Food defence: Refining the taxonomy of food defence threats

Louise Manning

Louise Manning, Department of Food Science and Agri-food Supply chains
Harper Adams University, Newport, Shropshire, TF10 8NB

Abstract

Background
Awareness of the need to address food defence is gaining pace in the food industry. Indeed implementing an effective food defence strategy is a key pre-requisite to comply with third party certification standards. There is however a knowledge gap with regard to the types of threat that fall within the scope of a food defence strategy and also how these issues can then be mitigated and where possible eliminated.

Scope and Approach
This research seeks to position food defence as a supply chain risk mitigation strategy and use case studies of real-world issues to frame the taxonomy of food defence threats.

Key findings
In order to differentiate food defence threats (food attack) from wider food crime, the research postulates that food defence strategies needs to address intentional adulteration to gain personal attention, to gain financial reward through extortion or to gain attention for a particular cause or ideology i.e. food terrorism. More covert threats include sabotage, espionage, intellectual property theft, and cybercrime, including hacktivism. These threats can cause actual harm to individuals, members of certain populations and communities or to organisations. This can lead to large scale, economic, political or social unrest and disruption of the supply chain and thus fit within the scope of food defence activities. To inform food defence risk assessment and management processes, this taxonomy needs to be developed and accepted across the food industry so that threats can be consistently and effectively addressed and as a result consumers, industry partners, shareholders and also the organisation itself can be protected.

Keywords: adulteration; extortion; sabotage; espionage; cybercrime; terrorism

Highlights:
- Food defence is an under-researched phenomenon.
- Food defence strategies addresses multiple product and supply chain threats
- More supply chain focused guidance should be developed to inform food defence strategies.
1. Introduction

The United States (US) Federal Food, Drug, and Cosmetic Act Section 342 determines adulterated food principally as food that bears or contains: “any poisonous or deleterious substance which may render it injurious to health.” The US FDA “Mitigation Strategies to Protect Food Against Intentional Adulteration: Guidance for Industry” defines a contaminant as “any biological, chemical, physical, or radiological agent that may be added to food to intentionally cause illness, injury, or death” (FDA, 2018a). However other sources distinguish between the use of the terms “adulterant” and “contaminant”, with some stating that unintentional contamination of food is the focus of established food safety measures (Mitenius, Kennedy & Busta, 2014), and adulteration is within the area of food fraud. In this context, adulteration is considered by the food industry as “the addition of an undeclared material into a food item or raw material for economic gain” (BRC, 2018:108) or for wider fraudulent purposes (Spink & Moyer, 2011a; Manning & Soon, 2014). GFSI (2017) defines food defense as “the process to ensure the security of food and drink from all forms of intentional malicious attack including ideologically motivated attack leading to contamination.” This definition uses the term contamination rather than adulteration. Other definitions of adulteration include both intentional substitution and unintentional contamination (Bansal, Singh, Mangal et al. 2017; Kowalska, Soon & Manning, 2018).

Some suggest that food defence related activities are distinct from food fraud (Spink & Moyer, 2011b) as they are motivated by the impact they cause i.e. food defence strategies encompasses the activities or efforts undertaken to protect food from intentional acts of adulteration (FDA, 2018b). However, other US regulatory sources state food defense “means the effort to protect food from intentional acts of adulteration where there is an intent to cause wide scale public health harm.” (FDA, 2018a). This suggests that food defense plans should only address those threats where the intent is widespread harm and it is the size of impact that
predetermines what should be considered and addressed in a food defence plan. This is at odds with the Global Food Safety Initiative definition that states it includes all forms of intentional malicious attack (GFSI, 2014; GFSI, 2017; BRC, 2018), malicious tampering or terrorism (Spink & Moyer, 2011b), or a malicious and ideologically motivated attack leading to compromised products and/or supply chain disruption (PAS 96, 2017), panic or fear (Spink, Moyer, Park, & Heinonen, 2013).

This narrative across the literature suggests intentional adulteration addressed by food defence strategies is separate from the strategies to address economically motivated adulteration (EMA). Whilst with EMA the aim of the perpetrators is for intentional adulteration to continue undiscovered for as long as possible so that the maximum financial benefit can be derived, food defence threats are different. Food defence threats include activities that are “impact motivated” whereby an agent that is chemical, biological, radiological, nuclear (CBRN) or physical in nature, is used by perpetrators who seek to maliciously and intentionally adulterate food where such activities are actively disclosed to organisations and the general public in order to derive the associated personal, political or social impact. Food defence threats reflect a motivation to do harm to distinct and targeted victim(s) with notions of personal benefit to the perpetrator in terms of underpinning an ideological statement, a means to gain notoriety, revenge, restorative justice or envy, (Hirschl, 1969; Cohen & Felson, 1979; Pease, 2006; Walklate, 2007; Hirschauer & Zwoll, 2008). Some sources consider that the scope of food defense includes all intentional activities seen as a threat including food fraud, tampering and food terrorism (Davidson et al. 2016) and wider threats too (PAS 96, 2017).

A threat is “something that can cause loss or harm which arises from the ill-intent of people” (PAS 96, 2017:3). The distinction between an agent and the threat is again confused in the literature with some sources defining the material agent itself as a threat. PAS 96 (2017) differentiates between six types of threats to that need to be addressed under food fraud (EMA,
counterfeiting) and food defence mitigation strategies i.e. malicious contamination, extortion, espionage, and cyber-crime. The scope of PAS 96 (2017) is wider than that suggested by the FDA (2018a) in terms of food defence which states that:

“Acts of intentional adulteration may take several forms: acts intended to cause wide scale public health harm, such as acts of terrorism focused on the food supply; acts of disgruntled employees, consumers, or competitors; and economically motivated adulteration (EMA)… Acts of disgruntled employees, consumers, and competitors are generally intended to attack the reputation of a company, and EMA is intended to obtain economic gain. In the spectrum of risk associated with intentional adulteration of food, attacks intended to cause wide scale public health harm to humans are ranked as the highest risk. Therefore, the IA [international adulteration] rule is focused on addressing those acts and not acts of disgruntled employees, consumers, or competitors, or acts of EMA.”

