Canada's increasingly connected agricultural and food systems require a coordinated approach to cybersecurity and resilience. AI-generated using ChatGPT by OpenAI, 2026.

Cybersecurity and Food-System Resilience in the Age of Artificial Intelligence

Farm and food systems should be treated as a critical-infrastructure priority. Those who feed the country should not be left to manage emerging risks alone.

Agriculture has digitized faster than its cybersecurity posture has matured. Connected systems now support production across large operations and family farms alike and while productivity has increased, so too have the risks.

Agriculture's fragmentation has offered protection in the digital era. Farms are generally too small and dispersed to serve as viable targets for cyber criminals or malicious actors.

Artificial Intelligence presents a new paradigm, offering automation that makes the sector's wide attack surface cheaper to test and easier to exploit. Agriculture remains fragmented in ownership, but increasingly, farms are turning to common providers, creating shared digital dependencies.

Food is one of Canada's ten critical infrastructure sectors, and while the Federal Government has produced cyber-hygiene guidance for farms, guidance alone is not a cybersecurity strategy. But, with the emergence of powerful AI and corresponding threats, policy makers have been heavily focused on energy, finance, and telecommunications. [1, 2, 9]. Food-sector cybersecurity cuts across the systems Canada depends on and can no longer remain a neglected vulnerability in Canada's critical-infrastructure posture.[20]

Agriculture's unique risk profile

Agriculture is seasonal, geographically dispersed, and built around many smaller operators with limited internal cybersecurity capacity. Even as food-system experts see significant and growing vulnerabilities across the sector, Canadian farmers, as recently as 2025, generally view cybersecurity as a low priority [1]. Nearly 80 percent of farms surveyed by MNP reported having no formal cybersecurity plan [16]

Farms are private businesses, but collectively they perform a critical-infrastructure function. They depend on infrastructure and services that extend beyond the gate of any one farm, and cyber incidents in the sector have too often been viewed, by federal decision makers, as local operational problems rather than national resilience warnings.

Agriculture also adheres to deadlines that are outside the control of operators, though largely predictable based on publicly available information. Planting and harvest, storage and shipping, even livestock care and food safety are tied to weather and biology, which produce narrow operating windows. Attackers understand that downtime costs are exorbitant in those windows. The Federal Bureau of Investigation has warned that ransomware actors may be more likely to target agricultural operations during planting and harvest because of the profit motive incurred by food-system operators in those peak periods [5].

In addition to biology and weather, modern farming practices increasingly depend on operational technology: digital systems that monitor or control physical processes. This means remote attackers can interfere directly with the physical conditions that make food production possible.

Agriculture and Agri-Food Canada has linked the sector's digitization and supply-chain connectivity to cyber risk, including service disruptions, food-security impacts, loss of consumer trust, and reduced profits; however, no strategy has emerged in response to threats posed by artificial intelligence [4].

AI makes existing weaknesses easier to exploit

Ransomware remains a serious concern in agriculture. In 2021, ransomware disrupted JBS, one of the world's largest meat processors, affecting North American and Australian operations. The same year, a cyberattack on NEW Cooperative, an agricultural technology and grain cooperative, raised concerns about grain purchasing, livestock feeding, and farm operations [5].

And while attacks on large targets make the headlines, Microsoft's 2025 Digital Defense Report makes clear that small size is no longer a shield. It's reporting found that extortion and ransomware drove more than half of observed cyberattacks, and that attackers increasingly target organizations "big or small" when the opportunity exists [14].

This is supported by reporting out of the United States, where Food and Ag-ISAC disclosed 265 ransomware attacks against food and agriculture in 2025 [17].

Beyond ransomware, Canada must prepare for operational misoperation: cyber activity that changes how physical systems behave.

In October 2025, the Canadian Centre for Cyber Security and the Royal Canadian Mounted Police reported multiple incidents involving internet-accessible industrial control systems. One involved a grain drying silo on a Canadian farm, where temperature and humidity levels were manipulated, creating potentially unsafe conditions if the issue had not been caught in time. The same alert cited incidents involving a water facility, pointing to a broader weakness in internet-accessible operational systems [6].

