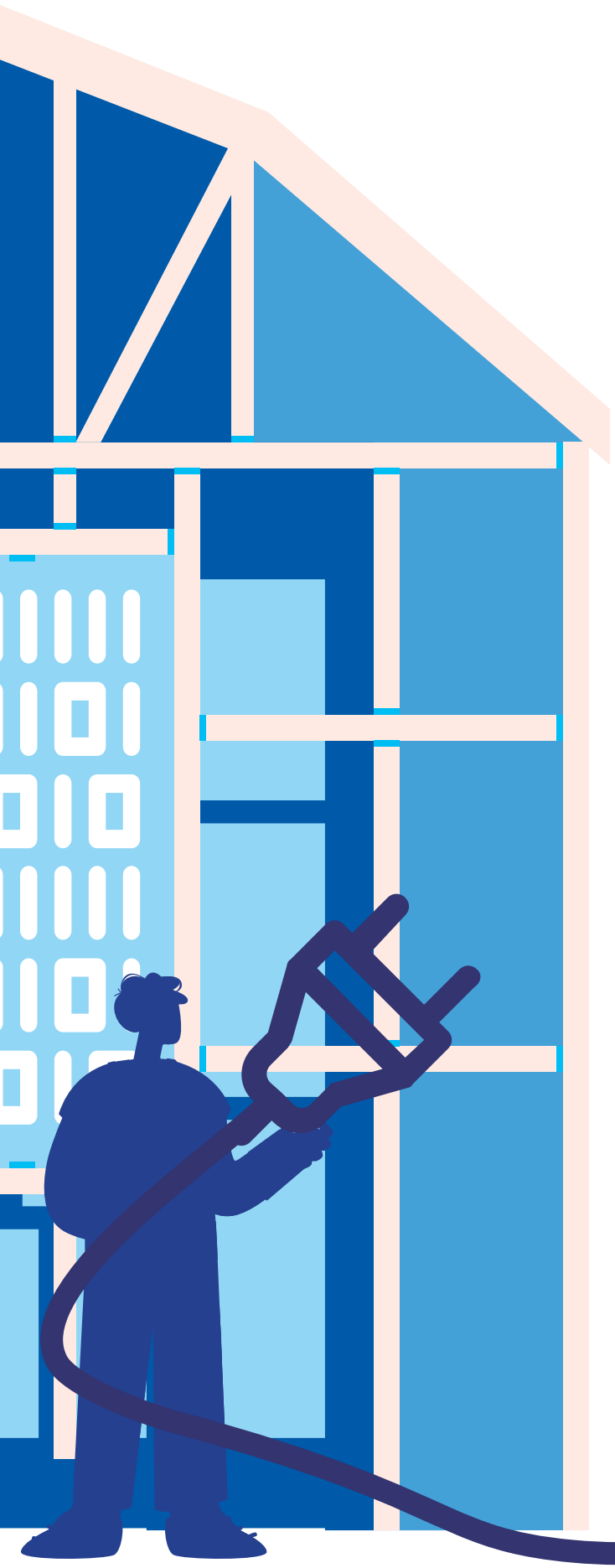
CYBER BARN RAISING™

A Framework and Recommendations for Strengthening Cyber Resilience in Canadian Agriculture

November 2022

CSKA
Community Safety Knowledge Alliance
Research to Practice to Alignment



November, 2022

This report is one of a series of knowledge products by the Community Safety Knowledge Alliance for the Cyber Security Capacity in Canadian Agriculture initiative.

Partly funded by Canada

CSKA Community Safety Knowledge Alliance
Research to Practice to Alignment

The Community Safety Knowledge Alliance (CSKA) is a non-profit corporation that supports governments and others in developing, implementing and assessing new approaches to improving community safety and wellbeing outcomes.

www.cskacanada.ca

Contributors:
Janos Botschner
with
Cal Corley
Evan Fraser
Ritesh Kotak
Dave McMahon

Preface

As part of Public Safety Canada's commitment to build a safe and resilient Canada, the Cyber Security Cooperation Program (CSCP) is supporting projects that contribute to security and prosperity in the digital age while positioning Canada as a global leader in cyber security.

The CSCP is aligned to The National Cyber Security Strategy (NCSS), which describes the Government of Canada's vision for cyber security. The NCSS has three key goals, which provide a focus for the activities and investments funded by the Government of Canada, and also serve to guide projects funded through the CSCP.

- Goal 1: Secure and Resilient Canadian Systems;
- Goal 2: An Innovative and Adaptive Cyber Ecosystem; and
- Goal 3: Effective Leadership, Governance and Collaboration.

This document provides a framework for cybersecurity in the agricultural sector, together with four recommended areas of activity focused on collaborative capacity building involving government and the private sector. It is a result of a multi-year research initiative, Cyber Security Capacity in Canadian Agriculture – funded through CSCP and conducted by the Community Safety Knowledge Alliance. This initiative aims to strengthen cybersecurity capacity across Canada's agricultural ecosystem[1].

In addition to a summary of research conducted as part of this initiative[2], a set of producer-facing resources is being released up to the end of 2024.

Key Findings and Features of Cyber Barn Raising

Food production occupies a unique position. It is a critical infrastructure at the intersection of several other critical infrastructures. It also contributes to the health of all Canadians, and is a driver of national prosperity. For these and other reasons, the integrity and vitality of this system is an issue of national security and resilience. Investing in cybersecurity capacity in Canadian agriculture can also be thought of as investing in the prosperity and resilience of the country, as a whole. This isn't something that can be done in isolation of other sectors, or the broader context of Canada in the world today. It's a journey that involves joined-up effort.

The evolving agri-food system is a vital part of the Canadian economy. The Fourth Industrial Revolution is poised to transform agriculture by revolutionizing how we produce food and how we distribute it. Canada is positioned to become an agri-food 'superpower'.

Producers, as business people and entrepreneurs, are at the front lines of maintaining strong and resilient communities while also contributing to sustainable development goals.

Next-generation equipment – and information flows within the Internet of Things – are giving producers the opportunity to manage each unit of production – whether land, lab, greenhouse or animal – in near real-time.

Food security is national security, but it is under threat. When food systems are compromised by cyber incidents, we are all affected.

