

Food defence: Refining the taxonomy of food defence threats

by Manning, L.

Copyright, publisher and additional information: This is the author accepted manuscript. The final published version (version of record) is available online via Elsevier.

This version is made available under the CC-BY-ND-NC licence:
<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

Please refer to any applicable terms of use of the publisher

DOI: <https://doi.org/10.1016/j.tifs.2019.01.008>



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.

43 **1. Introduction**

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

61 Some suggest that food defence related activities are distinct from food fraud (Spink &
62 Moyer, 2011b) as they are motivated by the impact they cause i.e. food defence strategies
63 encompasses the activities or efforts undertaken to protect food from intentional acts of
64 adulteration (FDA, 2018b). However, other US regulatory sources state food defense “means
65 the effort to protect food from intentional acts of adulteration where there is an intent to cause
66 wide scale public health harm.” (FDA, 2018a). This suggests that food defense plans should
67 only address those threats where the intent is widespread harm and it is the size of impact that

68 predetermines what should be considered and addressed in a food defence plan. This is at odds
69 with the Global Food Safety Initiative definition that states it includes all forms of intentional
70 malicious attack (GFSI, 2014; GFSI, 2017; BRC, 2018), malicious tampering or terrorism
71 (Spink & Moyer, 2011b), or a malicious and ideologically motivated attack leading to
72 compromised products and/or supply chain disruption (PAS 96, 2017), panic or fear (Spink,
73 Moyer, Park, & Heinonen, 2013).

74 This narrative across the literature suggests intentional adulteration addressed by food
75 defence strategies is separate from the strategies to address economically motivated
76 adulteration (EMA). Whilst with EMA the aim of the perpetrators is for intentional adulteration
77 to continue undiscovered for as long as possible so that the maximum financial benefit can be
78 derived, food defence threats are different. Food defence threats include activities that are
79 “impact motivated” whereby an agent that is chemical, biological, radiological, nuclear
80 (CBRN) or physical in nature, is used by perpetrators who seek to maliciously and intentionally
81 adulterate food where such activities are actively disclosed to organisations and the general
82 public in order to derive the associated personal, political or social impact. Food defence threats
83 reflect a motivation to do harm to distinct and targeted victim(s) with notions of personal
84 benefit to the perpetrator in terms of underpinning an ideological statement, a means to gain
85 notoriety, revenge, restorative justice or envy, (Hirschl, 1969; Cohen & Felson, 1979; Pease,
86 2006; Walklate, 2007; Hirschauer & Zwoll, 2008). Some sources consider that the scope of
87 food defense includes all intentional activities seen as a threat including food fraud, tampering
88 and food terrorism (Davidson et al. 2016) and wider threats too (PAS 96, 2017).

89 A threat is “something that can cause loss or harm which arises from the ill-intent of
90 people” (PAS 96, 2017:3). The distinction between an agent and the threat is again confused
91 in the literature with some sources defining the material agent itself as a threat. PAS 96 (2017)
92 differentiates between six types of threats to that need to be addressed under food fraud (EMA,

93 counterfeiting) and food defence mitigation strategies i.e. malicious contamination, extortion,
94 espionage, and cyber-crime. The scope of PAS 96 (2017) is wider than that suggested by the
95 FDA (2018a) in terms of food defence which states that:

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

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

113 Therefore, food defense encompasses the active steps taken, the protection activities, and/or
114 the security assurance process or procedures, often called countermeasures, that deliver product
115 safety with regard to intentional acts of adulteration to cause harm (Manning & Soon, 2016).
116 The term food defense describes what needs to be done i.e. procedures, protocols, or processes
117 to mitigate a given activity or threat rather than focusing on the specific taxonomy of activities

118 or perpetrators. Increasingly, these procedures and protocols are seen by retailers,
119 manufacturers and food service as a pre-requisite to supply (Wiśniewska, 2015). However, in
120 order to be able to implement effective food defense mitigation strategies, a clear understanding
121 of the potential threats, and associated motivations and rationalisation used by perpetrators and
122 also the agents they might employ is essential. This level of understanding is further framed by
123 determining how to develop countermeasures that reduce both the capability of the perpetrators
124 to take action and also reduce the opportunities for such action to occur.