This shows a clear differentiation between regulatory requirements with regard to the scope of food defence plans and market compliance approaches that require the use of Threat Analysis Critical Control Point (TACCP) via the use of the PAS 96 guidelines as a pre-requisite to supply. TACCP focuses not only on the threat but also the typology of perpetrators that need to be considered when developing a food defence strategy including: the extortionist, the extremist, the irrational individual and here perpetrators suffering with mental health issues should be considered, the disgruntled individual especially those who have previously worked for a food business and/or associated supply chain and the hacktivist or cybercriminal.

Therefore, food defense encompasses the active steps taken, the protection activities, and/or the security assurance process or procedures, often called countermeasures, that deliver product safety with regard to intentional acts of adulteration to cause harm (Manning & Soon, 2016). The term food defense describes what needs to be done i.e. procedures, protocols, or processes to mitigate a given activity or threat rather than focusing on the specific taxonomy of activities.
or perpetrators. Increasingly, these procedures and protocols are seen by retailers, manufacturers and food service as a pre-requisite to supply (Wiśniewska, 2015). However, in order to be able to implement effective food defense mitigation strategies, a clear understanding of the potential threats, and associated motivations and rationalisation used by perpetrators and also the agents they might employ is essential. This level of understanding is further framed by determining how to develop countermeasures that reduce both the capability of the perpetrators to take action and also reduce the opportunities for such action to occur.

The aim of this paper is develop the taxonomy of food defence threats in order to postulate what forms the associated food defense strategies need to take. The methodological approach employed was to undertake a review of existing literature to then frame the conceptual research. Screening of both academic and grey literature has demonstrated there is limited previous research in terms of food defence strategies at the level of the food organisation. This is especially true of emerging threats defined in PAS 96 such as hacktivism or cybercrime. This is the research gap that this paper seeks to address.

2. Taxonomy of food defense threats and perpetrators

2.1 Intentional impact orientated adulteration and extortion

At its simplest the taxonomy of food defense threats for impact orientated adulteration rather than EMA can be described in terms of adulteration through the use of hazardous agents i.e. biological agents, chemical agents, physical agents and radiological agents (Dalziel, 2009; Fredrickson, 2014). The diversity of these agents is complex driven primarily by ease of access e.g. the decision to use glass which is readily available versus radionuclear material which is not, and secondly, the means and opportunity for contamination e.g. on farm, within manufacturing and processing, food service, retail or the home (Meulenbelt, 2018). Table 1 synthesizes data on confirmed incidents in the literature, examples of agents used by location in the supply chain and their impact. The data shows that confirmed incidents are
predominantly at the tertiary stages of the supply chain and also in the home some of which are cases of domestic poisoning which do not fit within a reflection on food defense strategies employed at organisational level. The majority of the confirmed cases take place pre-harvest (n=365), then in the home (n=265) and then at retail and food service (n=89). Agents used at farm level have included glyphosate, plant toxin, cyanide, and rodenticide, with a much wider range of agents at food service and retail level.

**Take in Table 1**

These incidents are linked to the extortionist, the extremist, the irrational or disgruntled individual i.e. perpetrators either internal or external to the organisation who have opportunity to commit this offense. Extortion can be described as the actions undertaken to obtain something which the perpetrator values (e.g. money, assets, influence or impact) from a person or organisation by force, intimidation, threat or illegal activity. Information on extortion cases in the food supply chain rarely appear in the public domain, but one incident with Heinz Baby Food in the United Kingdom (UK) was the catalyst in the 1990s for tamper evident packaging and improved product security within the distribution chain and on retail shelves.

**Case study 1: Heinz Baby Food 1988**

In 1989 Heinz had to withdraw from sale batches of baby food in the UK worth an estimated £30 million pounds when Rodney Whitchelo, a former Scotland Yard detective who was later sentenced to seventeen years in prison, attempted to extort millions of pounds from the food giant by spiking the food with bleach and razor blades (The Independent, 1999). Fisher (1989) highlights how after the initial publicity about contamination of food, copy-cat cases occurred causing concern and fear to escalate with 220 reported incidents of baby food contamination in April 1989. However police first began their investigations in August 1988 when £20,000 was demanded by the extortionist and paid into a bank account and then
subsequently removed from various cash points (ATMs). After the initial payments stopped
the extortionist demanded £1 million from Heinz contaminating two cans of baby food after
the demand. The perpetrator was eventually charged, tried and imprisoned. This case study
shows the challenges of the renegade insider who commits a crime whilst being aware of the
protocols and checks and balances in place within criminal investigations i.e. they can
circumvent the food defence systems that have been designed and implemented. This case is
not alone.

In a case in 2016 in the UK an extortionist who demanded £2 million not to contaminate
food with cyanide was traced through his DNA on the stamp on the letter and was jailed for
seven years. The vial sent with the letter contained five to ten lethal doses of cyanide (Smith,
2016). In September 2017, a German man was charged with threatening to put poisoned baby
food throughout Europe with a demand to multiple supermarkets for nearly £8.8 million (Licea,
2017: Rojas, 2017). The man’s DNA was found on five jars that were recovered from stores
and then found to contain ethylene glycol. Psychological issues were cited as a mitigating issue
with the perpetrator, but this was rejected in court and he was found guilty of attempted murder
and extortion and sentenced to twelve and a half years in prison (BBC, 2018).

