Food Security and Cyber Warfare: Vulnerabilities, Implications and Resilience-building

Richard Jones
Edinburgh Law School, UK

richard.jones@ed.ac.uk

Abstract: This paper examines cyber security readiness in the food sector, considers whether this sector could potentially be targeted as part of a future cyber warfare attack, and discusses why the sector may be vulnerable to attack, the implications of such an attack, and potential routes for enhancing its cyber resilience. The food sector is recognised as a part of critical national infrastructure, and academic literature has reviewed some of the cyber security risks associated with the use of agricultural sensors, the emergence of 'Agriculture 4.0, and the use of computer systems across the food production supply chain. However, the field of 'food security' studies does not yet feature a sustained focus on cyber security, and only a few studies in cyber security have considered the wider implications of cyber vulnerabilities for the sector. Moreover, the emergence of offensive cyber weapons raises the prospect that such weapons could in future be used to target food systems. Although International Humanitarian Law prohibits the targeting of the civilian food supply, it cannot be guaranteed that this supply is not impacted by cyber warfare attacks in the future. The paper draws from a recent systematic literature review as well as from relevant areas of scholarship to present a preliminary analysis of possible cyber vulnerabilities in the food sector and policy recommendations.

Keywords: Cyber warfare, Food security, Cyber security, Resilience

1. Introduction

Food security is of vital significance to nations, especially during times of inter-state conflict. As food production systems become increasingly computerised, however, they become increasingly vulnerable to cyber-attack. Although cyber security research and policy-making in many countries has long recognised the importance of securing critical national infrastructure including the food sector from cyber-attacks, relatively little research has been undertaken on food cyber security, and even less on securing food systems from deliberate attack on the part of hostile nations. Despite the starvation of civilians being prohibited by international humanitarian law, and indeed potentially constituting a war crime, the direct or indirect targeting of food production by cyber-attacks may nevertheless still take place during times of inter-state conflict. This paper demonstrates how nations' food production systems are potentially vulnerable to a cyber warfare attack; discusses research evidence as to the nature of such vulnerabilities; identifies the implications of a cyber-attack for food production and distribution; and outlines measures governments could undertake to enhance the resilience of food production systems to cyber-attacks. A key question is whether the cyber security requirements of the food sector are any different from other critical infrastructure sectors such as energy, transport or communications. While it might be assumed that since the food sector is a recognised sector of critical national infrastructure (CNI) extensive defensive measures are already in place, research suggests that advice and guidance provided to different sectors of CNI may be inconsistent (Topping et al., 2021). Moreover, it is possible that the diffuse nature of the food sector, together with the fact that its disruption may be less immediately publicly apparent than in other sectors, mean that it does not always attract the attention of policymakers it deserves. Drawing from a recent systematic literature review on current cyber security vulnerabilities in the food production and distribution sector, this paper presents a conceptual typology of cyber vulnerabilities, attack scenarios, and implications for national food security. The paper concludes that food production systems may currently be vulnerable to cyber-attacks and that measures are urgently required to assess current readiness to attack and develop greater cyber resilience across the food sector. Whilst in many respects the measures required to enhance cyber security within the food sector are the same as required in any other sector of critical national infrastructure, there are some features of the food sector that require specific measures.

2. Cyber Security of Food Production Systems: Current Vulnerabilities

2.1 Agriculture 4.0 and AgTech

Industrial processes are being transformed by the adoption of sensors, automation, robotics, satellite imagery, Internet of Things (IoT) devices, and AI. Agricultural production, food distribution and food retailing systems have experienced high levels of computerisation and utilisation of smart systems, dubbed 'Agriculture 4.0'

(Abbasi et al., 2022, Araújo et al., 2021) or 'AgTech' (Marshall et al., 2022) (a term also applied to startup companies innovating in this sector).