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

132 **2. Taxonomy of food defense threats and perpetrators**

133 **2.1 Intentional impact orientated adulteration and extortion**

134 At its simplest the taxonomy of food defense threats for impact orientated adulteration
135 rather than EMA can be described in terms of adulteration through the use of hazardous agents
136 i.e. biological agents, chemical agents, physical agents and radiological agents (Dalziel, 2009;
137 Fredrickson, 2014). The diversity of these agents is complex driven primarily by ease of access
138 e.g. the decision to use glass which is readily available versus radionuclear material which is
139 not, and secondly, the means and opportunity for contamination e.g. on farm, within
140 manufacturing and processing, food service, retail or the home (Meulenbelt, 2018). Table 1
141 synthesizes data on confirmed incidents in the literature, examples of agents used by location
142 in the supply chain and their impact. The data shows that confirmed incidents are

143 predominantly at the tertiary stages of the supply chain and also in the home some of which
144 are cases of domestic poisoning which do not fit within a reflection on food defense strategies
145 employed at organisational level. The majority of the confirmed cases take place pre-harvest
146 (n=365), then in the home (n=265) and then at retail and food service (n=89). Agents used at
147 farm level have included glyphosate, plant toxin, cyanide, and rodenticide, with a much wider
148 range of agents at food service and retail level.

149 **Take in Table 1**

150

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

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

160 In 1989 Heinz had to withdraw from sale batches of baby food in the UK worth an
161 estimated £30 million pounds when Rodney Whitchelo, a former Scotland Yard detective who
162 was later sentenced to seventeen years in prison, attempted to extort millions of pounds from
163 the food giant by spiking the food with bleach and razor blades (The Independent, 1999). Fisher
164 (1989) highlights how after the initial publicity about contamination of food, copy-cat cases
165 occurred causing concern and fear to escalate with 220 reported incidents of baby food
166 contamination in April 1989. However police first began their investigations in August 1988
167 when £20,000 was demanded by the extortionist and paid into a bank account and then

168 subsequently removed from various cash points (ATMs). After the initial payments stopped
169 the extortionist demanded £1 million from Heinz contaminating two cans of baby food after
170 the demand. The perpetrator was eventually charged, tried and imprisoned. This case study
171 shows the challenges of the renegade insider who commits a crime whilst being aware of the
172 protocols and checks and balances in place within criminal investigations i.e. they can
173 circumvent the food defence systems that have been designed and implemented . This case is
174 not alone.

175 In a case in 2016 in the UK an extortionist who demanded £2 million not to contaminate
176 food with cyanide was traced through his DNA on the stamp on the letter and was jailed for
177 seven years. The vial sent with the letter contained five to ten lethal doses of cyanide (Smith,
178 2016). In September 2017, a German man was charged with threatening to put poisoned baby
179 food throughout Europe with a demand to multiple supermarkets for nearly £8.8 million (Licea,
180 2017; Rojas, 2017). The man's DNA was found on five jars that were recovered from stores
181 and then found to contain ethylene glycol. Psychological issues were cited as a mitigating issue
182 with the perpetrator, but this was rejected in court and he was found guilty of attempted murder
183 and extortion and sentenced to twelve and a half years in prison (BBC, 2018).