While digital technologies are creating many benefits, they also have vulnerabilities that can be exploited for criminal or other offensive purposes. The agri-food sector is becoming a growing target for cyber attacks, but cybersecurity has not been a top priority for agricultural producers. While total security can't be achieved, preparedness and resilience can be greatly strengthened through collaboration and farmer-centred support.

We can strengthen cyber preparedness and resilience across the agricultural sector through Cyber Barn Raising.

We outline an adaptive approach to strengthening cyber resilience in Canadian agriculture by building networked capacity for sustained collaboration and support. We call this *Cyber Barn Raising*. It involves four areas of activity spanning the agri-food value-chain and its ecosystem:

- Producer-centred support for on-farm cybersecurity
- Cross-sector partnerships
- Workforce capacity development
- Strengthened governance to strengthen trust

Agriculture is Key to Canadian Prosperity and Wellbeing, but it's Under Threat

We Need to Strengthen the Sector's Resilience Now

The agri-food system is a vital part of the Canadian economy and our global position. Producers, as business people and entrepreneurs, are at the front lines of maintaining strong and resilient communities.

As a critical infrastructure[3], the food supply chain – from farm to fork – is essential to the health and wellbeing of Canadians and our country.

During the course of the COVID-19 pandemic, this supply chain, and the people upon which it is based, demonstrated its resilience, despite the vulnerability of its multiple interdependencies and just-in-time processes. This is remarkable, at a time when, globally, nearly every industry has been experiencing supply shortages owing to shipping and transport challenges across borders and oceans.

Evolving food systems capable of supporting eight billion people is one of the 21st century's key global challenges. Nationwide, a renewed public policy conversation is helping to position Canada as a global leader in food quality and productivity, informed by sustainable development goals. In the face of these challenges and opportunities, strong and resilient rural communities will be essential contributors to the health of Canada's economy, and of Canadians.

An important new value proposition for the agricultural sector is emerging based on the role it can play in addressing: emissions; global food security; the quality and characteristics of our domestic food supply chain; and the economic and health impacts on millions of Canadians – particularly those living in rural areas.

The opportunity for transformative innovation in the agricultural sector has been recognized at the highest policy levels. The federal finance minister's Advisory Council for Economic Growth[4] recommended that investments in agricultural technology are one of the most strategic ways of growing Canada's economy. Their report's findings were echoed by the Senate of Canada's 2019 report on growing Canada's value-added food sector[5], the BC Premier's Food Security Task Force[6], and the new federal Food Policy for Canada. From this we note widespread enthusiasm about the potential for digital innovation to radically transform this vital sector of Canada's economy..

The Fourth Industrial Revolution (4IR)[7], featuring robotics, big data and artificial intelligence, blockchain technologies, nanotechnology and low-cost sensors is poised to transform agriculture by revolutionizing how we produce food and how we distribute it. While digital transformation is not without its challenges[8], next-generation equipment – along with agronomic and other data analytic services – are giving producers the opportunity to manage each unit of production – whether land, lab, greenhouse or animal – in near real-time. These "precision agriculture" or "smart farming" technologies promise to boost productivity and profitability and to enhance traceability.

In addition to driving economic growth, digitalization also can help farmers use inputs such as antibiotics or fertilizers more precisely, and lessen harmful outputs (emissions, waste and land disturbance), benefitting agriculture's environmental footprint.

The growth of these connected devices, machine-to-machine communication and smart devices – the internet of things (IoT)[9] – is generating unprecedented flows of data within and across communications networks. But, this comes at a potential cost in terms of the potential for security breaches.

> *"The information flows within the IoT are creating not just benefits, but also vulnerabilities that can be exploited for criminal and offensive purposes[10]."*

Attention to cyber security has grown over the past decade. Public awareness has tended to focus on threats to privacy, proprietary data, and industrial control systems associated largely with financial services, health services, and telecommunications.

Less attention has been paid to digital agriculture and how risk management should be conceptualised in this sector[11], even though a recent survey of Canadian businesses found that over a fifth had been impacted by cybersecurity incidents in the preceding year[12].

Insights[13] from our present research echoed findings from other jurisdications[14] – namely, that cybersecurity is not a high priority for agricultural producers, despite suggestions that up to about one-in-ten may have experienced attempted or successful cyber events. And, while industry associations may exercise great care in safeguarding their own digital assets, less attention has often been paid to ways of supporting their members in strengthening on-farm cybersecurity preparedness.

> *At present, cybersecurity is not a top priority across the agricultural sector.*

A series of incidents in Canada, the US, the UK and Australia in 2021 and 2022 showed just how vulnerable this infrastructure can be[15].

- In 2021, the network of global meat processing company JBS was attacked by a Russian cyber crime organization[16], resulting in the shutdown of some US plants and potential data loss. This ultimately caused a shortage in the meat supply and drove up wholesale prices by 25 percent.
- The Australian Wool Exchange was paralyzed for a week early in 2021, with losses of between $60M and $80M AUD[17].
- A ransomware attack on the National Milk Records systems disabled services to UK dairy farmers for a month in 2019[18].
- During the 2021 harvest – a stressful season for producers – an attack by Russian hackers on the farmer member-owned corn and soy products producer, New Cooperative in Iowa, threatened the movement of 40 percent of US grain production that runs through its software[19].
- In the same week, Crystal Valley Co-op, which serves 2,500 farmers and livestock producers in southern Minnesota and northern Iowa, was hit with a similar ransomware attack attributed to the same group[20].
- When Schreiber Foods, one of the largest milk processors in Wisconsin, was subjected to a ransomware attack in the autumn of 2021, the milk supply chain was disrupted for 5 days[21].
- In November 2022, Maple Leaf Foods, Canada's largest prepared meats and poultry producer, experienced a widespread outage resulting from a cybersecurity incident[22].
- That same month, Sobeys filed data breach reports that were widely presumed to have resulted from some type of cybersecurity incident[23].

Looking ahead, we can anticipate a rise in ransomware attacks on 'softer' (more vulnerable to disruption) targets in the agricultural sector. Two examples make this point – one reflecting current practices, and one reflecting emerging business opportunities related to climate adaptation:

- Livestock operations depend on a narrow range of environmental conditions. If a poultry, swine or egg producer's environmental control systems are disrupted during the warmest or the coldest seasons of the year, the resulting losses would be significant, not only for the farm business, but also from an animal welfare perspective and possibly also for the mental health of the farm family.
- As new opportunities emerge related to carbon sequestration, land ownership and automation could play big roles in profitability for farmers. Should rapid adoption of carbon credit technologies take place without sufficient foresight around cybersecurity, 'carbon farms' and their financial infrastructures will become targets of opportunity for criminal and nation-state actors.