2.2 Systematic Literature Review: Design and Findings

A recent study of cybersecurity vulnerabilities in the food supply chain (XXXX, 2025) identified three research questions that were then used to guide a systematic literature review, namely, RQ1: What types of digital technologies are used in the food supply chain and what are the adoption trends and barriers?; RQ2: What is the nature and extent of cybersecurity vulnerabilities associated with these technologies?; and RQ3: What are the food security implications of cybersecurity incidents in the food supply chain? For RQ 1, 70 articles were initially identified and following an evaluation process were reduced to a total of 22 articles; and for RQs 2 and 3, a total of 21 articles was included from the 331 articles initially identified.

The literature review found that there is already a wide range of digital technologies used in the food supply chain, and that their use generates a large volume of data. It was noted, however, that many studies were published recently, suggesting that adoption is ongoing and that the implications of such technological adoption may not necessarily yet be fully understood; and that there was a clear geographical bias in adoption between countries.

Maffezzoli et al. (2022) identify various domains in which digital technologies are used including water management, crop monitoring, microclimatic prediction and monitoring, soil monitoring, livestock monitoring, hydroponics, and autonomous machinery. This is important in the context of identifying cyber vulnerabilities as it sheds light both on where technologies are starting to be used, and the nature of the disruption that would result were such systems to be attacked. Terence and Purushothaman (2020) examine the use of IoT devices in food production, suggesting that their use typically falls into one of three categories, namely agricultural monitoring and control systems, automatic irrigation systems, or plant disease monitoring systems. Such devices typically continually generate new data, leading to the need for 'big data' analytics in order to inform 'precision agriculture' (Cisternas et al., 2020) and facilitate modelling using 'digital twins' (Slob and Hurst, 2022). AI and machine learning are already being used to optimise production and increase profitability (Elbasi et al., 2023), including by forecasting crop yields; predicting weather, disease and nutrient levels; calculating how to reduce waste; and maximising product freshness by managing real-time supply, smart vehicle routing and consumer demand analysis within the food distribution and retail chain (Sharma et al., 2020).

XXXX (2025) identified some awareness of cybersecurity vulnerabilities present within the food supply chain. For example, Matana et al. (2023) note the centrality of cyber-physical systems, meaning that disruption of computer systems is likely also to impact both physical and organic systems. Consequently, this generates a 'wide attack surface' across digital agriculture (Alahmadi et al., 2022). Padhy et al. (2023) distinguish between four layers of computing within agricultural cyber-physical systems. First, the physical layer includes computing devices, sensors, machinery, robotics, or autonomous vehicles. Second, the network layer involves local networks, routers, Wi-Fi, mobile connectivity, and cloud networks. Third, the edge layer comprises edge computing devices and sensors where the network meets the physical world and where some degree of computation may directly take place. Lastly, the application layer features the software and systems running on computers and devices, and with which end users typically interact. Each of these layers is associated with specific cybersecurity threats. The physical layer may be attacked via tampering with physical equipment, power management systems (e.g. 'sleeplessness' attacks, keeping devices awake in order to drain their batteries and make them inoperative) (Padhy et al., 2023) or side-channel attacks. Network layer attacks may target local data transport protocols, involve DDoS attacks, or attacks on the wider communications networks on which they rely. At the edge layer, devices may have poor cybersecurity configuration and be vulnerable to unauthorised access, disruption or firmware modification. Finally, the application layer may be vulnerable to various forms of attack including social engineering and the insertion of malware (Padhy et al., 2023). Farmers and food distributors may not always practice the highest levels of cyber security. In a study of six Finnish dairy farms, Nikander et al. (2020) found that several 'farmers use the same computer for management of milking/feeding systems and web browsing'; network devices were often consumer-level products; 'equipment had been left on default [password] settings'; malware protection was not adequate; and systems were not adequately backed up.

In a review of cybersecurity research across the entire food and beverages industry, Latino and Menegoli (2022) found that whereas agricultural cybersecurity received considerable attention, there was little focus on food processing, distribution or retail. van der Linden et al. (2020) draw attention to the significance of food

availability, a key component of food security, pointing out that a cyberattack on food production could potential impact food availability in shops. XXXX (2025) concluded that although there is some awareness of areas of food production in which technical cybersecurity should be strengthened, there was less awareness of the wider implications of cyber vulnerabilities for the integrity of the food supply and food security in general.