Case Study 2: Fonterra, New Zealand (NZ)

In November 2014, Fonterra was the victim of anonymous threats to contaminate
commercial milk supplies with sodium fluoroacetate or 1080, a pesticide, unless its usage was
halted on farm (Manhire, 2015). Highly concentrated levels of 1080 were mixed with infant
formula and posted to Fonterra and Federated Farmers with a letter stating contaminated infant
milk powder would enter the Chinese and other markets (NZHerald, 2016). Whilst
ecoterrorism was cited by some as a possible motive that led to the £18 million costs of the
incident, a NZ businessman, Jeremy Kerr was subsequently jailed for eight and a half years
after pleading guilty to two charges of attempted blackmail and the judge ruled that as he owned
a company that made an alternative pesticide to 1080 this had motivated his activities because of the potential economic gain (BBC, 2016). The extortion threat required the dairy organisation, Fonterra, to take action to develop a robust methodology for detection of 1080 in milk and powdered milk products (Cooney, Varelis & Bendall, 2016). Cooney et al. (2016) state that having developed and validated the methodology between January and July 2015, 136,000 fluid milk samples were tested as part of a multi-agency food defense strategy to maintain confidence in the safety of NZ milk and dairy products. This case study highlights the challenge of addressing a food defense incident early on in the investigation, especially where no existing tests exist to check for the presence of the reported agent in the supply chain, the crucial role of intelligence and the need for police forces to work closely with food businesses. The risk of food terrorism was hinted at in this case study, but food terrorism is a real threat and is now considered.

2.2. Food terrorism

Terrorism is defined in Title 22 Chapter 38 of US. Code 2656f as "premeditated, politically motivated violence perpetrated against noncombatant [civilian] targets by subnational groups or clandestine agents.” The North Atlantic Treaty Organisation (2014) define terrorism as “the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives.” Terrorist activities, usually but not always undertaken by non-nation actors, are designed to engender fear, terror, panic and anxiety in the population and as a result reduce the level of confidence in the government, leading to uncertainty and political instability (Alvarez et al. 2010: Fredrickson, 2014) or the attainment of a specific political goal (Nestle, 2003). Food terrorism is defined as “the deliberate (or threat of) contamination of food with hazardous agents (biological, chemical, physical, or radionuclear) for the purpose of causing injury or death and/or disrupting social, economic, or political
Thus food terrorism, if it occurs, could cause severe health implications to the population and economic and trade disruption either through direct costs due to the culling of livestock, disposal of food products and the potential compensation paid to farmers and producers and the impact on public health services including the cost of hospitalisation (Manning et al. 2005). Further, food terrorism can lead to consequential loss to the local or national economy, loss of consumer confidence in the food supply chain and loss of political confidence and support following a major food product recall or the mass culling of livestock (Manning et al. 2005). An example of the impact on public health services of a terrorism incident is the 1995 nerve gas attack on the Tokyo subway system that caused 12 deaths and required 5000 people to seek medical attention involving 131 ambulances, 1364 emergency technicians and over 4000 people needing to get to medical care themselves (WHO, 2002). A similar incident associated with food could have equal impact. In 2011, there was an Escherichia coli O104:H4 outbreak in Germany associated with sprouts from fenugreek seeds which was not explicitly connected to a food defence threat, but its impact demonstrates how a similar food defense issue could cause significant challenges. Between May 2011 and July 2011, the outbreak involved 3,842 cases (including 2,987 cases of gastrointestinal disease characterised by diarrhea), with 855 cases of hemolytic uremic syndrome (HUS) and 53 deaths (RKI, 2012) with at the peak of the outbreak more than 50 reported cases of HUS per day (McIntyre & Monaghan, 2016). The outbreak caused widespread concern and panic and a change to eating habits, as well as economic consequences impact particularly for farmers with the EU paying 220 million Euros for the loss of income (Burger, 2012).

Terrorism acts can be differentiated by those that seek to cause actual harm to individuals or populations and alternatively those acts that are symbolic to provoke anxiety and concern, and to change consumer behaviour leading to economic loss (Alvarez et al. 2010).
“guidance for establishing and strengthening prevention and response systems” states that an essential means to preventing food terrorism is the development, validation, implementation, monitoring and effective verification of food safety management programmes and their associated security measures, described here as countermeasures. To minimise risk, the report states that effective prevention requires food defence strategies to provide a concerted approach between government and industry. Prevention is not the only approach within food defence strategies, surveillance is another element that should be employed. Agro-terrorism is the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses, and/or undermining social stability (Monke, 2007).

Agro-defence, the actions that can be taken to reduce the likelihood of an agro-terrorism incident specifically can be addressed through the use of emerging testing methods such as biosensors, colourmetric assays and digital apps that could prove to be an opportunity for early detection of agents such as viruses or pathogens (Neethirajan, Ragavan, & Weng, 2018). However, a recent conviction for planning of terrorism acts in the UK was determined through traditional policing/anti-terrorism methods.