An area receiving less attention involves exploits aimed at influencing attitudes and behaviour. Prior to the recent surge in ransomware attacks, a number of influence operations targeted elements of agri-food supply chains:

- In 2019, China insinuated that Canadian canola and pork were tainted, and banned shipments from Canadian companies without producing scientific evidence to back its claims[24]. These trade-related moves happened in the context of rising geopolitical tensions between China and Canada.
- A decade earlier, in the midst of a fight by Potash Corporation of Saskatchewan against a multi-billion dollar hostile takeover attempt by an Australian mining conglomerate, law firms for both sides, as well as the federal Department of Finance and Treasury Board, were attacked by cyber criminals believed to be based in China[25]. Chinese interests had been strenuously opposed to the transaction and the attacks appeared to be focused on disrupting the process.
- A year before the 2016 US presidential election, a disinformation campaign perpetrated against a Pennsylvania turkey farm was uncovered by the Wallstreet Journal, which attributed the source to Russia's Internet Research Agency[26]. This appeared to be a test run of the use of social media to propagate and amplify mistrust.
- Two years following the 2016 election, an automated Russian social media disinformation campaign attempted to create a scare about the use of herbicides and GMO crops within US agriculture[27]. This took place against a backdrop of Russia's increasing reliance on agricultural exports as a source of revenue, tied to aspirations to be the world's largest supplier of GMO-free food[28].

With costs potentially reaching into billions of dollars, we could see massive economic repercussions, and significant collateral damage to public trust and social stability, should vulnerabilities of our agri-food system be further targeted. Although the sector is largely decentralized, there are several key pinch-points, from farm to fork. Targeting these, or combining attacks on specific commodity producers with rapidly-scalable influence operations, could trigger cascading disruptions across the system. In the case of international conflict, targeting of smaller 'softer' targets, like groups of individual farms, and agri-food supply chains, could be expected as a run-up to, and follow-up from, attacks on 'harder' infrastructures – exposing the sector to two waves of attacks.

As a result of the growing reliance of agriculture on information communications technology (ICT), the cyber preparedness and resilience of this critical infrastructure must move to the forefront of efforts to ensure sustainable system performance.

"[Although the idea of] total security is an illusion" [29]
preparedness and resilience can be greatly strengthened through collaboration and support.

Resilience is Boosted Through Networks of Support and Can be Transformative

New research is challenging the assumption that managing threats to stability or wellbeing is about possessing the right combination of characteristics and technical safeguards. We're also learning that resilience can mean more than helping organizations or systems recover to a state that existed before a cyber incident occurred.

Whether we're thinking about individuals[30], organizations[31], communities or nation states[32], we need to consider: environmental conditions; the availability of key resources; and the people processes that provide support to access needed resources. These are the assets that can help organizations and individuals adapt – and maybe even transform – in the face of complex challenges[33].

The traditional notion of resilience has to do with the capacity to withstand stressful events or circumstances while maintaining a core functionality[34]. It often refers to: the properties of structural components like building materials that can *maintain* their functional role of *withstanding* stress without breaking; or natural systems, like lakes and oceans, that return to a steady-state environment for plants and animals, despite fluctuations in temperature[35].

A newer way to think about resilience focuses on:

> *"the ability and capacity of individuals, organizations, and structures to cope, adapt, and recover from shocks and stresses, in a way that reduces the overall vulnerability to similar shocks and stresses in the long term … and is … the capacity to 'bounce back better'… [including]… the capacity to learn from past experiences and improve (even transform) institutions and systems."* [36]

Organizations under constant threat can learn how to protect themselves and adapt to changing circumstances, building more resilience than those that live in walled gardens and are confronted by a threat for the first time. This has been evident throughout the COVID-19 pandemic, as organizations have been forced to digitally transform overnight, adopting cloud-based solutions and learning how to support and benefit from remote work arrangements.

> ***"Resilience is not a do-it-yourself endeavor…***
> ***[It] depends more on what we receive than on what we have."*** [37]

Building on the idea of resilience as a process of learning and development, Ungar's work with children, vulnerable populations, and community-based interventions in the aftermath of disasters, emphasized that resilience goes beyond maintaining a static level of resources. He argues that it depends more on the right resources being available when they are needed, and that they are relevant to those needing help[38]. In other words, resources and solutions need to be present, accessible and understandable to users. These supports need to make sense, from the standpoint of personal[39], organizational or business contexts.

Dupont, Shearing and colleagues[40] explored the implications of a refined definition of resilience for today's cybersecurity challenges. They proposed that cyber resilience involves a broader range of factors than the engineered features of a cyber physical system that might help it survive disruptions.

Drawing from The National Academies (2012) definition of disaster resilience, as a shared responsibility that should involve individuals, organizations and governments, Dupont, et al. proposed a holistic view of cyber resilience that encompasses the activities (preparations, responses, recovery and adaptation) that enhance an organization's ability to deliver intended outcomes *despite* disruptions[41]. They observed that, even when an organization's conventional cybersecurity measures (which are aimed at predicting and preventing adverse events[42]) have been overwhelmed, the process of grappling with a massive disruption can sometimes trigger an equally significant process of adaptation. They suggested that "the ultimate goal of resilience is not survival until the next crisis but adaptation to a dynamic environment to reach a new state of equilibrium[43]". This view emphasizes that there is more to cyber resilience than business continuity and disaster recovery.

The speed of cyber and the global reach of threat actors will require an updated conceptualization of cyber resilience as a human-based set of practices and processes, as well as more dynamic and adaptive technologies, enabled by artificial intelligence and machine learning.

Traditional disaster response models underpinning business continuity were designed for events like earthquakes, floods and hurricanes, not the increasingly dynamic and evolving cyber threat landscape[44].