Overall, research suggests that the cyberattack surface of the food industry is large, diverse, and that it may not have a high level of cyber resilience. Key issues include the large number of companies and computing devices involved; the resulting network complexity; lack of computing, networking and cyber security expertise by farmers or smaller retailers; and inadequate configuration of security settings. Additionally, it is possible that the food sector could be vulnerable to hardware and software supply chain attacks, as well as to DDoS attacks.

3. Cyber Warfare Attacks and Food Systems

3.1 Cyber Warfare Techniques and Methods

The notion of 'cyber war' has been met with scepticism in some quarters (Katagiri, 2021), but today is a real form of attack, potentially targeting computing or cyber-physical systems. Since cyberattacks can form part of military combat, they are subject to the Law of Armed Conflict as set out in International Humanitarian Law (IHL). However, as van den Bosch (2021: 213) observes, there are various forms of physical military 'operations which, because they 'are not aimed at, nor result in physical injury or damage', are not considered 'attacks' under IHL. Such operations include a 'reconnaissance operation, an intelligence operation or electronic and psychological warfare'. Nonetheless, van den Bosch argues that both such non-lethal operations and cyberattacks falling below the threshold of attack should be subject to other principles of IHL. In any case, cyber-attacks are potentially deadly if they interfere with life-sustaining cyber-physical systems. Moreover, because cyberattacks can safely be conducted from afar, and concealed to make actor attribution difficult if not impossible, it seems likely that they are a daily phenomenon and are being used for a variety of purposes including espionage, sabotage, deployment of advanced persistent threats (APTs), an expression of (cyber) power and capability, and for probing/assessing the target's intrusion detection systems. Accordingly, techniques of cyberattack may equally be employed for cyberwarfare and for activities falling 'below the threshold of [cyberwar] attack'.

3.2 International Legal Framework Prohibiting Starvation of the Civilian Population

Attacking the food supply of an adversary could be attempted by a belligerent nation for military advantage. However, such an attack could potentially lead to significant loss of life were people to starve as a result. International law and the law of armed conflict distinguishes between combatants and civilians, seeking to protect civilians from the ravages of war. The international legal framework prohibiting the starvation of the civilian population includes international humanitarian law (IHL), as well as international criminal law including war crimes defined as 'serious violations of laws and customs of war' (Akande and Gillard, 2019). Additionally, various 'rules regulating the conduct of hostilities that are considered customary and applicable in both international and non-international armed conflicts' include, 'the prohibition on directing attacks against civilian objects, which include objects necessary for food production and distribution such as agricultural lands, crops, livestock, farms, mills, water installations and markets'; and 'the prohibition on indiscriminate attacks, i.e. attacks against military objectives and civilian objects, such as those just listed, without distinction' (Akande and Gillard, 2019: 756). Article 54(1) of Additional Protocol I to the Geneva Conventions sets out a general prohibition of starvation of civilians as a method of warfare. Akande and Gillard (2019: 760-761) consider the meaning of 'starvation' here and suggest that while it 'implies a high degree of deprivation, where survival is threatened […] it is not necessary for death to occur'. Although the international legal framework was presumably drafted with physical warfare in mind, there appears no reason as such why an act of cyber warfare should not be held to the same standards and its conduct assessed according to the same principles.

The Tallinn Manual is a non-binding interpretation of the application of international law to cyber-attacks and warfare. Rule 107 of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations states that, 'Starvation of civilians as a method of cyber warfare is prohibited' (Schmitt, 2017). The guidance notes accompanying this rule advise that, 'the term 'starvation' means deliberately depriving a civilian population of nourishment (including water) with a view to weakening or killing it', and that 'Reference to 'as a method of cyber warfare' excludes from the Rule the incidental starvation of the civilian population'. The phrase, 'with a view', suggests this merely requires an attack to succeed in depriving such a population of nourishment with the *aim* of weakening it, rather than necessarily actually leading to widespread fatalities. The notes conclude

that, 'Cyber operations will only violate this Rule in exceptional cases', but it is not clear whether this assessment was reached because the authors considered cyber operations targeting the food sector to be unlikely to take place, or whether they considered it unlikely that the necessary legal threshold would be reached. Nevertheless:

> *Such a violation could, however, arise during an armed conflict in which a party to the conflict seeks to annihilate the enemy civilian population through starvation. Consider a case in which a party launches cyber operations for the exclusive purpose of disrupting transportation of food to civilian population centres and targets food processing and storage facilities in order to cause civilian food stocks to spoil. It is the civilian hunger that these operations are designed to cause that qualifies them as prohibited starvation of the population (see also Rule 141 regarding protection of objects indispensable to the civilian population). Denying foodstuffs to enemy armed forces or organised armed enemy groups does not violate this Rule, even if the incidental effect affects civilians.*

Rule 141 of the Tallinn Manual 2.0 asserts that, 'Attacking, destroying, removing, or rendering useless objects indispensable to the survival of the civilian population by means of cyber operations is prohibited'. Guidance note 4 for this Rule explains further that:

> *The cited provisions of Additional Protocols I and II offer the following examples of objects indispensable to the survival of the civilian population: foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies, and irrigation works. Food and medical supplies are also generally accepted as essential to the survival of the civilian population […] Although these lists are not exhaustive, the objects to which the Rule applies must be 'indispensable to survival'. This is a very narrow category; objects not required for survival (e.g., those that merely enhance civilian well-being or quality of life) fall outside the scope of application of this Rule.*

It is perhaps slightly odd that the Manual characterises the phrasing 'indispensable to the survival' of the civilian population as a 'very narrow' one given the broad category of 'objects' listed and their evident indispensability to human life, but does nonetheless emphasise the high threshold required (since an action merely reducing food availability would not by itself contravene the Rule).

Note 5 for the same Rule goes on to add that:

> *The Internet (or other communications networks) does not, in and of itself, qualify as an object indispensable to the survival of the civilian population. In the context of cyber operations, however, cyber infrastructure indispensable to the functioning of electrical generators, irrigation works and installations, drinking water installations, and food production facilities could, depending on the circumstances, qualify.*

Overall, then, it is clear that the Tallinn Manual 2.0 directly envisages the possibility of cyberattacks being used to target an enemy's food supply and maintains that while this would be permissible under International Humanitarian Law were it to target combatants, it would not be permitted were it to deliberately target a civilian population.

3.3 Typology of Cyberattacks Against Food Systems

Disruption of a food system potentially leads to malnutrition, disease and ill health, societal discontent, public disorder, looting, and economic disruption. An adversary may consider these advantageous to precipitate, including as a precursor to or in combination with a wider attack, whether involving kinetic or cyber weapons. Despite IHL expressly prohibiting the deliberate starvation of civilians during times of conflict, there remains the possibility that a hostile state will mount such a cyber warfare attack in the future, for various reasons. First states do not always comply with international humanitarian law during times of conflict. Second, a belligerent state may claim that its aim is to target food systems dedicated to supplying military personnel, and that any impact on a civilian population is unintended. Third, food systems supplying the civilian population may be disrupted due to a wider cyber-attack—targeting a particular operating system, device, or network, for example—on which the food system relies. Fourth, where food systems are reliant on computers and networks, any cyberwarfare attack launched against a country's energy system or communications backbone has the potential to severely impair food production and distribution as a result. Fifth, a hostile state may deliberately calibrate its attack so that, although disruptive, it is classed as a 'military cyber-operation' falling 'below the threshold of 'attack' (van den Bosch, 2021).

Cyber warfare attacks may thus target the food sector directly or may impact the food sector indirectly. The following table presents a four-fold typology of cyber attacks against the food sector, distinguishing between degrees of intentionality and the directedness of attack targeting:

Table 1: Typology of cyber warfare attacks against the food sector.