Case study 3: Kerry Foods, UK

Temporary factory worker Munir Mohammed who was involved in ready meal manufacture at the Kerry Foods factory, and a pharmacist, Rowaida El Hasssan were arrested in December 2016 and convicted in January 2018 of planning a terrorist attack using food as the vehicle (Stones, 2018). They were arrested after counter-terrorism surveillance identified that they had undertaken extensive on-line research on acetone peroxide or TATP and ricin both realistic agents for a terror attack on the food supply. The food company as well as the UK population were potential victims here. Kerry Foods were unaware that Munir Mohammed had been working illegally at the factory as he used EU documents in another man's name to gain work at the factory (Kreft & Crowson, 2018). This shows how important induction checks are for
assuring that individuals working at food factories are who they claim to be. However these
checks have limited preventive capacity if individuals intentionally lie about their identity.
Other examples of recent food related terror threats include: in June 2016, Italian anarchists
threatened to contaminate foodstuff in supermarkets in Lombardy with herbicide and in
December 2016, Greek anarchists claimed they had contaminated several food and drink
products of multinational companies (EUROPOL, 2017). However intentional adulteration
linked to the product is just one type of overt threat that needs to be addressed by food defense
strategies. Clandestine or covert threats, where activities or the identity of perpetrators is
purposefully hidden (Lord, 2015) are now considered.

2.3 Covert Threats (Sabotage)
In history, there have been multiple occasions when civilian food supplies have been
sabotaged deliberately, during military campaigns or to deliver a specific social or
political impact (Torok et al. 1997) with the associated trade and economic repercussions
(WHO, 2002). Biological sabotage agents include zoonoses or animal disease (Manning,
Baines & Chadd, 2005), but other agents could be used and their nature is primarily driven by
their availability to the perpetrator. Previous sabotage actions against the food supply include
to fruit trees and livestock in Palestine in 1933, or just more generally instances of working
slowly, or instances of deliberate fire, damaging goods and intentionally breaking equipment.
Thus, a saboteur is an individual who deliberately damages or destroys assets or infrastructure
in order to weaken an enemy or make a protest (Collins Dictionary, nd). At the supply chain
level, sabotage involves the “destruction of essential infrastructure affects people’s ability to
access, process, distribute and utilise food.” (Koc, Jernigan, & Das, 2007:321) or a clandestine
act to destroy, damage or render assets unusable (Douthit, 1987). The motivation for
sabotage behaviour is a wish to “damage, disrupt, or subvert the organisation’s operations for
the personal purposes of the saboteur by creating unfavourable publicity, embarrassment,
delays in production, damage to property, the destruction of working relationships, or the harm of employees or customers” (Crino, 1994:312). In this context, industrial sabotage can be seen as a form of counterproductive work behaviour (CWB) i.e. wilful behaviour by employees that could cause harm to fellow employees or the organisation itself (Spector & Fox, 2005; Krischer, Penney, & Hunter, 2010). Taylor and Walton (1971) cite a number of examples of industrial sabotage including one organisation having to throw away half a mile of “Blackpool rock” because an offensive expletive had been printed through the product. They argue that sabotage can be a singular or group activity, demonstrates underlying industrial conflict, and may link with other deviant and often irrational behaviour. Therefore the potential for an employee to undertake sabotage could be highlighted in advance by other negative behaviours such as absenteeism, low morale and job satisfaction, stress, and poor performance with job satisfaction being the mediating factor (Alias, Mohd Rasdi, Ismail, & Abu Samah, 2013). This work suggests that early warning systems can be developed to identify those employees more likely to commit sabotage and to implement preventive strategies including improving staff morale to reduce the risk of occurrence. A sense of injustice or inequality can also be a leading motivational factor in workplace sabotage as can a sense of powerlessness or lack of autonomy. Frustration, often a secondary motivational factor, is triggered by previous incidents that then fuels anger, and a transition by workers from being rule compliance to bending the rules i.e. simple deviance from prescribed organisational norms to ultimately breaking the rules during work activities. This behaviour may have negative intent, be motivated more simply by a need to meet organisational goals that cannot otherwise be met by compliant behaviour, as a mechanism to reduce workplace boredom i.e. a means of entertainment or to deliver what the perpetrator believes is a form of retaliatory action or restorative justice (Ambrose, Seabright & Schminke, 2002). Reducing the risk of actions seen by employees as restorative justice lies at the heart of how sabotage can be prevented by food
defence strategies. This includes the development of positive organisational culture to reduce
the potential for power dynamics, reducing management decisions that can be perceived as
driving inequality within the workplace or supply chain and not promoting goals (financial,
operational etc.) that can only be achieved by deviant behaviour.

There is limited evidence in the literature of sabotage in the food supply chain so a more
detailed example case study is not provided here.

2.4 Covert Threats (Industrial Espionage)

Private or confidential information means “any kind of information which the
organisation feels should not be freely available to outsiders and which therefore should be
subject to some kind of moral or legal protection.” (Crane, 2005:237). Consideration of
espionage in the food science literature is novel and thus requires the development of the
terminology used in other sectors that can then be applied to food defense threats. Crane (2005)
states that the test of whether an activity can be determined as espionage is to consider: the
nature of the information that is under threat, the tactics employed, and the purpose for which
the information will be used. There are multiple tactics that Crane suggests could be defined
as questionable (Table 2) including breaking and entering into a competitor’s premises to steal
information through to posing as fictitious supplies, potential employees or customers. In order
for such threats to be actioned it may involve stealing the information, infiltration using insiders
to report, electronic eavesdropping or covert recording to gain information or material, or
remote attacks through digital systems (PAS 95, 2017), or to weaken the capabilities, reputation
and brand value of a competing business (van Arnam, 2001).