From a critical infrastructure perspective, traditional technology-based cyber resilience schemes don't fully recognize the importance of relationships among organizations within an ecosystem, and the degree to which even competitors may rely on one another's stability as part of sustaining business operations within a larger marketplace. They also tend to focus on business recovery, instead of on opportunities to learn from and transform, in the midst of evolving threat landscapes.

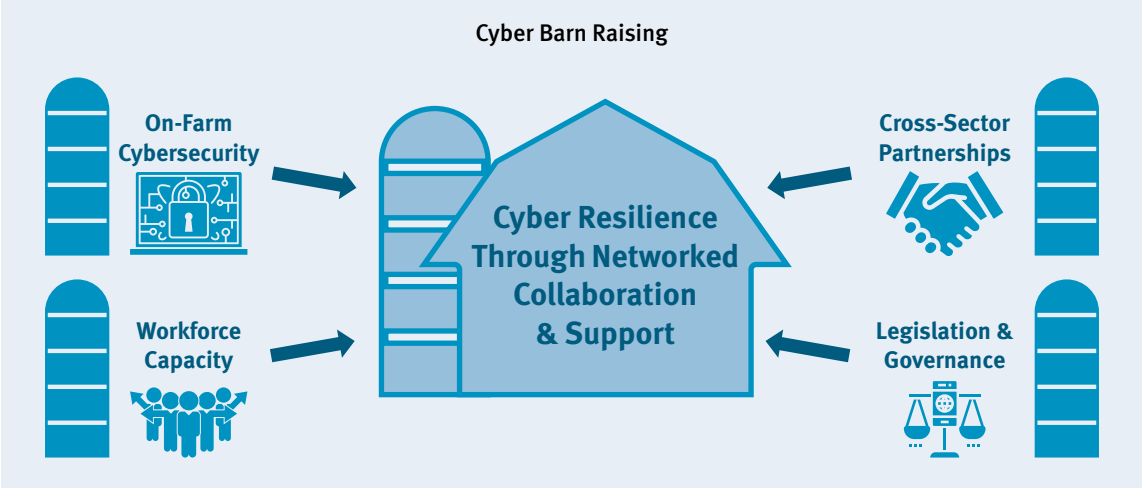
Failure should not be a starting point for security.

From a values perspective, it will be equally important to consider where we want investments in resilience to be made, and what kinds of transformations will be most aligned with broader goals such as those related to sustainable development[45].

Cyber Barn Raising: A Framework and Recommendations

A Framework for Resilience Through Partnership and Collaboration

An adaptive approach to strengthening cyber resilience in Canadian agriculture is possible. It can be achieved by building networked capacity for sustained collaboration and support. We call this *Cyber Barn Raising*.



On-Farm Cybersecurity

Understanding the business context of farming and the related objectives for a cyber physical system are essential to ensure well-informed decisions pertaining to developing and maintaining an effective cyber security posture.

Situational awareness should be integrated with all business functions in the context of the cyber threat landscape the business inhabits. This includes an internal view to 'threats to' and an external focus on 'threats from'. It also means thinking about the situations that make careful decision-making difficult for producers – notably, busy and stressful times of the year like planting and harvesting. This underscores the value of integrated risk management.

As cyber-enabled incidents become more complex and multi-layered, our understanding of smart farming architecture also needs to evolve. There's a growing recognition that, in addition to the physical, network and application security layers attention must also be paid to the 'cognitive' layer – that is, the human mind and human behaviour as a focus of attack.

Social engineering (e.g., phishing and business email fraud) typically exploit this layer to gain access to the other layers of an IT system. By tuning their practiced situational awareness to cybersecurity threats and implementing basic cyber hygiene practices, there is a lot that producers can do to improve their on-farm cybersecurity posture. But, they should not have to do this alone – responsibility for cyber resilience of entire agri-food sector, as-a-whole, needs to be shared across the system. Capacity building should start with the producers in mind, and build security and resilience by involving all key players.

Producers should not be left to shoulder the task of strengthening cyber resilience across the agri-food sector – this needs to be a shared undertaking.

Cross-Sector Partnerships

The opportunities and risks associated with the digitalization of agriculture should be a shared interest and a shared concern. Food security is also national security. If our agri-food system is compromised, we are all affected. If it thrives by adapting to climate disruptions, we all stand to benefit.

The opportunities and risks associated with the digitalization of agriculture should be a matter of shared interest and shared concern. Food security is also national security. If our food systems are compromised, we are all affected.

Crafting a more adaptive and resilient food system requires collaboration – to understand opportunities and risks, and to address them in effective and sustainable ways. Safety is not so much the absence of threat, but the presence of connection" [46]

In the Netherlands, the National Cyber Security Centre (NCSC) of the Ministry of Justice and Security has been engaged in facilitating sectoral cooperation to support organization cybersecurity.

Early work in the United States led to the creation of several initiatives whose intention was to foster collaboration between government and industry to secure a range of critical infrastructures. One such approach is a framework to enable sectoral stakeholders from the public and private sectors to develop collaborative information sharing and analysis centres (ISACs)[47]. The rationale behind ISACs is that, by sharing information and analyzing cyber incidents together, participating organizations will be better informed about threats and countermeasures that make sense for their businesses. But, historically, the methods and resources required for achieving these partnerships were often asymmetrical – industry was tapped to carry the bulk of the financial and human resource burden[48], while having to meet government established compliance requirements. As NCSC documentation points out, the willingness of competitor organizations to participate voluntarily in sharing sensitive information through an ISAC depends on their capacity to foster and sustain trust.

In Canada, most critical infrastructures work with American ISACs because Canada does not currently have any. In this country, the relationship between critical infrastructure operators and government is primarily regulatory, rather than intentionally collaborative. Yet, collaboration is just what will be required. The complex and sometimes hybrid nature of transnational crime, projections of geo-political power, and the availability of malware-as-a-service to smaller-scale actors, mean that traditional approaches to cybersecurity are no longer enough . We will require more robust intra- and inter-sectoral capacities to predict, deter and prevent cyber incidents, along with a network of collective defence-in-depth spanning critical infrastructures. In some cases, this may extend to detection and deterrence. In other cases (under relevant legislative authorities), this may involve degrading and disrupting the capacity of actors to instigate attacks on the agri-food system.

