. Any exceptions must be communicated to stakeholders early and transparently.

10. Activities should be mutually reinforcing to ensure that although not all participants are doing the same thing to contribute towards project goals, each is investing its energies and resources where it can have the greatest impact, while reinforcing the activities of others.

11. Stakeholder input must be genuinely respected and utilized (when someone takes the time to contribute their ideas to the collaboration, they should see them reflected).

12. Relevant/impacted government agencies must be adequately engaged and represented (sometimes this means that government has do to some of the work to convince their counterparts of the value and importance of the engaging in the initiative).

13. Government and industry must follow through on partnership related decisions, ideally with progress measured against a mutually identified set of success metrics.

14. Measurement of progress should be shared and simple, ideally delivered through a single, unified and short list of indicators.

15. Adequate and competent support services are critical to coordinating joint activities, arranging for discussions and meetings, maintaining communications, tracking project progress, identifying improvements, and providing backbone administrative support.[19,20]

Collaborative activities pursued in concert by public and private stakeholders will have a much greater chance of success if they can ensure that the 15 core success factors noted above are reflected and deliberately woven into the fabric of any new collaborative arrangements. While these core factors were tested and proven by Canada's allies, they do not by themselves guarantee the success of any future collaboration. Their absence, through omission or willful ignorance, will almost certainly contribute to failure.

16 Collective Impact, Standford Social Innovation Review, John Kania and Mark Kramer, Winter 2011.

17 The Ecosystem of Shared Value Creation, Harvard Business Review, Mark Kramer and Marc Pfitzer, Oct 2016.

18 Best Practices for Operating Government-Industry Partnerships in Cyber Security, Journal of Strategic Security, Larry Clinton, Winter 2015.

19 Kania and Kramer, Ibid.

20 Kramer and Pfitzer, Ibid.

PRIORITIZING
PRIVATE SECTOR PARTNERS

At an operational level, collaborative initiatives with the private sector should be targeted at organizations "that are best positioned to take cybersecurity actions on behalf of the largest possible constituency; have access to cybersecurity information and intelligence that can be used for protection and can be shared broadly; or have high-level national or economic security relevance and are positioned to contribute to cybersecurity on a systemic basis." These can be broken down into five categories of private sector entities:

- Cybersecurity providers;

- Telecommunications and Internet Service Providers (ISPs);

- Information technology companies (hardware, software, and service providers);

- Systemically important critical infrastructure sector companies; and

- Information sharing organizations that have developed particular cybersecurity capabilities and information sources[21].

In pursuing collaborative activities with industry, these are the core stakeholder groups that governments need to ensure are represented at senior levels.

---

21 An Operational Collaboration Framework for Cybersecurity, Aspen Cybersecurity Group, Nov 2018.

CONCLUSION

Together, the focus areas, supporting activities, enabling policies and leading practices, core success factors, guiding principles, and prioritized partner list can be assembled into a close approximation of a comprehensive public-private collaboration model for national cyber defence.

> The list of prioritized partners can provide government with a jumping off point to reach out immediately to a focused set of firms with the recognized potential to impact the broadest set of cyber systems and environments.

Utilizing this model as a baseline, governments can first identify their core cyber challenges, and then look to determine if collaboration could be helpful in finding and developing solutions. If the challenges fall within the scope of one of the four focus areas of collaboration, specific activities can then be identified with the capacity to respond, and the potential effectiveness and delivery method of alternative solutions can be explored. At this stage, governments can then consider initiating collaborative discussions or engagements with industry and can use the success factors and guiding principles to form a strong relational foundation to ensure a mutually productive and rewarding collaborative engagement. Finally, the initial list of prioritized partners can provide government with an effective jumping off point to reach out immediately to a focused set of firms with the recognized potential to impact the broadest combined set of cyber systems and environments.