AI requires a coordinated response. OpenAI's threat reporting reinforces the point: by automating reconnaissance and credential testing, AI tools lower financial and technical barriers, increasing the reach of less-skilled actors [13]. This includes actors with little understanding of a sector's specific operations.

AI can help attackers understand targets, interpret technical documentation, adapt known tools, and test access more efficiently. A threat actor may once have ignored a family farm. But when AI reduces the work required to target that farm, or a group of farms using the same control-system provider, those farms become viable opportunities.

The U.K. National Cyber Security Centre has assessed that AI will make parts of cyber intrusion more effective and efficient, and that some organizations will be better able to keep up than others [3]. Canada's farmers sit on the wrong side of that divide. AI will also improve cyber defence, but agricultural operators are already facing AI-enabled threats, well before Canada has taken the steps needed to ensure they can benefit from AI-enabled protection.

On risk, AI introduces two related categories of cyber risk for agriculture.

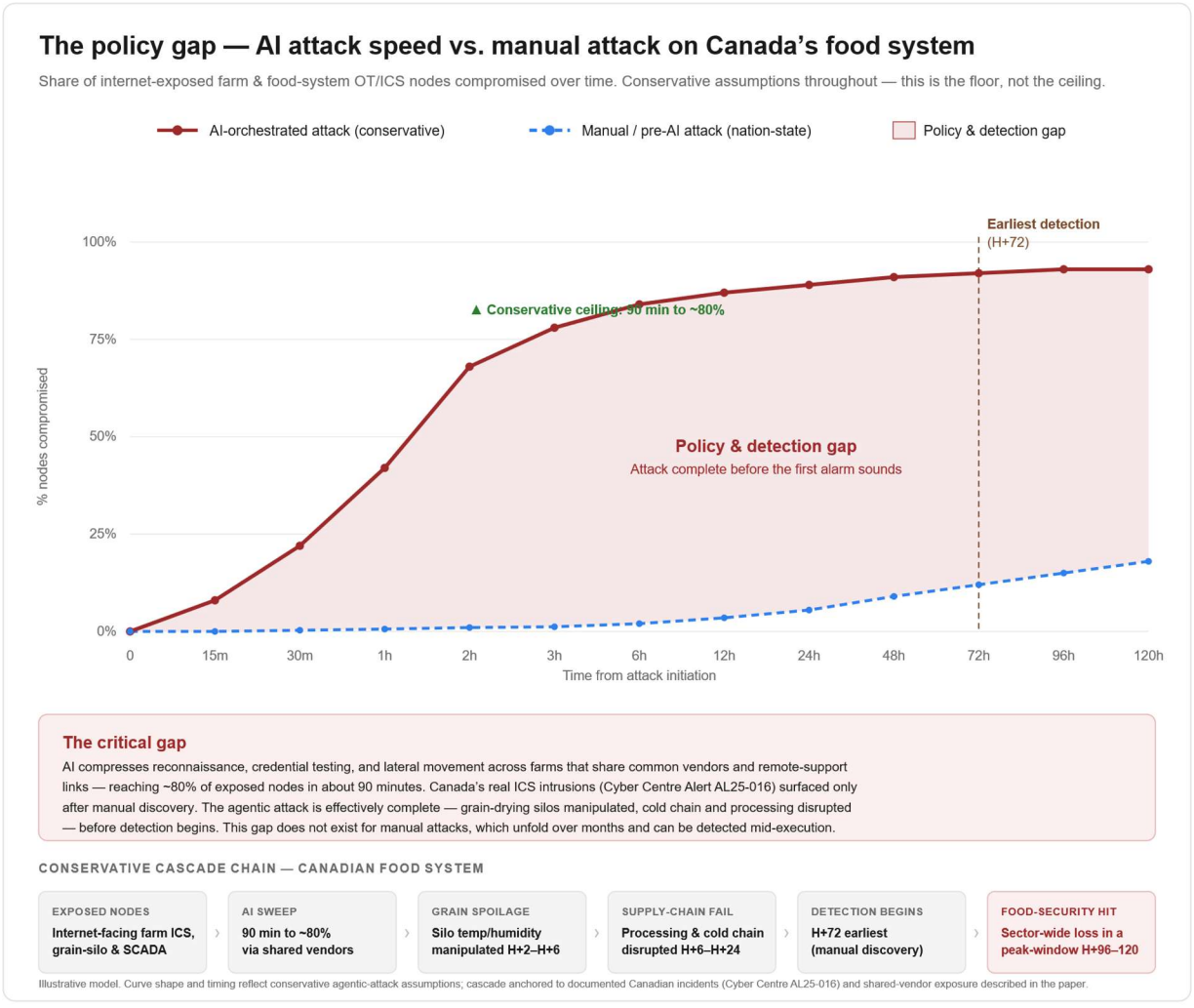
The first is AI-assisted activity. Attackers use generative models to perform work that previously required more sector knowledge, technical skill, or linguistic ability. AI lowers the price of entry into cyber operations. This expands the pool of actors able to participate, including less experienced criminals, hacktivists, poorly resourced groups, and foreign proxies. Europol has warned that more accessible AI tools allow cybercriminals to lower barriers to entry, scale operations more effectively, and reduce the time needed to launch attacks [12]. Anthropic's analysis points in the same direction: the proportion of threat actors categorized as medium risk or higher while leveraging these capabilities rose from 33 per cent to 56 per cent in under a year [8].