Cyber-attack type	Illustration
Direct targeting of entire food system	Hostile nation state systematically launches a cyberattack against numerous key computer systems involved in food production, ranging from agricultural sensors to food distribution systems, to food retailers' computer systems, with the aim of collapsing the target nation's civilian food supply.
Direct targeting of key component within food system	Hostile nation state launches a cyberattack against a specific key component of a nation's food system, with the aim of significantly disrupting the food supply, gathering intelligence on food supply levels, diverting resources and attention from elsewhere, instilling fear in the population, triggering food hoarding and a run on supermarkets, or expressing symbolic dominance.
Indirect targeting from a wider cyber attack	Computerised systems involved in food supply process become compromised by a cyberattack targeting specific software, operating systems, device vulnerabilities (e.g. routers, network switches, sensors), or networks, in which these components are used both by the food sector but also more widely. In this case, the food sector is just one among a number of sectors within critical national infrastructure that are affected.
Collateral damage from a wider attack on cyber-physical systems	A wider attack, whether kinetic, nuclear or cyber, in which the Internet communications network and/or the electricity supply of a nation is impaired, leading to outages of computer systems, devices and networks, including those used within the food sector.

Attacks will vary in their impact, immediacy of consequences, and economic costs. The scale of impact is likely to reflect either the market share of the affected producer, distributor or retailer, or their centrality/criticality within the overall food system. The impact may be the (a) quantity of food available to sustain the population, (b) quality of food (safety of consumption), (c) direct financial loss to food sector, (d) wider economic loss to society, and (e) impact on military capability. In terms of its immediacy, the timeframe is likely to be more varied than in the case of attacks against telecommunications, transport or energy sectors in which the impact may be immediately apparent, because it may take days, weeks or even months for the consequences of a cyber-attack to work their way through the agricultural production and food distribution systems. Conversely, where an attack results in restricted availability of food in shops, this may rapidly lead to visible and vocal social discontent, public protest or political instability.

4. Resilience-Building Strategies for Food Cyber Security

4.1 Components of Resilience

'Resilience' has become a key concept in security strategy and policymaking (see e.g. Fekete and Fiedrich, 2018), including in relation to food security (Béné and Devereux, 2023) and cyber security (Tjoa et al., 2024). The term 'resilience' may be attractive to policymakers because it is simultaneously evocative and nebulous. However, it is worth seeking precision in its definition and use. Resilience is a curious concept insofar as it speaks both of a *goal* to be sought (since if a system were already fully resilient there would be no need for a policy seeking to enhance resilience), and of a real-world *property* of a system (since systems may be said to differ in their actual real-world resilience, ranging from 'not resilient at all' to 'highly resilient'). As such, the resilience of a given system cannot be taken for granted; faced with an external shock or attack, a system may in fact simply fail (Raab et al., 2015: 23). Resilience should be distinguished from 'resistance', and resilience is not merely the ability to absorb shocks. Instead, resilience can usefully be considered an umbrella concept, involving a series of related activities. These involve activities designed to *anticipate*, *survey*, *prevent*, *withstand*, *recover* from, *restore* (or even '*bounce forward* from'), and *learn* from the exogenous event (a stress, shock or attack) (list modified from Montpellier_Panel, 2012). A key question, however, is what is the 'thing' whose resilience we might seek to build in relation to a cyberattack from a hostile nation state targeting

the food sector. It is helpful here to distinguish between three different systems to understand the different kinds of activities that may be required to enhance resilience in each case.

4.2 Cybersecurity of Food Sector

The review above suggests that smaller food producers may not currently practice good cybersecurity. As the UK's NCSC has noted in relation to the UK's cybersecurity stance in general, many cyberattacks could be prevented simply by implementing basic principles of cybersecurity. Addressing this 'low-hanging fruit' should therefore be an urgent priority. Cybersecurity within the food sector involves technical measures, configuring socio-technical systems, and reducing human vulnerabilities (e.g. to initial social engineering attacks). A range of actors will necessarily need to be involved in enhancing cybersecurity in this sector, including farmers, food distributors, hardware/software vendors, trade organisations, local and national government, and intelligence agencies. A benefit of enhancing cyber resilience in the food sector is that in addition to greater preparedness in the face of any future cyberwar attack, it would also be better prepared against attacks from less sophisticated but more common threat actors such as organised cybercriminal gangs.