Although initially positioned as a comprehensive model, when the current level and maturity of public-private collaboration in cyber defence in Canada is taken into consideration (described as "nascent" by several interview respondents), this model is likely best used selectively, to identify one or two priority areas where Canada faces seemingly intractable cyber challenges, and where industry can support the delivery of successful solutions through collaborative arrangements. (See Figure 3)

Figure 3
A Proposed Model for Public Private Collaboration in
National Cyber Defence

Focus Areas Where Collaboration Can Help to Solve Cyber Challenges	Specific Activities, Policies and Practices That Can Be Engaged to Respond	Success Factors and Guiding Principles to Ensure Productive and Healthy Collaboration	Prioritized List of Industry Partners to Engage
Governance, Strategy, Policy and Programs	• Permanent National Level Coordination and Cooperation Structures • Collaborative Governance Structures in Program Delivery • Procurement Reform • Other Transactional Authorities • Urgent Operational Requirements	• Government should seek private sector insight early, ideally at the initial priority, goal and objective setting phase • A common agenda should be developed that drives participants to reach a shared vision for what must be done • Senior government and industry executives must commit to the collaboration and demonstrate this commitment consistently • A recognized model or process should be used wherever possible to structure collaborative activities	• Cybersecurity providers • Telecommunications and Internet Service Providers (ISPs) • Information technology companies (hardware, software, and service providers)
Missions and Operations	• Deep Contractor Integration into Government Operations • Cyber Experimental Ranges and Capability Testing Environments • Talent Exchange Programs • Scenario Planning and Joint Exercises	• Stakeholder outreach should be broad, and begin early • Continuous interaction and communication must be maintained between government and industry stakeholders • Government must provide adequate time for stakeholders to review and respond to materials, requests for decision, etc. • Co-leadership or mutually acceptable shared-leadership roles should be created across programs and activities	• Systemically important critical infrastructure owners and operators • Information sharing organizations with access to public and/ or private sources of threat and breach information.
Protection of Critical Assets	• Jointly Developed Critical Infrastructure Protection Frameworks • Information Sharing and Analysis Centres	• Decision making should be consensus-based • Activities should be mutually reinforcing • Stakeholder input must be genuinely respected and utilized	
Technology Development	• Cyber Accelerators and Innovation Hubs • Rapid Capability Development and Deployment Centres • Collaborative Research and Development Agreements • Technology Roadmaps • Industry Managed Innovation and Collaboration Networks	• Relevant/impacted government agencies must be adequately engaged and represented • Government and industry must follow through on partnership decisions • Measurement of progress should be shared and simple, ideally delivered through a single, unified and short list of indicators • Adequate and competent support services and backbone administrative support are critical to success	

RECOMMENDATIONS

Based on the research reviewed for this study and informed through extensive interviews and follow-up discussions with leading cyber experts in private and public sectors, CADSI has identified three priority actions and initiatives that the Government of Canada should pursue to improve public-private collaboration in cyber defence. The recommendations build on existing Canadian constructs and programming where possible, take inspiration from allied leading practices, and are listed in sequence.

> "Lack of trust and dialogue" was consistently stated as the number one contributing reason for the current lag in collaboration in cyber defence.

Lead Recommendation (near term: 1-2 years)

1. Innovation, Science and Economic Development Canada (ISED) should create a Cyber Defence and Security Economic Strategy Table (EST).

- "Lack of trust and dialogue" was consistently stated as the number one contributing reason for the current lag in Canadian government-industry collaboration in cyber defence. An EST would allow for a recurring forum to support strategic discussions and joint planning between government and industry, setting a process to address the relational, economic, and policy barriers mutually agreed to be holding back collaboration in cyber defence.

- The ESTs are a new public-private collaboration approach launched by the federal government in 2017 (additional ESTs launched in 2019) to identify and remove barriers to growth facing key sectors of the economy.

- The ESTs have already demonstrated early successes, contributing to important policy and regulatory changes by pairing industry executives with senior-level government officials to jointly develop strategies to tackle the most pressing challenges facing a sector.

- The proposed Cyber Defence and Security EST should be distinct from the existing Digital EST. The Digital EST is focused on the proliferation of technologies throughout society; the Cyber Defence and Security EST would be focused on ensuring the benefits of this proliferation can be sustained in the face of mounting cyber aggression and attacks against governments, citizens and businesses. They are on opposite sides of the same bitcoin, and essential to each other.

Supporting Recommendations (mid-term: 2-3 years)

The medium-term recommendations focus on the delivery of admittedly more ambitious collaborative projects and aim to respond to the growing cyber talent gap and the lack of digital environments to support joint research, analysis, testing, and operations. These types of activities move collaboration further along the spectrum (see Figure 1), and begin to encompass not only joint planning, but joint development and delivery of solutions, and shared accountability for outcomes. They also require greater trust between partners, and confidence in each other's commitment and ability to complete tasks and deliver outcomes that advance joint objectives. As such, they should follow sequentially from the first recommendation.