184 **Case Study 2: Fonterra, New Zealand (NZ)**

185 In November 2014, Fonterra was the victim of anonymous threats to contaminate
186 commercial milk supplies with sodium fluoroacetate or 1080, a pesticide, unless its usage was
187 halted on farm (Manhire, 2015). Highly concentrated levels of 1080 were mixed with infant
188 formula and posted to Fonterra and Federated Farmers with a letter stating contaminated infant
189 milk powder would enter the Chinese and other markets (NZHerald, 2016). Whilst
190 ecoterrorism was cited by some as a possible motive that led to the £18 million costs of the
191 incident, a NZ businessman, Jeremy Kerr was subsequently jailed for eight and a half years
192 after pleading guilty to two charges of attempted blackmail and the judge ruled that as he owned

193 a company that made an alternative pesticide to 1080 this had motivated his activities because
194 of the potential economic gain (BBC, 2016). The extortion threat required the dairy
195 organisation, Fonterra, to take action to develop a robust methodology for detection of 1080 in
196 milk and powdered milk products (Cooney, Varelis & Bendall, 2016). Cooney et al. (2016)
197 state that having developed and validated the methodology between January and July 2015,
198 136,000 fluid milk samples were tested as part of a multi-agency food defense strategy to
199 maintain confidence in the safety of NZ milk and dairy products. This case study highlights
200 the challenge of addressing a food defense incident early on in the investigation, especially
201 where no existing tests exist to check for the presence of the reported agent in the supply chain,
202 the crucial role of intelligence and the need for police forces to work closely with food
203 businesses. The risk of food terrorism was hinted at in this case study, but food terrorism is a
204 real threat and is now considered.

205 **2.2. Food terrorism**

206 Terrorism is defined in Title 22 Chapter 38 of US. Code 2656f as "premeditated,
207 politically motivated violence perpetrated against noncombatant [civilian] targets by
208 subnational groups or clandestine agents." The North Atlantic Treaty Organisation (2014)
209 define terrorism as "the unlawful use or threatened use of force or violence against individuals
210 or property in an attempt to coerce or intimidate governments or societies to achieve political,
211 religious or ideological objectives." Terrorist activities, usually but not always undertaken by
212 non-nation actors, are designed to engender fear, terror, panic and anxiety in the population
213 and as a result reduce the level of confidence in the government, leading to uncertainty and
214 political instability (Alvarez et al. 2010; Fredrickson, 2014) or the attainment of a specific
215 political goal (Nestle, 2003). Food terrorism is defined as "the deliberate (or threat of)
216 contamination of food with hazardous agents (biological, chemical, physical, or radionuclear)
217 for the purpose of causing injury or death and/or disrupting social, economic, or political

218 stability” (Fredrickson, 2014:311). Thus food terrorism, if it occurs, could cause severe health
219 implications to the population and economic and trade disruption either through direct costs
220 due to the culling of livestock, disposal of food products and the potential compensation paid
221 to farmers and producers and the impact on public health services including the cost of
222 hospitalisation (Manning et al. 2005). Further, food terrorism can lead to consequential loss to
223 the local or national economy, loss of consumer confidence in the food supply chain and loss
224 of political confidence and support following a major food product recall or the mass culling
225 of livestock (Manning et al. 2005). An example of the impact on public health services of a
226 terrorism incident is the 1995 nerve gas attack on the Tokyo subway system that caused 12
227 deaths and required 5000 people to seek medical attention involving 131 ambulances, 1364
228 emergency technicians and over 4000 people needing to get to medical care themselves (WHO,
229 2002). A similar incident associated with food could have equal impact. In 2011, there was an
230 *Escherichia coli* O104:H4 outbreak in Germany associated with sprouts from fenugreek seeds
231 which was not explicitly connected to a food defence threat, but its impact demonstrates how
232 a similar food defense issue could cause significant challenges. Between May 2011 and July
233 2011, the outbreak involved 3,842 cases (including 2,987 cases of gastrointestinal disease
234 characterised by diarrhea), with 855 cases of hemolytic uremic syndrome (HUS) and 53 deaths
235 (RKI, 2012) with at the peak of the outbreak more than 50 reported cases of HUS per day
236 (McIntyre & Monaghan, 2016). The outbreak caused widespread concern and panic and a
237 change to eating habits, as well as economic consequences impact particularly for farmers with
238 the EU paying 220 million Euros for the loss of income (Burger, 2012).