Fulfilling the promise, while addressing the perils of the new era in agricultural production, will benefit from a diversity of perspectives. A producer-centric approach should also include sectoral and commodity organizations, the private sector, NGOs, academe, and government. It will also be important to welcome into the conversation stakeholders reflecting a diversity of gender, socio-economic and ethnocultural backgrounds, including broad representation from equity-deserving groups – with a key place at the table for those involved in Indigenous food security. This will help to mobilise a broader range of insights to support effective learning and planning, while addressing inequities experienced by marginalized food system actors[49].

Workforce Capacity

Building a cyber-capable workforce also supports innovation and economic activity[50]. This can involve the 'downstream' role of providing ongoing upskilling opportunities for those currently employed within an industrial sector. This will also need to involve the 'upstream' role traditionally filled by post-secondary institutions: preparing future generations of STEM professionals and practitioners – and agricultural operators to enter a workforce that is straining to keep pace with the demand for technically trained entry-level personnel and entrepreneurs.

It is generally acknowledged that, across all industries, there is a massive talent shortage in cybersecurity, and that STEM training alone will not solve a problem that affects everyone and belongs to everyone[51]. Deloitte (2018) reported an estimated global talent shortfall approaching 2 million workers for 2022. Canada has recognized that the demand for qualified cybersecurity practitioners is a significant opportunity for our country's workforce[52]. Among recommendations for addressing this workforce emergency is the idea of building local cybersecurity ecosystems based on connections to governmental organizations, industry groups and educational institutions[53].

In addition to filling the STEM pipeline with employment ready graduates, post-secondary institutions can plan more broadly to incorporate learning outcomes related to cybersecurity awareness into the design of many of their other programs, such as agricultural sciences and technology, business, and animal and plant sciences.

Awareness and training should also start early for children and youth, who may be interested in pursuing careers in Canada's agri-food sector.

Legislation, Governance, Standards & Incentives

Legislation, and other policy instruments – including data governance – need to be designed to address the full spectrum of interacting processes, opportunities and risks involved in the digital agricultural ecosystem. This includes producer and public trust in the people, processes and technologies that make up digital agriculture.

As The Conference Board of Canada has suggested, the governance structure for cyber resilience should be designed to suit specific needs and objectives[54]. This should also recognize that, as an ecosystem, these elements are part of dynamic, interacting feedback loops – no one piece should be considered in isolation of the others. And, because the core of the digital agricultural revolution is the collection and use of data[55], safeguarding the availability and integrity of data, and addressing concerns about confidentiality and data ownership need to be considered together.

Like other business sectors, attention to standards may help to advance cybersecurity maturity and resilience across the broader Canadian agri-food sector.

In 2023, the Strategic Advisory Group on Smart Farming (SAG SF) of the International Standards Organization (ISO) published a report [56] identifying specific, practical, opportunities for digital agricultural cybersecurity and standards to support Canadian food system security, safety, resilience and business continuity. The CSA Group and the American National Standards Institute led the development of a new bi-national standard for businesses, in general – CSA/ANSI T200:22, *Evaluation of software development and cybersecurity programs* [57]. This outlined a generally applicable maturity model approach aligned to the NIST Cybersecurity Framework to "help evaluate the organization's software development and cybersecurity practices related to IoT, operational technology and connected and embedded devices", to support "effective business decisions related to cybersecurity."

The successful development, implementation, adoption and utilization of cybersecurity standards across Canada's agri-food sector will depend on an understanding of both the technical and the human dimensions of our increasingly digitized food value chain.

Cybersecurity standards can be an enabler of constructive on-farm practice change benefitting individual producers, rural economic prosperity, Canada Brand, and Canada's geo-political position. They can also serve as encouragement to industry to refine, implement and clearly communicate cybersecurity safeguards across their equipment and services to strengthen and sustain transparency and trust with farm business consumers.

Recommendations

1. Take a producer-centred approach to strengthening on-farm cybersecurity

- Engage key stakeholder groups in the agricultural sector to build awareness of, and shared understanding about how cybersecurity can support both farm business risk management and farm business development, specifically :
    - Associated threats to the agri-food sector in general, and agricultural production in particular, as a critical infrastructure.
    - The business opportunities of digital technology, as an enabler of sustainable benefits involving productivity, profitability, and operational insights – for producers, for supply chain owners, for Canada and for the world.
- Address the organizational dimensions of on-farm cybersecurity practice:
    - Improve producer access to relevant information, technical services and supports.
    - Create producer-focused as incentives for improving on-farm cybersecurity posture across the country (e.g., retrofit and rebate programs[58] and credits).
- Build cyber advisory services into producer-facing products and services, concurrently creating new business opportunities for vendors, lenders and distributors.

2. Build and support cross-sector partnerships

- Convene and sustain an ecosystem roundtable and backbone structure to:
    - Enable the sharing of insights and the development, implementation and evaluation of all-of-ecosystem initiatives (including the present set of recommendations) at the speed of cyber – for example, by:
        - Sharing information related to system vulnerabilities and threats – including those relating to the global context of cyber crime, cyber espionage and cyber warfare.
        - Flagging and examining data governance concerns and opportunities to help strike the best balance among privacy, data ownership and control, intellectual property, incident reporting, and roles and responsibilities of stakeholders within the agricultural ecosystem and intersecting critical infrastructures and authorities.
        - Identifying and developing strategies and resources for rapid response and recovery.
        - Informing the development and revision of relevant standards and protocols.
        - Defending forward, where appropriate.
    - Update the National Cyber Security Strategy to incorporate those aspects specific to agriculture, including attention to relevant tie-ins to inter-connected critical infrastructures.
    - Ensure cross-pollination with operational policy development relating to: climate disruption; to public health and food security; to regional economics and international trade; to science and innovation; and to national security and national defence.

3. Develop workforce capacity

- Deliver continuing education and training on digital agricultural technology and cybersecurity to producers.
- Build the next generation of cyber-capable producers by developing and delivering educational and training opportunities to rural children and youth.
- Inform emerging cybersecurity professionals about issues and opportunities in Canada's agri-food sector by including digital agriculture as an element of educational curricula (including work integrated learning opportunities).
- Develop cybersecurity-focused secondment opportunities within and between departments and business units of the public and the agri-food sectors, as has been done between the Government of Canada and major telecommunications providers, among others.