2. The Communication Security Establishment (CSE) should pilot a talent sharing mechanism with industry to respond to Canada's acute cyber talent shortage.

- This program could be modeled after the U.K.'s Industry 100 and run by CSE's new Canadian Centre for Cyber Security (CCCS). This approach would mirror the successful U.K. model, which is run by the National Cyber Security Centre (NCSC) within the larger Government Communications Headquarters (GCHQ) construct.

- The exchange program could be structured similarly to the Industry 100, which permits government and industry to jointly engage around emerging policy, innovation and operational challenges through short-term, embedded, corporate secondments.

- These exchanges could be piloted in less sensitive areas (e.g. Data Analytics, Skills Forecasting) to first build trust between government and industry participants, before integrating into more sensitive areas (e.g. Attribution, Active Defence).

3. Innovation, Science and Economic Development Canada (ISED) should compete one of the three cyber networks announced in Budget 2019 to permit proposals for the creation of an operational network focused on government-industry threat sharing, analysis, response, and solution testing.

- As opposed to the traditional research-type networks typically supported by government funding, one network could create an operational environment with a backbone, secure physical network that is optimized to permit two-way threat information sharing, joint analysis and response, and the testing of solutions to live/real world problems.

- This could create a physical and virtual collaboration platform between government and industry focused on cyber threats with national security and defence implications.

- Existing public and private threat sharing assets could be integrated into this network.

It should be noted that CADSI has not directly addressed procurement reform in these recommendations. Procuring at cyber speed is a critical issue that our government must resolve, but a report focused on collaboration was not the place for such a discussion. CADSI will be pursuing follow-on research into cyber procurement best practices, and recognizes that our current acquisition system remains a substantial impediment to effective national cyber security and defence.

Annex A: Report Methodology

The methodology for this report involved reviewing, assessing, and identifying global leading practices, models, and programs of government-industry collaboration in cyber defence and security. The report examined the following three broad categories: policy, operational and international engagement. The policy aspect included the following functions: cyber security and defence governance, procurement, and talent development as key components; the operational aspect included functions of collaboration to prepare cyber capabilities, monitor, identify, report, and respond to cyber threats as well as information sharing, and coordination of the threat response. Recognizing the borderless nature of both the threat and market opportunities, the role of international allies and other nations was captured by examining the following functions under the international engagement category: interoperability (from operations to procurement) with allies within leading practices and differences in policy or legislation in other countries' models that enable a leading practice or effective cooperation, collaboration, partnerships, or procurement to inform a new Canadian model for collaboration and partnerships between the public and private sector.

Initial findings from examining and assessing publicly available and CADSI-provided reports, publications, news articles and other sources of information were validated and enriched by conducting interviews with subject matter experts from the Canadian government, industry and international partners. CADSI developed 5-6 key questions on governance and leading practices to allow for comparison of answers. These questions were provided to interviewees in advance. A total of 20 interviews were conducted. Focus was given to those most knowledgeable about cyber defence operations in Canada, U.S., U.K. and Australia.

The report outlines an idealized government-industry collaboration model in cyber defence and security including critical functions and activities as a foundation for a comparison of Canada with its allies. All recommendations made are supported by specific examples of successful cyber defence and security collaboration models and mechanisms in other nations and/or interview findings. This evidence constitutes the main body of the report.

Annex B: Key Contributors to Research & Recommendations

CADSI, as part of its ongoing efforts to promote Canada's innovative cyber defence sector, created a new Cyber Advisory Council. The Council is made up of industry cyber defence practitioners who provide ongoing feedback on CADSI's activities and research efforts in the cyber domain, as well as offering input as the association works to form closer links between home-grown industry and government.

CADSI's recommendations are designed to move collaboration further along the spectrum to encompass not only joint planning, but joint development and delivery of solutions, and shared accountability for outcomes.

The Cyber Advisory Council was instrumental in the development of this report and its recommendations, and is comprised of the following individuals.