239 Terrorism acts can be differentiated by those that seek to cause actual harm to
240 individuals or populations and alternatively those acts that are symbolic to provoke anxiety and
241 concern, and to change consumer behaviour leading to economic loss (Alvarez et al. 2010).
242 The World Health Organisation (WHO) in their 2002 Report “*Terrorist threats to food:*

243 *guidance for establishing and strengthening prevention and response systems”* states that an
244 essential means to preventing food terrorism is the development, validation, implementation,
245 monitoring and effective verification of food safety management programmes and their
246 associated security measures, described here as countermeasures. To minimise risk, the report
247 states that effective prevention requires food defence strategies to provide a concerted approach
248 between government and industry. Prevention is not the only approach within food defence
249 strategies, surveillance is another element that should be employed. Agro-terrorism is the
250 deliberate introduction of an animal or plant disease with the goal of generating fear, causing
251 economic losses, and/or undermining social stability (Monke, 2007).

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

258 **Case study 3: Kerry Foods, UK**

259 Temporary factory worker Munir Mohammed who was involved in ready meal manufacture at
260 the Kerry Foods factory, and a pharmacist, Rowaida El Hasssan were arrested in December
261 2016 and convicted in January 2018 of planning a terrorist attack using food as the vehicle
262 (Stones, 2018). They were arrested after counter-terrorism surveillance identified that they had
263 undertaken extensive on-line research on acetone peroxide or TATP and ricin both realistic
264 agents for a terror attack on the food supply. The food company as well as the UK population
265 were potential victims here. Kerry Foods were unaware that Munir Mohammed had been
266 working illegally at the factory as he used EU documents in another man's name to gain work
267 at the factory (Kreft & Crowson, 2018). This shows how important induction checks are for

268 assuring that individuals working at food factories are who they claim to be. However these
269 checks have limited preventive capacity if individuals intentionally lie about their identity.
270 Other examples of recent food related terror threats include: in June 2016, Italian anarchists
271 threatened to contaminate foodstuff in supermarkets in Lombardy with herbicide and in
272 December 2016, Greek anarchists claimed they had contaminated several food and drink
273 products of multinational companies (EUROPOL, 2017). However intentional adulteration
274 linked to the product is just one type of overt threat that needs to be addressed by food defense
275 strategies. Clandestine or covert threats, where activities or the identity of perpetrators is
276 purposefully hidden (Lord, 2015) are now considered.

277 **2.3 Covert Threats (Sabotage)**

278 In history, there have been multiple occasions when civilian food supplies have been
279 sabotaged deliberately, during military campaigns or to deliver a specific social or
280 political impact (Torok et al. 1997) with the associated trade and economic repercussions
281 (WHO, 2002). Biological sabotage agents include zoonoses or animal disease (Manning,
282 Baines & Chadd, 2005), but other agents could be used and their nature is primarily driven by
283 their availability to the perpetrator. Previous sabotage actions against the food supply include
284 to fruit trees and livestock in Palestine in 1933, or just more generally instances of working
285 slowly, or instances of deliberate fire, damaging goods and intentionally breaking equipment.
286 Thus, a saboteur is an individual who deliberately damages or destroys assets or infrastructure
287 in order to weaken an enemy or make a protest (Collins Dictionary, nd). At the supply chain
288 level, sabotage involves the “destruction of essential infrastructure affects people’s ability to
289 access, process, distribute and utilise food.” (Koc, Jernigan, & Das, 2007:321) or a clandestine
290 act to destroy, damage or render assets unusable (Douthit, 1987). The motivation for
291 sabotage behaviour is a wish to “damage, disrupt, or subvert the organisation’s operations for
292 the personal purposes of the saboteur by creating unfavourable publicity, embarrassment,