4. Strengthen legislation, governance, standards & incentives to strengthen trust within the agricultural value chain

- Review relevant legislation and data governance frameworks for opportunities to strengthen cybersecurity capacity in Canadian agriculture:
    - Examine opportunities to balance privacy, ownership and intellectual property concerns to build trust as a basis for expanded digital technology adoption and collaboration.
    - Develop, implement and incentivize standard cyber incident reporting across the agricultural sector to strengthen its capacity for collaborative cybersecurity practices.
    - Federal and provincial governments should engage industry and producers to create shared expectations and policy and legislative mechanisms that require and reward practices that strengthen cyber resilience in the agri-food sector, for example:
        - Occupational health and safety legislation, and consumer protection legislation should be examined for potential analogies that might be applied to cyber hygiene within the agri-food sector.
    - Cyber insurance is a developing space. Government can help to shape this space in constructive ways by convening dialogue among providers of cyber insurance products, producer groups, and public and private actors from across the cybersecurity community.
    - Agriculture-specific cybersecurity standards may hold promise for the agri-food sector in several ways: as an opportunity to foreground cybersecurity as a new best management practice (BMP) in food production and farm business risk management; as a way of framing a developmental journey of developing cybersecurity capacity and preparedness among small and medium farm businesses; by inviting discussions of the different roles of producers, agricultural service providers and equipment manufacturers and suppliers in achieving and sustaining food system security; and as a basis for considering the role of standards in all-of-system cyber resilience.
        - Following from this work, insights and recommendations emerging from ISO SAG SF, and in the context of the evolving global threat environment, now is an opportune time to identify the best practical opportunities for digital agriculture cybersecurity standards to support Canadian food system security, safety and sustainability.
        - To take hold and become incorporated as a best management practice in farm business risk management and business development, cybersecurity standards for digital agriculture will have to be crafted with an eye to the practical needs, legitimate aspirations, and day-to-day challenges of Canadian farmers. Drawing an analogy to the consumer product safety movement of the 1960s and 1970s, standards should also reflect the role that technology vendors and service providers have in ensuring that the equipment and services they provide reflect a transparent commitment to the confidentiality, integrity and availability of agricultural data and processes.
        - Recognizing the current interest in the topic of 'right-to-repair', consideration should be given to the interplay between standards supporting interoperability and cybersecurity, the potential legislative and regulatory dimensions the may arrive, and the opportunities and challenges that may emerge for producers, equipment manufacturers and supply chains, as a result of technologies becoming more accessible

Conclusion

"One of the most common misconceptions about Internet security is that it is a technical problem. It is not. To address Internet security as a technical issue without simultaneously addressing the economic, human resource and other risk management issues is to fundamentally misunderstand the issue." [59]

Research on the cyber physical systems and cybersecurity dimension of smart farming is still in its infancy. Cyber-maturity in the sector appears to lag other critical infrastructures. Few approaches to cybersecurity in digital agriculture have considered the full complexity of the business opportunities and business risks that define agri-food in the 21st century.

This future is now. Increasingly, farm businesses, like many others, will need to consider supports for business continuity, along with cyber resilience, in addition to prevention, in their understandings of cybersecurity and its practices. Beyond the focus on risk management, cybersecurity also needs to be positioned as an enabler of farm business development and success.

The agri-food sector has an opportunity to make faster gains in improving its cybersecurity posture than have many other sectors, which started earlier, but developed capacity more slowly and more haphazardly.

The technical dimension of cybersecurity will always be a necessary part of all-of-ecosystem strategies for protecting Canada's critical infrastructures. But those behind cyber attacks know that exploiting the human element is the easiest road to disruption. This means that we must do more than protect critical infrastructures and safeguard data flows; we also need to cultivate awareness, deliver training and "protect what we know and how we know it."[60]

The preceding recommendations, along with other resources created through the Cyber Security in Canadian Agriculture initiative, have been designed to address these neglected, but essential elements of critical infrastructure protection and defence.

This starts with people: individual producers; organizations; systems; and governments. It is helped where shared understanding can be created and shared effort can be fostered, in anticipation of threats, as well as in the aftermath of an incident.

The integrity and vitality of Canadian agriculture, is an issue of national security and resilience. Investing in cybersecurity capacity across the agri-food system can also be thought of as investing in the prosperity and resilience of the country, as a whole[61]. But, this is not something that can be done in isolation of other sectors, or the broader context of Canada in the world today. It's a journey that involves joined-up effort. We can build this capacity for mutual support and collaboration across a networked community of stakeholders – by leaning into a *Cyber Barn Raising* approach.

Research Team

Janos Botschner, PhD

Janos is a social scientist with deep experience in applied research, evaluation and strategic consulting across a range of issues and groups. He holds a joint doctorate in applied social and developmental psychology. His professional work covers the spectrum of issues related to collaborative public safety and well-being, with a focus on understanding, and responding adaptively to, the complex issues and emerging opportunities of today and tomorrow. Janos has held a number of adjunct faculty appointments and administrative positions during a lengthy career in the public sector. He is an Associate of CSKA and the Principal of HumInsight.

Cal Corley, MBA

Cal is CEO of the Community Safety Knowledge Alliance and a former Assistant Commissioner of the RCMP. Over the course of his career, Cal gained extensive experience in both operations and executive management, serving in such areas as national security, criminal intelligence, drug enforcement, human resources, and leading reform initiatives. He also served on secondments at the Privy Council Office and at Public Safety Canada.

Evan Fraser, PhD

Evan is a full professor of Geography at the University of Guelph and helps lead the Food from Thought initiative, which explores how to use big data to reduce agriculture's environmental footprint. As the director of Arrell Food Institute at the University of Guelph, he co-convened an ad hoc working group made up of producer groups, the food industry, philanthropy and civil society to propose that the Federal Government of Canada should create a National Food Policy Advisory Council. The creation of this council was announced by the Minister of Agriculture and Agri-food Canada in the summer of 2019.

Ritesh Kotak, MBA, JD

Ritesh advises and assists several police services, government bodies, the judiciary, major financial institutions, community partners and private sector organizations with investigations, analytics, principles, practices, challenges and opportunities with respect to the use of social/cyber/digital technology. Ritesh frequently provides interviews to mainstream media to highlight organizational achievements and provide analysis & insights into tech related stories.