Take in Table 2

Estimates of the cost of such activity to US industry run between $45 billion and $100
billion per annum; an average of $50 million per incident and a loss of employment estimated
at six million jobs (van Arnam, 2001). Industrial espionage can also be described as corporate
spying, corporate espionage, or economic espionage. Essentially, industrial espionage is the use of espionage or spying techniques often focused on commercial rivals for commercial purposes e.g. seeking to access trade secrets, intellectual property (IP) such as patents, copyrights, trademarks, recipes, product formulations, theories, software, processing techniques, designs or data that could impact brand value for commercial advantage (Crane, 2005; Bogadi, Banović, & Babić, 2016). e.g. production details, strategic or marketing information (Budiono, & Sawitri, 2017).

Historical examples of industrial espionage include: two employees of DuPont Industrial Biosciences stealing information about the manufacturing process for titanium dioxide, an ingredient used in the food industry and then selling the information on to a Chinese chemical company (O’Halloran, 2014; Bogadi, Banović, & Babić, 2016); stealing the blueprints of the British Cartwright power loom (Fan, Jun, & Wolfstetter, 2016), an attempt to steal the blueprints for the Intel Pentium processor by an employee (van Arnam, 2001); smuggling of silkworms from China 1500 years ago and stealing of IP around porcelain (van Arnam, 2001); and theft of IP surrounding tea production in China (Budiono, & Sawitri, 2017; Fan, Jun, & Wolfstetter, 2017).

Case study 4: East India Company - Tea

In 1848, the British wanted to be able to grow tea in India and break into a trade monopolised at the time by China (Budiono, & Sawitri, 2017). Therefore the East India Co. employed a botanist, Robert Fortune, to visit China and to smuggle materials and obtain the information on growing tea plants and the making/processing of tea (Fortune, 1852; Budiono, & Sawitri, 2017). Sigley (2015) explores this case in more detail:

“[Fortune] was given the task of travelling to China, and in particular to the tea growing regions of Fujian and Anhui, to collect tea seeds and live tea seedlings and transport them back to India. He was also directed to obtain as much knowledge about the tea production
Robert Fortune’s mission was very successful. He collected a large horde of tea plants and seeds and also convinced a number of tea farmers from Anhui to go with him to India to assist in the growing and production of the tea.” (Sigley, 2015:332)

The case of espionage described here involved the stealing of physical material and information, however modern food defence strategies also need to include strategies to prevent covert digital threats such as cyber-crime and hacktivism.

2.5 Covert threats (Cyber-attacks)

Identity is the characteristics that determine who or what a person, product or organisation is and this identity can exist in both the physical and in the digital arena. Thus identity theft is the use of an individual’s or organisation’s identity by another individual or organisation for financial gain, espionage, revenge, or terrorism (Vidalis & Angelopoulou, 2014). Thus digital identity theft can be considered as an element of wider identity fraud.

Information security is very important. Indeed (Budiono, & Sawitri, 2017:31) state that threats focused on information theft “can infiltrate all levels of the organisation; product development, production, innovation, information security, personnel policies, finance, mergers & acquisitions, strategy, foreign relations, cultural diversity, ethics, technology and information policy.” Hackers, via security weaknesses, deface or disable web sites, attack networks, or disrupt programmes by adding code that is then used to gain access to more sensitive data (van Arnam, 2001). The most common reasons for an individual(s) to hack a given companies is to attempt to reduce the business efficiency of food companies as well as to enable data theft (Bogadi, Banović, & Babić, 2016). Hacktivists undertake cyber-attacks that are ideologically or politically motivated e.g. data exposure to highlight potential unethical practices by institutions. Examples include in the Stuxnet worm in July 2010 aimed at Siemens systems and specifically the Iran nuclear programme (Detica, 2011); 2014 the hacktivist group Anonymous caused major disruption in hospital operations at Boston’s Children’s Hospital (Mohammed,
The nature of cyber threats is evolving rapidly and there is constant evolution in technology and the ability to infiltrate digital networks (Khursheed, Kumar, & Sharma, 2016). Bendovschi (2015) divides cyber-attacks into four categories, based on the objective of the attack namely: cyber-crime, cyber espionage, cyber war (not considered here) and hacktivism. Cyber-crime is the unauthorised access to electronic communication and databases, networks, programmes and data in order to “compromise the confidentiality, integrity and availability of information” that belongs to given organisations or supply chains (Bendovschi, 2015:25). Cyber espionage is essentially the ability to obtain data without the permission of the data owner (Dawson, 2018). Particular mechanisms and techniques that fall within the scope of such cyber attacks include phishing, malware, and distributed denial of service (DDos) see Table 3. Take in Table 3

In 2012, two Romanian men admitted participating in an international conspiracy that hacked into Subway credit-card payment terminals at more than 150 Subway restaurant franchises and stole data from more than 146,000 compromised cards with more than $10 million in losses (Gross, 2012; Khursheed, Kumar, & Sharma, 2016). The work of Bendovschi (2015) highlights that while the public sector such as government, or law enforcement is most likely to be the victim of cyber espionage, cyber war and hacktivism techniques, cyber-crime is a problem for all business sectors. The UK Cyber Security Breaches Survey (2018) highlights that 43% of businesses surveyed in 2017 (n=1519) identified they had been victim to a cyber attack in the previous twelve months rising to 72% in large businesses (250 employees or more) and only 27% of the businesses had a formal cyber security policy, 13% had a formal cyber security incident management process and 9% held specific cyber security insurance. Further in the
survey only 20% of businesses had staff who had attended a cybersecurity training session in
the last twelve months barriers to take-up being cost, format and access and not seeing the need
for training. The multiple types of cyber-attack highlighted in Table 3 e.g. brute force attack,
distributed denial of service, financial attack, data corruption or data exposure, man in the
middle attacks, phishing, malware, scareware and system penetration are all viable food defense
risks that sit outside the definition of intentional product adulteration. The biggest vulnerability
to cyber-attacks was where staff used personal devices for work or cloud computing. McGuire
(2012) proposed a typology of six types of cybercrime groups with three subgroups each with
two subtypes (Table 4).