Al Amlani
Director Cyber Operations,
General Dynamics Mission Systems – Canada

Chris Bartlett
President
CCX Technologies

Shaun Covell
Director
Sapper Labs

Al Dillon
Chief Operating Office
Root9B-C

Steve Drennan
Director Cyber Security
& Enterprise Risk Management
ADGA

Bill Dunnion
Director Cyber Resilience
Calian

BGen Rob Mazzolin (Retired)
Chief Cyber Security Strategist RHEA Group
Former Vice-Director Plans & Policy
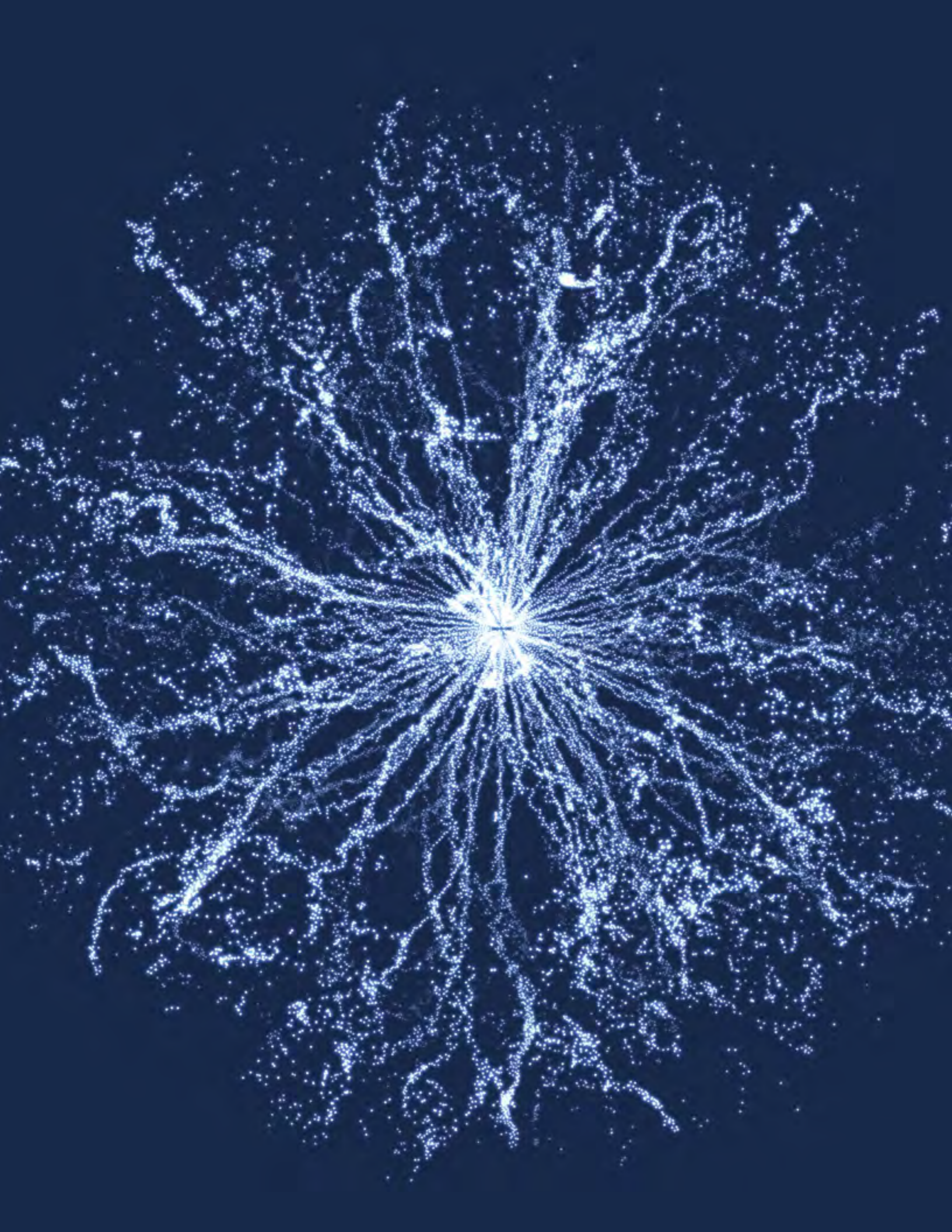U.S. Cyber Command

Dave McMahon (Chair)
Principal
Clairvoyance Cyber Corporation

Daina Proctor
Associate Partner, Security Intelligence
& Operations Consulting,
IBM

Rafal Rohozinski
Chief Executive Officer
SecDev

**Canadian Association of Defence
and Security Industries**

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

defenceandsecurity.ca
@cadsicanada