Dave McMahon, BEng

Dave's 35-year career has focused on engaged cyber defence, security and intelligence initiatives. Dave was a Special Advisor to the Canadian Security Telecommunications Advisory Committee and expert witness to Senate Standing Committee on Legal and Constitutional Affairs and the National Security and Defence Committees. He has acted in the capacity of a Special Advisor to the Privacy Commissioner of Canada as well as Canadian Intelligence Oversight and Review bodies. Dave serves as Chair of the Cyber Council for the Canadian Association of Defence and Security Industries (CADSI). Dave also served in various leadership positions with the Canadian Armed Forces, Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE). He is the Chief Intelligence Officer of Sapper Labs.

Endnotes

1 This report builds from other knowledge products created through the Cyber Security Capacity in Canadian Agriculture initiative, notably: Botschner, J, Corley, C., Fraser, E., Kotak, R. & McMahon, D. (2021). Cyber security in digital agriculture: Current state and future directions. Saskatoon and Ottawa: Community Safety Knowledge Alliance; and Botschner, J, Corley, C., Fraser, E., Kotak, R. & McMahon, D. (April, 2022). Cyber Security in Digital Agriculture: Research summery. Saskatoon and Ottawa: Community Safety Knowledge Alliance

2 Botschner, J., Corley, C., Fraser, E., Kotak, R. & McMahon, D. (April, 2022). Cyber Security Capacity in Canadian Agriculture: Research Summary. Saskatoon and Ottawa: Community Safety Knowledge Alliance.

3 Agriculture and Agri-Food Canada (2019). Food policy for Canada. https://multimedia.agr.gc.ca/pack/pdf/fpc_20190614-en.pdf

4 Advisory Council on Economic Growth (February, 2017). Unleashing the growth potential of key sectors. https://budget.gc.ca/aceg-ccce/pdf/key-sectors-secteurs-cles-eng.pdf

5 Standing Senate Committee on Agriculture and Forestry (July, 2019). Growing Canada's value-added food sector. https://sencanada.ca/content/sen/committee/421/AGFO/Reports/AGFO_SS-5_Report_Final_e.pdf

6 BC Food Security Task Force (2020). The future of BC's food system: Findings and recommendations from the BC food security task force. https://engage.gov.bc.ca/app/uploads/sites/121/2020/01/FSTF-Report-2020-The-Future-of-Food.pdf

7 Morgan (2016); WEF (2018, 2019)

8 e.g., For example, technology-enabled efficiencies, along with the economics of agriculture, are behind a growing consolidation of farmland in the hands of fewer operators, which has social implications for farming families and their communities. See: McKinsey and Company (2018). Unlocking success in digital transformations. McKinsey and Company, Organization, October, 2018. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Organization/Our%20Insights/Unlocking%20success%20in%20digital%20transformations/Unlocking-success-in-digital-transformations.ashx; and Rotz, S, Duncan, E., Small, M., Botschner, J., Dara, R., Mosby, I. & Fraser, E.D.G. (2019). The politics of digital agriculture: A preliminary review. Sociologia Ruralis, 59(2), April, 203-229.

9 Macaulay, T. (2016) RIoT Control: Understanding and managing risks and the internet of things. Amsterdam, NL: Science Direct/ Elsevier.

10 Macaulay (2016, p. 43)

11 Rotz, et al. (2019)

12 Bilodeau, H., Lari, M. & Uhrbach, M. (2019). Cybersecurity and cybercrime challenges of Canadian businesses, 2017. The Canadian Centre for Justice Statistics, Statistics Canada. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.pdf; Buil-Gil, D., Lord, N. & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. Victims and Offenders, 16(3), 286-315.

13 Botschner, et al. (April, 2022).

14 i.e., Australia and Finland. See: Borchi, J., Woodcock, M., Redshaw, M. & Raniga, B. (2021). Cyber security threats – are we prepared. Wagga Wagga, NSW: AgriFutures Australia (2021). https://www.agrifutures.com.au/wp-content/uploads/2021/07/21-070.pdf; and Nikander, J, Manninen, O & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communications networks. Computers and Electronics in Agriculture, 179. https://doi.org/10.1016/j.compag.2020.105776.

15 In addition to the widely-publicized ransomware attack on JBS in 2021, Maple Leaf Foods suffered an IT disruption in November 2022 following a cybersecurity incident. See Solomon, H. (Nov 7, 2022). Maple Leaf Foods suffers IT outage after cybersecurity incident. IT World Canada. https://www.itworldcanada.com/article/maple-leaf-foods-suffers-it-outage-after-cybersecurity-incident/511986

16 https://www.bbc.com/news/world-us-canada-57318965

17 https://www.abc.net.au/news/rural/2020-02-27/ransomware-cyber-attack-cripples-australian-wool-sales/12007912

18 https://edairynews.com/in/police-probe-virus-attack-on-national-milk-records-systems/

19 https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/new-cooperative-ransomware-attack-timeline-status-updates/; https://www.washingtonpost.com/business/2021/09/21/new-cooperative-hack-ransomware/

20 https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/new-cooperative-ransomware-attack-timeline-status-updates/

21 https://www.wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002/

22 https://www.cybertalk.org/2022/11/10/maple-leaf-foods-confirms-outage-due-to-cyber-security-incident/

23 https://globalnews.ca/news/9271365/privacy-sobeys-data-breach-perscriptions/

24 https://www.ctvnews.ca/politics/canada-calls-out-china-at-wto-council-meeting-for-evidence-to-back-canola-ban-1.4411277

25 https://financialpost.com/technology/chinese-hackers-went-after-aborted-potash-deal-report

26 https://www.inc.com/magazine/201905/tom-foster/russian-trolls-facebook-social-media-attacks-brands-hoax-fake-disinformation.html

27 Jahn, M., Oemichen, W.L., Treverton, G.F., David, S.L., Rose, M.A., Brosig, M.A., Jayamaha, B., Hutchison, W.K. & Rimestad, B.B. (2019). Cyber risk and security implications in smart agriculture and food systems. https://jahnresearchgroup.cals.wisc.edu/wp-content/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf.
See also: https://www.thetimes.co.uk/article/kremlin-bots-sow-fear-in-west-about-gm-crops-and-vaccines-f7h6woqq7; and https://geneticliteracyproject.org/2018/03/16/putin-pledges-to-make-russia-worlds-largest-supplier-of-gmo-free-food/

28 https://geneticliteracyproject.org/2018/03/16/putin-pledges-to-make-russia-worlds-largest-supplier-of-gmo-free-food/

29 Bogaardt, M.J., Poppe, K.J., Viool, V. & van Zuidam, E. (2016). Cybersecurity in the agrifood sector. Capgemini Consulting. https://www.capgemini.com/consulting-nl/wp-content/uploads/sites/33/2017/08/02-029.16_agrifood_pov_consulting_web.pdf

30 Ungar, M. (2018). Change your world: The science of resilience and the true path to success. Toronto, ON: Sutherland House.