**Take in Table 4**

The three types are firstly online offending via a swarm typical of hacktivist groups, hubs that
drive phishing attacks or use of scareware, type 2 hybrids with both online and offline
offending either as clusters or extended networks and thirdly mainly offline groups. This final
type can be based on hierarchical groups or temporary assemblages of aggregate groups that
can align and then realign. The existence of these cyber criminal groups means that food supply
chain organisations need to be on their guard and have effective food defense strategies to
mitigate risk. Further empirical research needs to be undertaken to determine whether this is
actually the case.

Cybersecurity can be described as the countermeasures taken to protect a computer system
and associated storage clouds or individual appliance against an intentional malicious target
attack and/or unauthorised access and unintentional or accidental access (Soon, Manning &
Smith, 2019). ISO 27001:2013 Information Security Management Systems is the international
standard that sets out a series of requirements for establishing, implementing, monitoring and
improving an Information Security Management System (ISMS). Security management is the
“systematic and coordinated activities and practices through which an organisation optimally
manages its risks, and the associated potential threats and impacts there from” (ISO 28000:2007). Security management is critical with regard to digital security and also with physical security in the supply chain as addressed by ISO 28000 especially with regard to threats such as theft, or terrorism. Specific and generic food defence strategies are now discussed.

3. Food defence strategies: supply chain and organisational levels

To be successful, perpetrators of the activities described in this paper rely on a lack of preparedness by the victim (Olson, 2012: Wiśniewska, 2015). Therefore, in order to be effective, food defence strategies needs to consider the perpetrator, the relevance of the impact of potential attacks in terms of risk to the consumer, and also how that frames the perpetrators motivation to cause harm (Manning and Soon, 2016).

3.1 Food defense strategies

Food defence risk assessment, especially with regard to microbial agents, should consider the availability of potential agents, the potential perpetrator, the means of weaponisation and the deliver of the agent, and the likelihood of detection between dissemination and infection as well as product associated risks such as geopolitical factors, specific consumer populations at risk, psychological impact e.g. threats centred on foods used for religious ceremonies and the challenge of mixing or diluting the agent in a given product (Elad, 2005). The FDA require food defence vulnerability assessments (FDA, 2018b) such as CARVER+Shock, whilst GFSI (2017) refers to food defence threat assessment such as TACCP. Risk assessment methods currently used by the industry include TACCP (see Manning and Soon (2016) for a wider discussion) and a combined food safety (hazard analysis critical control point or HACCP). Another approach is to develop a food defence plan using a hazard analysis critical control and defense points (HACCP-DP) plan, where HACCPDP is an extension of a food safety plan and TACCP is a stand-alone threat and vulnerability risk assessment process and associated plan
(Wiśniewska, 2015). Essentially the process for developing a HACCP-DP plan as outlined by Yoe and Schwartz (2010) is to build on the established seven principles and twelve steps of HACCP with three further steps to build the food defence element:

- Step 1 – determine critical defence points (CDPs) in your process
- Step 2 – define food defence mitigation (more recently termed countermeasures)
- Step 3 – implement test, assess and maintain defence mitigation activities

This holistic approach is limited within the scope of food defence used in this paper as it would mainly address examples of intentional adulteration rather than food defence threats such as espionage, cyber-crime and hacktivism that are not necessarily related to food product adulteration. The HACCP-DP approach and requires those applying the tool to have appropriate training on food safety, food fraud (if that falls within the scope of the HACCP-DP) and food defence. The application of TACCP aims to reduce the likelihood and consequences of a food fraud or a food defence threat being realised. The scope of TACCP includes both EMA, wider aspects of food fraud such as counterfeiting and also intentional adulteration, food terrorism, and extortion, as well as covert activities such as sabotage, espionage and cybercrime. HACCP-DP, and TACCP both use a semi-quantitative risk assessment as does CARVER-SHOCK approaches and vulnerability analysis critical control point (VACCP) and wider vulnerability assessment tools. This creates a challenge in that only known and assessable threats can be prioritised in this way. Indeed the greatest flaw in these approaches is the recognised hazard (threat), control measure (countermeasure) and then a subjective scoring system to identify CCPs or CDPs. The weaknesses embedded in assessing non-microbial food safety hazards via a HACCP, translates to TACCP in terms of what is deemed an acceptable risk has both scientific, legal and moral aspects and thus is a relative construct and not just a binary decision. However as Wiśniewska (2015) outlines the advantage of using HACCP-based approaches to build food defence strategies is that they are familiar to
the food industry and thus are more easily adopted and integrated into existing systems and practices. A concern that can be raised though, is that whilst a food safety HACCP plan is in continuous use and this maintains familiarity with controls and preventive and corrective actions, food defence issues occur much less frequently and this means that knowledge and understanding of food defence strategies and how they are employed may be lost unless regular refresher training is undertaken. Further, given the very relative low probability of a deliberate food defense event, some organisations may feel that the costs of implementing food defense plans is disproportionate to the actual risk (Davidson et al. 2017). The risk assessment tools (HACCP, TACCP, VACCP, HACCP-DP) considered here have limited value in terms of unknown or unquantifiable threats creating then potential for vulnerabilities to be unrecognised and this leads to the possibility that decision-makers may identify a subsequent incident as being unforeseeable.