293 delays in production, damage to property, the destruction of working relationships, or the
294 harming of employees or customers’’ (Crino, 1994:312). In this context, industrial sabotage
295 can be seen as a form of counterproductive work behaviour (CWB) i.e. wilful behaviour by
296 employees that could cause harm to fellow employees or the organisation itself (Spector &
297 Fox, 2005; Krischer, Penney, & Hunter, 2010). Taylor and Walton (1971) cite a number of
298 examples of industrial sabotage including one organisation having to throw away half a mile
299 of “Blackpool rock” because an offensive expletive had been printed through the product. They
300 argue that sabotage can be a singular or group activity, demonstrates underlying industrial
301 conflict, and may link with other deviant and often irrational behaviour. Therefore the potential
302 for an employee to undertake sabotage could be highlighted in advance by other negative
303 behaviours such as absenteeism, low morale and job satisfaction, stress, and poor performance
304 with job satisfaction being the mediating factor (Alias, Mohd Rasdi, Ismail, & Abu Samah,
305 2013). This work suggests that early warning systems can be developed to identify those
306 employees more likely to commit sabotage and to implement preventive strategies including
307 improving staff morale to reduce the risk of occurrence. A sense of injustice or inequality can
308 also be a leading motivational factor in workplace sabotage as can a sense of powerlessness or
309 lack of autonomy. Frustration, often a secondary motivational factor, is triggered by previous
310 incidents that then fuels anger, and a transition by workers from being rule compliance to
311 bending the rules i.e. simple deviance from prescribed organisational norms to ultimately
312 breaking the rules during work activities. This behaviour may have negative intent, be
313 motivated more simply by a need to meet organisational goals that cannot otherwise be met by
314 compliant behaviour, as a mechanism to reduce workplace boredom i.e. a means of
315 entertainment or to deliver what the perpetrator believes is a form of retaliatory action or
316 restorative justice (Ambrose, Seabright & Schminke, 2002). Reducing the risk of actions seen
317 by employees as restorative justice lies at the heart of how sabotage can be prevented by food

318 defence strategies. This includes the development of positive organisational culture to reduce
319 the potential for power dynamics, reducing management decisions that can be perceived as
320 driving inequality within the workplace or supply chain and not promoting goals (financial,
321 operational etc.) that can only be achieved by deviant behaviour.

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

324 **2.4 Covert Threats (Industrial Espionage)**

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

339 **Take in Table 2**

340 Estimates of the cost of such activity to US industry run between \$45 billion and \$100
341 billion per annum; an average of \$50 million per incident and a loss of employment estimated
342 at six million jobs (van Arnam, 2001). Industrial espionage can also be described as corporate

343 spying, corporate espionage, or economic espionage. Essentially, industrial espionage is the
344 use of espionage or spying techniques often focused on commercial rivals for commercial
345 purposes e.g. seeking to access trade secrets, intellectual property (IP) such as patents,
346 copyrights, trademarks, recipes, product formulations, theories, software, processing
347 techniques, designs or data that could impact brand value for commercial advantage (Crane,
348 2005; Bogadi, Banović, & Babić, 2016). e.g. production details, strategic or marketing
349 information (Budiono, & Sawitri, 2017).

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

359 **Case study 4: East India Company - Tea**

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

365 “[Fortune] was given the task of travelling to China, and in particular to the tea growing
366 regions of Fujian and Anhui, to collect tea seeds and live tea seedlings and transport them
367 back to India. He was also directed to obtain as much knowledge about the tea production

368 process as possible. Robert Fortune's mission was very successful. He collected a large horde
369 of tea plants and seeds and also convinced a number of tea farmers from Anhui to go with
370 him to India to assist in the growing and production of the tea." (Sigley, 2015:332)