The result is a lower threshold for attacks. A target no longer needs to promise a major payout or strategic effect to be worth pursuing. If the work is cheaper, faster, and easier to repeat, smaller agricultural targets become viable. While a single farm, cooperative, or service provider may be attacked, the risk presented by AI is that many more of them may be attacked at once or in sequence. ENISA's 2025 threat landscape warns that AI-assisted actors can support near-

continuous campaigns and more diversified attack activity, which has the potential to erode resilience even when individual incidents are not catastrophic [15].

The second is AI-orchestrated or agentic activity. In this model, AI is connected directly to offensive tools and used to act inside digital environments with limited human involvement. These systems can compress the time between discovery, access, and internal movement. In agriculture, that risk is amplified because many independent operators rely on common vendors, remote support arrangements, connected precision equipment, and similar operational technology [8].

The figure below illustrates the difference between pre and post-AI attack execution timing. An agentic attack automates the collection and utilization of deep domain expertise and in-situ knowledge to make decisions in real time, assess and adjust, and dramatically accelerates the time to compromise. By the time detection occurs, the damage is done.



The MITRE ATT&CK framework, a widely used map of the tactics and techniques cyber actors use during an intrusion, helps show where this change is occurring. AI can assist across the attack lifecycle, but it is also increasingly used in live network environments, where attackers can read the digital landscape, test credentials, and move between connected systems faster than many agricultural operators can detect or respond [3, 8].

A recent threat intelligence report by Anthropic found that, in an analysis of 832 accounts associated with malicious cyber activity between March 2025 and March 2026, AI-enabled activity was identifiable across all 14 MITRE ATT&CK tactics and 482 unique sub-techniques [8]. Those findings suggest that AI-enabled cyber activity is already being used in operational practice by threat actors [8].

Governance in agriculture has not evolved

Canada must take seriously the shared digital relationships across farms and food systems. These paths can be exploited to reach many operators at once, turning local weaknesses into sector-wide risk.

In its work on critical water infrastructure, the Cyber Centre has warned that attackers do not need to compromise every physical asset when shared digital systems, suppliers, and remote-access relationships provide paths into operations [2]. Agriculture has the same exposure, but in a more distributed and under-resourced form.

This bears the characteristics of a market failure. Farmers are expected to absorb cybersecurity risks that they cannot see, assess, price, or negotiate into contracts. Technology providers can therefore externalize cybersecurity risk onto individual farms that lack the skills and resources to manage it. CSKA's Cyber Barn Raising framework makes the same policy point: producers have a role to play, but the resilience of the agri-food sector cannot depend on producers carrying this burden alone [18].