3.2 Guardians and hurdles

Appealing to criminology literature gives rise to specific terminology which those developing food defence strategies meet to be conversant with. The crime triangle as explored by Spink et al. (2016) includes consideration of the perpetrator, the victim and how opportunity for the activity to take place is mediated by guardians and hurdles. The food defence team members and the plan implementers roles are to be “guardians” i.e. the individuals operating at supply chain or individual business or production line levels (Spink et al. 2015) that have the knowledge, skills and understanding to develop and implement food defence strategies. The visibility of food defence guardians acts as a deterrent (Reynald, 2009; Hollis & Willson, 2014; Manning, Soon & Smith, 2019) and thus is essential to delivering effective food defence strategies. However those designated as guardians need to understand their role and what is expected of them so effective training is essential with refresher activities in the event that new threats emerge. *Hurdles* are the formal system components that reduce opportunity for food
crime by either assisting detection or by acting as a deterrent (Spink et al. 2015; Manning, Soon & Smith, 2019). Hurdles can be physical hurdles in terms of protecting structural assets (barriers, enclosed production systems), or artefact-based hurdles such as procedures and protocols or cyber-protection via firewalls and virus software. Thus the HACCP-DP plan will signpost to relevant hurdles and guardians as well as defining countermeasures that are adopted within food defense strategies to mitigate risk.

3.3 Countermeasures

Countermeasures are measures, often preventive in nature, are intended to reduce criminal opportunity in food supply chains (Spink et al. 2015). Physical and technical countermeasures such as physical hurdles are referred to as hard controls whereas managerial controls (artefact based hurdles) are termed soft controls (van Ruth, Huisman & Luning, 2017).

Passive countermeasures are in operation at all times e.g. supplier assessment protocols whereas reactive countermeasures are implemented should an incident occur in order to lessen the impact once the threat is realised (Mitenus, Kennedy & Busta, 2014), for example product recall strategies or product testing programmes as in the case of the 1080 incident in NZ. Countermeasures for food defence are often the same global or specific protocols and policies that have been developed as part of existing pre-requisite programmes such as good manufacturing practice (GMP) or good hygienic practice (GHP).

With regard to cyber attacks specifically, organisations need to have a clear defence strategy and will often need outside expertise to assist them to reduce vulnerability. Bendovschi (2015) determines three kinds of countermeasure within a cybersecurity strategy: preventive security controls that aim to prevent the realisation of a threat i.e. to restrict and prevent unauthorised access to an organisation’s network, programmes or data; detective security controls that seek to detect information security threats e.g. intrusion detection systems that monitors network traffic and potentially suspicious activity; corrective security controls
that are implemented if non-conformity is identified and implement business recovery procedures after a cyber attack.

4. Concluding thoughts

Food defence is an under-researched phenomenon and there is limited information in the public domain on the topic area. At the same time as an inherent knowledge gap in industry on what food defence strategies need to address, there is an increasing requirement for organisations in the food supply chain to develop and adopt food defence strategies to assure market entry through third-party certification of their management systems. Certification standards include those benchmarked to the GFSI standards. In order countries such as the US there is a regulatory requirement to develop food defense strategies too. To develop food industry guidance and to inform food defence risk assessment and management processes, a taxonomy needs to be developed and accepted across the food industry so that threats can be consistently identified and effectively addressed and as a result consumers, industry partners, shareholders and also the organisation itself can be protected. The taxonomy developed in this research frames both physical and digital threats, and overt and covert threats and introduces the term impact orientated adulteration to clearly distinguish these types of product-related threats from wider EMA issues. The work gives particular insight into the types of cyber crimes and cyber criminals that are of concern in the food supply chain and this will support more effective risk assessment of these particular types of threats.
5. References


BBC (2018), Poisoned baby food: German jailed for attempted murder, Available at: https://www.bbc.co.uk/news/amp/world-europe-45951642 [Accessed 23 October 2018]

BBC (2016), New Zealand man jailed for milk formula 1080 threat, Available at: https://www.bbc.co.uk/news/world-asia-35878645 [Accessed 10th October 2018].


FDA (2018b), Food defense, Available at: https://www.fda.gov/Food/FoodDefense/default.htm [Accessed 21 September 2018]


Smith, L. (2016). £2 million blackmail plotter claimed he had laced supermarket food with cyanide. Available at: https://www.mirror.co.uk/news/trials/2million-blackmail-plotter-claimed-laced-8751269 [Accessed 16 October 2018]


The Independent (1999), Food Scare Scandals Available at: https://www.independent.co.uk/news/food-scare-scandals-1100385.html [Accessed 12 October 2018]


US Code Title 22 Chapter 38 2656f – Annual country reports on terrorism Available at: https://www.law.cornell.edu/uscode/text/22/2656f [Accessed 15 December 2018]