31 McArthur-Blair, J. & Cockell, J. (2018). Building resilience with appreciative inquiry. Oakland, CA: Berrett-Koehler.

32 Bosetti, L., Ivanovic, A & Munshey, M. (2016). Fragility, risk and resilience: A review of existing frameworks. United Nations University Centre for Policy Research, October, 2016. https://i.unu.edu/media/cpr.unu.edu/attachment/2232/Assessing-Fragility-Risk-and-Resilience-Frameworks.pdf

33 Ungar, M. (2018).

34 Bosetti, et al. (2016); Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. Journal of Cybersecurity, 591), 1-17. DOI: 1093/cybsec/tyz013; Holling, C. S. (1986). The resilience of terrestrial ecosystems: Local surprise and global change, In W. C. Clark, & R. E. Munn (Eds.), Sustainable development of the biosphere (pp. 292-317). Cambridge: Cambridge University Press.

35 In living systems, this is known as homeostasis. When the capacity of a system to maintain homeostasis – its resilience – is overtaxed, it can become dysregulated, leading to the onset of disease or decay (Childs, 1999).

36 Bosetti, et al. (2016, p.4)

37 Ungar (2018)

38 Ungar (2018); Ungar, M. (n.d.) What works: A manual for designing programs that build resilience. Halifax, NS: Resilience Research Centre. WhatWorks-Ungar-WebVersion.pdf; Ungar, M. (2021). Recovery can be just another word for failure. Psychology Today, February 25, 2021. https://www.psychologytoday.com/ca/blog/nurturing-resilience/202102/recovery-can-be-just-another-word-failure

39 Botschner, J. (2000). Doing, not providing: A discourse-analytic investigation of social support as a responsive process. Unpublished doctoral dissertation. Guelph, ON: University of Guelph.

40 Dupont (2019); Dupont, B., Shearing, C. & Bernier, M. (2020). Withstanding cyber-attacks: Cyber-resilience practices in the financial sector. Global Risk Institute, April 2020. file:///C:/Users/botsc/AppData/Local/Temp/Global-Risk-Institute-Research-Withstanding-Cyber-Attacks-FINAL.pdf

41 Dupont, et al. (2020, p.3)

42 The authors note that cyber resilience is often reduced to steps taken in the immediate aftermath of an incident

43 Dupont, et al. (2020, p. 13) emphasis added

44 Dupont, et al. (2020)

45 United Nations Department of Economic and Social Affairs. Sustainable development. https://sdgs.un.org/goals

46 Maté, G. (2011). When the body says no: The hidden cost of stress. Toronto, ON: Knopf Canada

47 National Cyber Security Centre (2018). The Hague, NL: Ministry of Justice and Security. file:///C:/Users/botsc/AppData/Local/Temp/ncsc_guide_isac.pdf. Retrieved March 5, 2021.

48 Clinton, L. (2015). Best practices for operating government-industry partnerships in cybersecurity. Journal of Strategic Security, 8(4), 53-68. DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

49 Rotz, et al. (2019)

50 See, for example, Russell, C. (2022). Cyber Security in Digital Agriculture: Investigating farmer perceptions, preferences and expert knowledge. Unpublished masters thesis, Guelph, ON: University of Guelph.

51 Public Safety Canada (2019). National cyber security action plan: 2019 - 2024. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf

52 e.g, Deloitte (2018). The cybersecurity talent shortage: An emerging challenge for consumer products companies. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-cb-cybersecurity-talent-shortage-consumer-products.pdf; van Zadelhoff, M. (2017). Cybersecurity has a serious talent sortage. Here's how to fix it. Harvard Business Review, May 4, 2017. https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

53 van Zadelhoff, M. (2017). Cybersecurity has a serious talent sortage. Here's how to fix it. Harvard Business Review, May 4, 2017. https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it Retrieved May 28, 2021

54 The Conference Board of Canada (2018). Building cyber resilience. Briefing, July, 2018. https://www.conferenceboard.ca/temp/299d7330-4c42-4aa7-ac87-73097d7bac58/9796_Building%20Cyber%20Resilience_BR.pdf Retrieved March 5, 2021.

55 Rotz, et al. (2019)

56 https://www.iso.org/files/live/sites/isoorg/files/publications/en/2023_SAG-SF_Final_Report.pdf

57 https://www.csagroup.org/store/product/2705256/

58 e.g., Russell (2022)

59 Internet Security Alliance (2008). The cyber security social contract policy recommendations for the Obama administration and 111th congress: A twenty-first centurt model for protecting and defending critical technology systems and information. Internet Security Alliance. https://obamawhitehouse.archives.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf

60 Wilner, A.S. (2018). Cybersecurity and its discontents: Artificial intelligence, the internet of things and digital misinformation. International Journal, 73(2), 308-316. DOI: 10.1177/0020702018782249 6

61 This insight is inspired by an observation made by Guardian journalist Fiona Harvey, reflecting on COP27, in relation investments toward addressing the climate crisis. See: Harvey, F. (November 8, 2022) Money still top of the agenda at this Cop. The Guardian. com. https://www.theguardian.com/environment/live/2022/nov/08/cop27-un-climate-conference-day-two-crisis-live?filterKeyEvents=false&page=with:block-636a45008f08f43127befc2c#block-636a45008f08f43127befc2c

CSKA

Community Safety Knowledge Alliance

Research to Practice to Alignment

The Community Safety Knowledge Alliance (CSKA) is a non-profit corporation that supports governments and others in developing, implementing and assessing new approaches to improving community safety and wellbeing outcomes.

www.cskacanada.ca