4.3 National 'Food Security'

A second way of approaching resilience is regarding the nation's 'food security' overall. Sassi (2018: 1) argues that '[t]he four basic and distinctive characteristics of food security [are] food availability ("sufficient, safe and nutritious food"), access ("physical and economic access"), utilisation ("to meet dietary needs and food preferences), and stability ("[for] all people at all times"). Food security is thus distinct from cyber security, even if they are now starting to share some common factors. Establishing food security has long been a challenge for developing nations, but food security can also periodically be jeopardised in wealthy nations too. While it is crucial that computer systems within the food sector are resilient in the face of adverse shock, this is only one component of the security and resilience of the food sector. For example, the availability of food in shops is dependent on the overall supply chain and the integrity of food storage facilities, which can potentially be disrupted by factors including drought, flooding, energy shortages, the economy, or political protests. The global COVID-19 pandemic also quickly drew attention to global food security (Mardones et al., 2020), in the face of disruptions to the food production, distribution and retail subsectors, as well as in the face of consumer 'stockpiling' leading to shortages. Computer systems enable monitoring of food supply across the supply chain and can play a key role in enhancing efficiency (Ababou et al., 2023: 13), but at the same time present a potential attack surface for threat actors seeking to undermine food security. As such, consideration of national food security from a policy perspective today clearly requires attention to all its components, including in relation to cyber security.

4.4 Cyberwar Defensive and Countermeasures Capabilities

If a large-scale cyberattack against its food system is considered by a nation to have been directed by a hostile nation state, either as a prelude to or as a component of a wider armed conflict, in addition to the defensive and offensive services that the nation's signals intelligence agency is able to offer, the attack will also likely trigger military involvement, including for example of specialised cyberwarfare units. Notwithstanding the problem of 'attribution' (i.e. being able confidently to prove the identity of the attacker) (Rid and Buchanan, 2015), cyberwarfare capabilities may be deployed defensively in support of one or more critical national infrastructure sectors under attack, or in the form of offensive countermeasures seek to respond, retaliate and deter future attacks, such as via 'hacking back' operations. Such operations are not without their challenges (Katagiri, 2021), risk escalating the conflict, and thus require careful consideration of the authority and conditions under which they are used, including where they are automated (Haataja, 2024). It has been argued that an attack that 'paralyses or massively disrupts' part of a nation's critical national infrastructure, such as its food services, could for self-defence purposes be considered analogous to an armed attack even if it did not cause human injury or physical damage (Tsagourias, 2012). More recently, it has been argued that for self-defence justificatory purposes, three levels of cyberattack severity should be distinguished, ranging from 'cyber-attacks comparable to kinetic attacks, directly leading to physical damage' (the most serious level of attack), to the mid-level 'cyber-attacks comparable to kinetic attacks, indirectly leading to physical damage', and the lowest level, 'cyber-attacks not comparable to kinetic attacks, leading to societal disruption' (Oorsprong et al., 2023). The category under which a cyberattack was considered to fall would depend on its scale, consequences and the nature of the damage caused (e.g. whether there was loss of life, or the harm was merely economic).