<table>
<thead>
<tr>
<th>Stage of supply chain</th>
<th>Total confirmed cases</th>
<th>Agents used</th>
<th>Fatalities</th>
<th>Injuries</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water Supply</td>
<td>7</td>
<td>Pesticide, Insecticide, Cyanide, Sheep dip, VX, Sarin</td>
<td>3</td>
<td>&lt;100</td>
<td>Multiple additional unconfirmed incidents</td>
</tr>
<tr>
<td>Pre-harvest</td>
<td>365</td>
<td>Glyphosate, plant toxin, cyanide, cattle feed as a vehicle, rodenticide</td>
<td>0</td>
<td>0</td>
<td>Impact limited to the animals concerned or the crops prevented from entering the food supply chain. Key countermeasure is investigation post livestock death or identification of crop contamination and removal from the market.</td>
</tr>
<tr>
<td>Post harvest, and manufacturing</td>
<td>3</td>
<td>Mercury, glass, needles, rat poison</td>
<td>0</td>
<td>125</td>
<td>Numerous unconfirmed incidents</td>
</tr>
<tr>
<td>Retail and food service</td>
<td>89</td>
<td>Acetone, Arsenic, Atropine, Cyanide, Herbicide, Insecticide, Pesticide, Physical contaminants incl. rodenticide, Rohypnol, Salmonella Typhimurium, Thallium</td>
<td>123</td>
<td>3394</td>
<td>These cases include alleged assassination attempts. The 1984 Rajneeshee cult incident affected 751 people. An incident in 1992 in Zhengzhou, China affected 788 people who fell ill from arsenic poisoning in flour in the school cafeteria. In 2005, 28 people died and 130 were injured from organophosphate pesticide in cassava fritters sold to school children</td>
</tr>
<tr>
<td>Consumer/Home</td>
<td>265</td>
<td>Multiple</td>
<td>265</td>
<td>670</td>
<td>Many cases were intentional homicide focused on specific individuals (victims) often family members.</td>
</tr>
</tbody>
</table>
Table 2. Examples of questionable espionage tactics (Adapted from Crane, 2005)

<table>
<thead>
<tr>
<th>Questionable tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaking and entering into a competitor’s premises to steal information or installing recording devices.</td>
</tr>
<tr>
<td>Contacting competitors with fake identity such as a potential customer or supplier</td>
</tr>
<tr>
<td>Covert surveillance through spy cameras.</td>
</tr>
<tr>
<td>Hiring private detectives to track competitor’s staff.</td>
</tr>
<tr>
<td>Infiltrating competitor organisations with industrial spies.</td>
</tr>
<tr>
<td>Interviewing competitors’ employees for a bogus job vacancy.</td>
</tr>
<tr>
<td>Pressuring the customers or suppliers of competitors to reveal sensitive information about their operations.</td>
</tr>
<tr>
<td>Searching through a competitor’s rubbish.</td>
</tr>
<tr>
<td>Type of attack</td>
</tr>
<tr>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Brute force attack</strong></td>
</tr>
<tr>
<td>describes repeated attempts to gain access to protected information (e.g. passwords, encryption, etc.) until the correct key is found, and security is breached. <strong>Social engineering</strong> is the general term that describes techniques used to gain unauthorised access to information through human interaction</td>
</tr>
<tr>
<td><strong>Data corruption</strong></td>
</tr>
<tr>
<td>to cause disruption to services and activities</td>
</tr>
<tr>
<td><strong>Data exposure</strong></td>
</tr>
<tr>
<td>often in an attempt to show unethical behaviour or conduct</td>
</tr>
<tr>
<td><strong>Defacement</strong></td>
</tr>
<tr>
<td>of websites often with political or ideological slogans</td>
</tr>
<tr>
<td><strong>Distributed Denial of Service (DDoS)</strong> is a type of attack that compromises the availability of data, in the way that the attacker floods the victim (e.g. server) with commands, thus becoming inoperable. Extortion attempts may them be made by the attacker to clean up the computer or recover full services</td>
</tr>
<tr>
<td><strong>Financial attack</strong></td>
</tr>
<tr>
<td>to steal money from accounts or fraudulent emails or links to fake tax revenue forms</td>
</tr>
<tr>
<td><strong>Malware</strong></td>
</tr>
<tr>
<td>is a generic term describing types of malicious software. Examples of malware are: viruses, worms, trojans, spyware, ransomware, adware and scareware/rogware.</td>
</tr>
<tr>
<td><strong>Man in the middle (MitM) attack</strong> occurs when the attacker interferes between two organisations i.e. every message sent from source A to source B and vice versa reaches the attacker before reaching its destination.</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
</tr>
<tr>
<td>is a technique that aims to steal confidential information from users by masquerading as a trusted source (e.g. website)</td>
</tr>
<tr>
<td><strong>Scareware</strong></td>
</tr>
<tr>
<td>is a technique where the attacker misleads individuals into downloading software onto their computer by using fear tactics or unethical marketing practices e.g. by frightening individuals that their computer is at risk</td>
</tr>
<tr>
<td><strong>System penetration</strong></td>
</tr>
</tbody>
</table>
Table 4: Typology of cyber criminals (Adapted from McGuire, 2012; Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014).

<table>
<thead>
<tr>
<th>Sub-group</th>
<th>Sub-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1 – online offending</td>
<td>Swarms</td>
<td>Large disorganised networks that are active online and are typically made up of clusters of ideologically driven individuals. Lack clear command structure. Swarms are characteristic of hacktivist groups.</td>
</tr>
<tr>
<td></td>
<td>Hubs</td>
<td>Large collective organisations/networks with clear focal point (hub) and command structure. Strong ties and continued interaction between individual members. Activities include development of botnets, phishing attacks, use of scareware</td>
</tr>
<tr>
<td>Type 2 – Hybrids with online and offline offending</td>
<td>Clustered hybrid</td>
<td>Small group of individuals that are focused on specific activities and interactions as with a hub but their activity is both online and offline offending e.g. skimming cards in the physical world to then use the data online.</td>
</tr>
<tr>
<td></td>
<td>Extended hybrid</td>
<td>Not as centralised as a clustered hybrid. More subgroups and associates but still with a level of coordination</td>
</tr>
<tr>
<td>Type 3 – Mainly offline but undertake some activity online</td>
<td>Hierarchies</td>
<td>Traditional criminal groups who transpose some activities online e.g. increasing scope of extortion activities.</td>
</tr>
<tr>
<td></td>
<td>Aggregate groups</td>
<td>Loosely organised, temporary groups with opaque purpose that use digital technology in a disorganised way to support other activities</td>
</tr>
</tbody>
</table>