Federal guidance, university research, training initiatives, industry reporting, and food-value-chain research all show that agricultural cybersecurity is on the radar in Canada [11, 16, 18, 19, 20]. But CSA Group's 2026 research found that food-system cybersecurity lags other sectors, remains thin in the research and standards literature, and is largely absent from cybersecurity policies and frameworks [20].

What remains missing is a sector-wide strategy and a national, industry-facing leader with the intelligence, convening power, and decision-making authority to bring these actors together around agricultural cyber resilience.

When attempting to adapt to AI, that missing capacity leaves agriculture exposed on two fronts: malicious use of AI against critical infrastructure, and weaknesses in AI systems deployed inside critical infrastructure. A CSET workshop report identified both risks and warned that resource

gaps shape whether infrastructure providers can adopt AI safely and manage AI-related risk [7, 9].

The Cyber Centre's 2025 alert shows that critical-infrastructure cybersecurity depends on knowing what is exposed, who is responsible, and how incidents move from discovery to response. Individual farmers cannot reasonably be expected to fund or perform that work on their own [6, 10].

Other jurisdictions have begun treating food-system cybersecurity as a sector-specific problem rather than a general small-business issue, including the Food and Agriculture Information Sharing and Analysis Center in the United States.

Canada should view agricultural cybersecurity as a systemic risk and build a federal response tailored to the structure of the sector. It should move responsibility upstream, give farms trusted support, identify the dependencies that could spread disruption, and test continuity under real agricultural conditions.

Conclusion

Cybersecurity and food security are increasingly linked. Catastrophic attacks powered by artificial intelligence are increasingly likely, especially as existing weaknesses become faster to exploit, easier to scale, and harder to contain.

Food is critical infrastructure, but the food sector is fragmented. Canada needs a cybersecurity response tailored to agricultural systems. The federal government possesses the skills, intelligence and convening power to drive change in this sector, and to ensure responsibility for resilience sits with those that shape the digital systems agriculture now depends on.

Those who feed the country should not be left to manage this risk alone.

Areas for practical federal action

1. Establish a Centre of Excellence for Agricultural Cybersecurity
The federal government should establish a centre of excellence for agricultural cybersecurity with the mandate to translate national cyber threat intelligence into practical, unclassified guidance for farms and food-system operators, and latitude to work with provincial and territorial partners, agricultural organizations, and critical-infrastructure experts to build trusted capacity and harden the sector against existing and emerging threats [11, 18, 20].

2. Set cybersecurity expectations for agricultural technology vendors and managed service providers
Canada should set baseline cybersecurity expectations for companies that sell, connect, monitor, or support technology used on Canadian farms. Where federal programs support connected agricultural technology, cybersecurity should be built into funding conditions from the start.

Farmers and smaller operators should not be left carrying risks created by the products, platforms, and services they rely on [10, 20].

3. Map systemic food-system cyber dependencies
Canada should map digital dependencies across the agricultural sector to support mitigation, exercises, incident planning, and targeted resilience funding [2, 6, 10, 20].

4. Test continuity when digital systems fail
A centre of excellence or other federal entity should conduct exercises to prepare for operational questions before incidents occur, including how farms, vendors, processors, and public authorities continue essential food-system functions when digital systems fail [5, 6, 10, 20].

Dylan Odd – Research Fellow NC-CIPSeR

Dylan Odd is an experienced policy advisor with more than a decade of experience working on Parliament Hill. He has supported several Canadian senators as a Chief of Staff and Director of Parliamentary Affairs, with a focus on legislative affairs, public policy, and emerging risks.

Mario Daigle – Research Fellow NC-CIPSeR

Mario is a seasoned product management and operations executive with over 25 years of experience building and refining product offerings in general analytics, applied analytics, cloud and SaaS, and cybersecurity.