5. Policy Recommendations Regarding Cyber Warfare, Cybersecurity, and the Food Sector

Enhancing food security resilience and food cybersecurity resilience ahead of any future cyberattack, including cyber warfare attack, would help prepare for such an attack while also conferring ongoing benefits in terms of bolstering against lower-level cybercrime threats. As an initial step, nations may wish to *model the impact* of a cyberattacks both on specific parts of the food sector as well as on the food sector as a whole; *assess the adequacy* of current food cybersecurity on the ground; and consider how best to *enhance the resilience* of the food system to cyberattacks. Many dimensions of cyber security within the food sector are likely to be identical to cyber security needs in any other sector of CNI. These include the need to ensure security of the hardware supply chain, use of redundancy and backup systems, managed updating of software and firmware, physical security of hardware and networking, risk management, training and education, authentication management policies, and data management policies. Consolidation of food distribution and retail in which a small number of large companies have dominant market positions is likely to facilitate government efforts at enhancing their cyber security. At the same time, however, the studies discussed above suggest that there may be various characteristics of cyber security in the food sector that are relatively distinct from other CNI sectors. These include the involvement of numerous small-scale producers and their lack of specialist technical expertise; a reliance on hardware and software purchased from the consumer market; use of the same computers on smaller farms both as agricultural control systems and for everyday personal Internet use; the interdependence on a large number of commercial actors in complex supply chains; and reliance on third party cloud and online service providers. Among the measures that could potentially be explored, should remedial measures be required, are: setting cybersecurity standards for relevant IT vendors; awareness-raising, education and training within the agriculture and food sector; lesson-learning from previous global events such as COVID-19 and the war in Ukraine (a major food producer); building food cyber disruption into military war-gaming scenarios; enhancing linkages between food security strategy and cyber security strategy; and contingency planning in the event of an actual cyberwar attack.

6. Conclusion

This paper has contended that the cybersecurity of food production and distribution systems may currently be suboptimal and vulnerable to cyberattack, including by hostile nation states. Such attacks could potentially be mounted as part of a wider conflict, and cyberweapons could potentially be directed at food supply systems. The criticality of food security from a national security perspective is high, and thus academic researchers, governmental agencies and policymakers should give priority to further evaluating current cybersecurity readiness across the food sector; determining the resilience of food security in the event of a cyberattack; and leading awareness-raising across both the food industry and IT vendors. Strengthening of cyber security of food systems would not only help build resilience in the event of a targeted attack by a hostile adversary as a component of a cyber warfare attack but would additionally enhance cyber resilience in the event of smaller-scale (but much more likely) attacks by other threat actors such as individual hackers, hacktivist groups, or organised cybercriminal gangs.

References

Ababou, M., Chelh, S., and Elhiri, M. (2023) “A Bibliometric Analysis of the Literature on Food Industry Supply Chain Resilience: Investigating Key Contributors and Global Trends”, *Sustainability*, Vol. 15, No. 11, pp

Abbasi, R., Martinez, P., and Ahmad, R. (2022) “The digitization of agricultural industry - a systematic literature review on agriculture 4.0”, *Smart Agricultural Technology*, Vol. 2, No. 100042, pp 100042.

Akande, D. and Gillard, E.C. (2019) “Conflict-induced Food Insecurity and the War Crime of Starvation of Civilians as a Method of Warfare The Underlying Rules of International Humanitarian Law”, *Journal of International Criminal Justice*, Vol. 17, No. 4, pp 753-779.

Alahmadi, A.N., et al. (2022) “Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture”, *Sensors*, Vol. 22, No. 9, pp 3520.

Araújo, S.O., et al. (2021) “Characterising the Agriculture 4.0 Landscape-Emerging Trends, Challenges and Opportunities”, *Agronomy*, Vol. 11, No. 4, pp 667.

Béné, C. and Devereux, S. (eds) (2023) *Resilience and food security in a food systems context*, Cham: Palgrave Macmillan.

Cisternas, I., et al. (2020) “Systematic literature review of implementations of precision agriculture”, *Computers and Electronics in Agriculture*, Vol. 176, No. 105626, pp 105626.

Elbasi, E., et al. (2023) “Artificial Intelligence Technology in the Agricultural Sector: A Systematic Literature Review”, *IEEE Access*, Vol. 11, No., pp 171-202.

Fekete, A. and Fiedrich, F. (eds) (2018) *Urban Disaster Resilience and Security: Addressing Risks in Societies*, Cham: Springer International Publishing.

Haataja, S. (2024) "Cyber operations and automatic hack backs under international law on necessity", *Computer Law & Security Review*, Vol. 53, No. 105992, pp 105992.

Katagiri, N. (2021) "Cyber countermeasures for democracies at war", in R. Johnson, M. Kitzen, and T. Sweijs (eds) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*, Routledge, Abingdon, UK, pp

Latino, M.E. and Menegoli, M. (2022) "Cybersecurity in the food and beverage industry: A reference framework", *Computers in Industry*, Vol. 141, No. 103702, pp 103702.