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

374 **2.5 Covert threats (Cyber-attacks)**

375 Identity is the characteristics that determine who or what a person, product or
376 organisation is and this identity can exist in both the physical and in the digital arena. Thus
377 identity theft is the use of an individual's or organisation's identity by another individual or
378 organisation for financial gain, espionage, revenge, or terrorism (Vidalis & Angelopoulou,
379 2014). Thus digital identity theft can be considered as an element of wider identity fraud.
380 Information security is very important. Indeed (Budiono, & Sawitri, 2017:31) state that threats
381 focused on information theft "can infiltrate all levels of the organisation; product development,
382 production, innovation, information security, personnel policies, finance, mergers &
383 acquisitions, strategy, foreign relations, cultural diversity, ethics, technology and information
384 policy." Hackers, via security weaknesses, deface or disable web sites, attack networks, or
385 disrupt programmes by adding code that is then used to gain access to more sensitive data (van
386 Arnam, 2001). The most common reasons for an individual(s) to hack a given companies is to
387 attempt to reduce the business efficiency of food companies as well as to enable data theft
388 (Bogadi, Banović, & Babić, 2016). Hacktivists undertake cyber-attacks that are ideologically
389 or politically motivated e.g. data exposure to highlight potential unethical practices by
390 institutions. Examples include in the Stuxnet worm in July 2010 aimed at Siemens systems and
391 specifically the Iran nuclear programme (Detica, 2011); 2014 the hacktivist group Anonymous
392 caused major disruption in hospital operations at Boston's Children's Hospital (Mohammed,

393 2017); data exposure for South African banks (Van Niekerk, 2017); defacement of
394 organisational websites (Van Niekerk, 2017); and a malware attack on Merck (Mohammed,
395 2017).

396 The nature of cyber threats is evolving rapidly and there is constant evolution in
397 technology and the ability to infiltrate digital networks (Khursheed, Kumar, & Sharma, 2016).
398 Bendovschi (2015) divides cyber-attacks into four categories, based on the objective of the
399 attack namely: cyber-crime, cyber espionage, cyber war (not considered here) and hacktivism.
400 Cyber-crime is the unauthorised access to electronic communication and databases, networks,
401 programmes and data in order to “compromise the confidentiality, integrity and availability of
402 information” that belongs to given organisations or supply chains (Bendovschi, 2015:25).
403 Cyber espionage is essentially the ability to obtain data without the permission of the data
404 owner (Dawson, 2018). Particular mechanisms and techniques that fall within the scope of such
405 cyber attacks include phishing, malware, and distributed denial of service (DDos) see Table 3.

406 **Take in Table 3**

407 In 2012, two Romanian men admitted participating in an international conspiracy that hacked
408 into Subway credit-card payment terminals at more than 150 Subway restaurant franchises and
409 stole data from more than 146,000 compromised cards with more than \$10 million in losses
410 (Gross, 2012; Khursheed, Kumar, & Sharma, 2016). The work of Bendovschi (2015) highlights
411 that while the public sector such as government, or law enforcement is most likely to be the
412 victim of cyber espionage, cyber war and hacktivism techniques, cyber-crime is a problem for
413 all business sectors. The UK Cyber Security Breaches Survey (2018) highlights that 43% of
414 businesses surveyed in 2017 (n=1519) identified they had been victim to a cyber attack in the
415 previous twelve months rising to 72% in large businesses (250 employees or more) and only
416 27% of the businesses had a formal cyber security policy, 13% had a formal cyber security
417 incident management process and 9% held specific cyber security insurance. Further in the

418 survey only 20% of businesses had staff who had attended a cybersecurity training session in
419 the last twelve months barriers to take-up being cost, format and access and not seeing the need
420 for training. The multiple types of cyber-attack highlighted in Table 3 e.g. brute force attack,
421 distributed denial of service, financial attack, data corruption or data exposure, man in the
422 middle attacks, phishing, malware, scareware and system penetration are all viable food defense
423 risks that sit outside the definition of intentional product adulteration. The biggest vulnerability
424 to cyber-attacks was where staff used personal devices for work or cloud computing. McGuire
425 (2012) proposed a typology of six types of cybercrime groups with three subgroups each with
426 two subtypes (Table 4).