[1] Russell, A., Botschner, S., Duncan, E., Dehghantanha, A., and Fraser, E. "I grow food, IT people do cybersecurity": Addressing cybersecurity risks in Canada's agri-food sector. *Smart Agricultural Technology*, Vol. 11, Article 100342, 2025.

[2] Canadian Centre for Cyber Security. *The cyber threat to Canada's water systems: Assessment and mitigation*. National Cyber Threat Assessment Series, Government of Canada, 2025.
https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

[3] National Cyber Security Centre. *Impact of AI on cyber threat from now to 2027*. Government of the United Kingdom, 2024.
https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat-now-to-2027

[4] Agriculture and Agri-Food Canada. *Cyber security and your farming business*. Government of Canada, 2023.
https://agriculture.canada.ca/en/programs/tools-manage-farm-risk-and-finance/cyber-security-and-your-farming-business

[5] Federal Bureau of Investigation. *Ransomware attacks on agricultural cooperatives potentially disrupt supply chain during critical planting and harvest seasons*. Cyber Division Private Industry Notification, PIN 20220420-001, U.S. Department of Justice, 2022.

[6] Canadian Centre for Cyber Security. *Alert AL25-016: Internet-accessible industrial control systems abused by hacktivists*. Government of Canada, October 29, 2025.
https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists

[7] Center for Security and Emerging Technology. *Securing critical infrastructure in the age of AI: Workshop report*. Georgetown University, 2024.
https://cset.georgetown.edu/publication/securing-critical-infrastructure-in-the-age-of-ai/

[8] Anthropic. *Mapping AI-enabled cyber threats: Insights from the LLM ATT&CK Navigator*. June 3, 2026.
https://www.anthropic.com/news/AI-enabled-cyber-threats-mitre-attack

[9] Public Safety Canada. *Canada's National Cyber Security Strategy*. Government of Canada, 2025.
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

[10] Canadian Centre for Cyber Security. *Cross-Sector Cyber Security Readiness Goals Toolkit*. Communications Security Establishment Canada, 2024.
https://www.cyber.gc.ca/en/cyber-security-readiness/cross-sector-cyber-security-readiness-goals-toolkit

[11] Swaile, N., and Fast, M. *More Cyber Safe: Key practices for on-farm cyber-hygiene*. Community Safety Knowledge Alliance, 2024.
https://cskacanada.ca/wp-content/uploads/2024/01/Basic-Steps-for-Farm-Cyber-Safety-CSKA.pdf

[12] Europol. *Internet Organised Crime Threat Assessment 2026*. European Union Agency for Law Enforcement Cooperation, 2026.
https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf

[13] OpenAI. *Disrupting malicious uses of AI: October 2025*. October 7, 2025.
https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/

[14] Microsoft. *Microsoft Digital Defense Report 2025*. Microsoft, 2025.
https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

[15] European Union Agency for Cybersecurity. *ENISA Threat Landscape 2025*. ENISA, 2025.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[16] MNP Digital. *Cyber Security on the Farm Report*. MNP, 2025.
https://mnpdigital.ca/insights/2025-mnp-digital-agriculture-cyber-security-report-download/

[17] Food and Agriculture Information Sharing and Analysis Center. Navigating the 2025 Food and Agriculture Sector Ransomware Landscape. February 18, 2026; updated February 20, 2026.
https://www.foodandag-isac.org/post/navigating-the-2025-food-and-agriculture-sector-ransomware-landscape

[18] Community Safety Knowledge Alliance. *Cyber Barn Raising: Building Capacity for Farm Cybersecurity in Canada*. Community Safety Knowledge Alliance, 2023.
https://cskacanada.ca/wp-content/uploads/2023/03/CSKA-CyberBarnRaising-FIN-digital.pdf

[19] Cyber Science Lab. *Agri-Food Cybersecurity*. University of Guelph.
https://cybersciencelab.com/ag-security/

[20] CSA Group. *Cybersecurity in the Canadian Food Value Chain*. Canadian Standards Association, 2026.
https://www.csagroup.org/article/research/cybersecurity-in-the-canadian-food-value-chain/