Maffezzoli, F., et al. (2022) "Agriculture 4.0: A systematic literature review on the paradigm, technologies and benefits", *Futures*, Vol. 142, No. 102998, pp 102998.

Mardones, F.O., et al. (2020) "The COVID-19 Pandemic and Global Food Security", *Frontiers in Veterinary Science*, Vol. 7, No. Article 578508, pp 1-8.

Marshall, A., et al. (2022) "Critical factors of digital AgTech adoption on Australian farms: from digital to data divide", *Information Communication & Society*, Vol. 25, No. 6, pp 868-886.

Matana, G., et al. (2023) "Cyber-Physical Systems as Key Element to Industry 4.0: Characteristics, Applications and Related Technologies", *Engineering Management Journal*, Vol. 35, No. 4, pp 377-404.

Montpellier_Panel (2012) *Growth with Resilience: Opportunities in African Agriculture*, Agriculture for Impact, London.

Nikander, J., Manninen, O., and Laajalahti, M. (2020) "Requirements for cybersecurity in agricultural communication networks", *Computers and Electronics in Agriculture*, Vol. 179, No. December 2020, pp 105776.

Oorsprong, F., Ducheine, P., and Pijpers, P. (2023) "Cyber-attacks and the right of self-defense: a case study of the Netherlands", *Policy Design and Practice*, Vol. 6, No. 2, pp 217-239.

Padhy, S., et al. (2023) "AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain", *Processes*, Vol. 11, No. 3, pp 757.

Raab, C.D., Jones, R., and Szekely, I. (2015) "Surveillance and Resilience in Theory and Practice", *Media and Communication* Vol. 3, No. 2, pp 21-41.

Rid, T. and Buchanan, B. (2015) "Attributing Cyber Attacks", *Journal of Strategic Studies*, Vol. 38, No. 1-2, pp 4-37.

Sassi, M. (2018) *Understanding Food Insecurity: Key Features, Indicators, and Response Design*, Springer, Cham, Switzerland.

Schmitt, M.N., editor; Vihul, Liis, editor.; NATO Cooperative Cyber Defence Centre of Excellence (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge.

Sharma, R., et al. (2020) "A systematic literature review on machine learning applications for sustainable agriculture supply chain performance", *Computers & Operations Research*, Vol. 119, No. July 2020, pp 104926.

Slob, N. and Hurst, W. (2022) "Digital Twins and Industry 4.0 Technologies for Agricultural Greenhouses", *Smart Cities*, Vol. 5, No. 3, pp 1179-1192.

Terence, S. and Purushothaman, G. (2020) "Systematic review of Internet of Things in smart farming", *Transactions on Emerging Telecommunications Technologies*, Vol. 31, No. 6, pp e3958.

Tjoa, S., Gafic, M., and Kieseberg, P. (eds) (2024) *Cyber Resilience Fundamentals*, Cham: Springer International Publishing.

Topping, C., et al. (2021) "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks", *Computers & Security*, Vol. 108, No., pp p.102324, Article 102324.

Tsagourias, N. (2012) "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict & Security Law*, Vol. 17, No. 2, pp 229-244.

van den Bosch, B. (2021) "Fighting a war without violence: The rules of International Humanitarian Law for military cyber-operations below the threshold of 'attack'", in R. Johnson, M. Kitzen, and T. Sweijs (eds) *The Conduct of War in the 21st Century: Kinetic, Connected and Synthetic*, Routledge, Abingdon, UK, pp

van der Linden, D., Michalec, O.A., and Zamansky, A. (2020) "Cybersecurity for Smart Farming: Socio-Cultural Context Matters", *Ieee Technology and Society Magazine*, Vol. 39, No. 4, pp 28-35.

XXXX (2025) "Cybersecurity vulnerabilities in the food supply chain and their impact on food security: A systematic literature review", *[Under review]*, Vol. xx, No. xx, pp xx-xx.