427 **Take in Table 4**

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

436 Cybersecurity can be described as the countermeasures taken to protect a computer system
437 and associated storage clouds or individual appliance against an intentional malicious target
438 attack and/or unauthorised access and unintentional or accidental access (Soon, Manning &
439 Smith, 2019). ISO 27001:2013 Information Security Management Systems is the international
440 standard that sets out a series of requirements for establishing, implementing, monitoring and
441 improving an Information Security Management System (ISMS). Security management is the
442 “systematic and coordinated activities and practices through which an organiaation optimally

443 manages its risks, and the associated potential threats and impacts there from” (ISO
444 28000:2007). Security management is critical with regard to digital security and also with
445 physical security in the supply chain as addressed by ISO 28000 especially with regard to
446 threats such as theft, or terrorism. Specific and generic food defence strategies are now
447 discussed.

448 **3. Food defence strategies: supply chain and organisational levels**

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

454 **3.1 Food defense strategies**

455 Food defence risk assessment, especially with regard to microbial agents, should consider the
456 availability of potential agents, the potential perpetrator, the means of weaponisation and the
457 deliver of the agent, and the likelihood of detection between dissemination and infection as
458 well as product associated risks such as geopolitical factors, specific consumer populations at
459 risk, psychological impact e.g. threats centred on foods used for religious ceremonies and the
460 challenge of mixing or diluting the agent in a given product (Elad, 2005). The FDA require
461 food defence vulnerability assessments (FDA, 2018b) such as CARVER+Shock, whilst GFSI
462 (2017) refers to food defence threat assessment such as TACCP. Risk assessment methods
463 currently used by the industry include TACCP (see Manning and Soon (2016) for a wider
464 discussion) and a combined food safety (hazard analysis critical control point or HACCP).
465 Another approach is to develop a food defence plan using a hazard analysis critical control and
466 defense points (HACCP-DP) plan, where HACCPDP is an extension of a food safety plan and
467 TACCP is a stand-alone threat and vulnerability risk assessment process and associated plan

468 (Wiśniewska, (2015). Essentially the process for developing a HACCP-DP plan as outlined by
469 Yoe and Schwartz (2010) is to build on the established seven principles and twelve steps of
470 HACCP with three further steps to build the food defence element:

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

474 This holistic approach is limited within the scope of food defence used in this paper as it would
475 mainly address examples of intentional adulteration rather than food defence threats such as
476 espionage, cyber-crime and hacktivism that are not necessarily related to food product
477 adulteration. The HACCP-DP approach and requires those applying the tool to have
478 appropriate training on food safety, food fraud (if that falls within the scope of the HACCP-
479 DP) and food defence. The application of TACCP aims to reduce the likelihood and
480 consequences of a food fraud or a food defence threat being realised. The scope of TACCP
481 includes both EMA, wider aspects of food fraud such as counterfeiting and also intentional
482 adulteration, food terrorism, and extortion, as well as covert activities such as sabotage,
483 espionage and cybercrime. HACCP-DP, and TACCP both use a semi-quantitative risk
484 assessment as does CARVER-SHOCK approaches and vulnerability analysis critical control
485 point (VACCP) and wider vulnerability assessment tools. This creates a challenge in that only
486 known and assessable threats can be prioritised in this way. Indeed the greatest flaw in these
487 approaches is the recognised hazard (threat), control measure (countermeasure) and then a
488 subjective scoring system to identify CCPs or CDPs. The weaknesses embedded in assessing
489 non-microbial food safety hazards via a HACCP, translates to TACCP in terms of what is
490 deemed an acceptable risk has both scientific, legal and moral aspects and thus is a relative
491 construct and not just a binary decision. However as Wiśniewska (2015) outlines the advantage
492 of using HACCP-based approaches to build food defence strategies is that they are familiar to

493 the food industry and thus are more easily adopted and integrated into existing systems and
494 practices. A concern that can be raised though, is that whilst a food safety HACCP plan is in
495 continuous use and this maintains familiarity with controls and preventive and corrective
496 actions, food defence issues occur much less frequently and this means that knowledge and
497 understanding of food defence strategies and how they are employed may be lost unless regular
498 refresher training is undertaken Further, given the very relative low probability of a deliberate
499 food defense event, some organisations may feel that the costs of implementing food defense
500 plans is disproportionate to the actual risk (Davidson et al. 2017). The risk assessment tools
501 (HACCP, TACCP< VACCP. HACCP-DP) considered here have limited value in terms of
502 unknown or unquantifiable threats creating then potential for vulnerabilities to be unrecognised
503 and this leads to the possibility that decision-makers may identify a subsequent incident as
504 being unforeseeable.

505 **3.2 Guardians and hurdles**

506 Appealing to criminology literature gives rise to specific terminology which those developing
507 food defence strategies meet to be conversant with. The crime triangle as explored by Spink et
508 al. (2016) includes consideration of the perpetrator, the victim and how opportunity for the
509 activity to take place is mediated by guardians and hurdles. The food defence team members
510 and the plan implementers roles are to be “guardians” i.e. the individuals operating at supply
511 chain or individual business or production line levels (Spink et al. 2015) that have the
512 knowledge, skills and understanding to develop and implement food defence strategies. The
513 visibility of food defence guardians acts as a deterrent (Reynald, 2009; Hollis & Willson, 2014;
514 Manning, Soon & Smith, 2019) and thus is essential to delivering effective food defence
515 strategies. However those designated as guardians need to understand their role and what is
516 expected of them so effective training is essential with refresher activities in the event that new
517 threats emerge. *Hurdles* are the formal system components that reduce opportunity for food

518 crime by either assisting detection or by acting as a deterrent (Spink et al. 2015; Manning, Soon
519 & Smith, 2019). Hurdles can be *physical hurdles* in terms of protecting structural assets
520 (barriers, enclosed production systems), or *artefact-based hurdles* such as procedures and
521 protocols or cyber-protection via firewalls and virus software. Thus the HACCP-DP plan will
522 signpost to relevant hurdles and guardians as well as defining countermeasures that are adopted
523 within food defense strategies to mitigate risk.

524 **3.3 Countermeasures**

525 *Countermeasures* are measures, often preventive in nature, are intended to
526 reduce criminal opportunity in food supply chains (Spink et al. 2015). Physical and technical
527 countermeasures such as physical hurdles are referred to as hard controls whereas managerial
528 controls (artefact based hurdles) are termed soft controls (van Ruth, Huisman & Luning, 2017).
529 Passive countermeasures are in operation at all times e.g. supplier assessment protocols
530 whereas reactive countermeasures are implemented should an incident occur in order to lessen
531 the impact once the threat is realised (Mitenus, Kennedy & Busta, 2014), for example product
532 recall strategies or product testing programmes as in the case of the 1080 incident in NZ.
533 Countermeasures for food defence are often the same global or specific protocols and policies
534 that have been developed as part of existing pre-requisite programmes such as good
535 manufacturing practice (GMP) or good hygienic practice (GHP).

536 With regard to cyber attacks specifically, organisations need to have a clear
537 defence strategy and will often need outside expertise to assist them to reduce vulnerability.
538 Bendovschi (2015) determines three kinds of countermeasure within a cybersecurity strategy:
539 preventive security controls that aim to prevent the realisation of a threat i.e. to restrict and
540 prevent unauthorised access to an organisation's network, programmes or data; detective
541 security controls that seek to detect information security threats e.g. intrusion detection systems
542 that monitors network traffic and potentially suspicious activity; corrective security controls

543 that are implemented if non-conformity is identified and implement business recovery
544 procedures after a cyber attack.

545 **4. Concluding thoughts**

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

562

563

- 565 AAP-06 (2014) North Atlantic Treaty Organisation (NATO) Glossary of Terms and
566 Definitions (English and French), Edition 2014. Available at:
567 http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf [Accessed on 15 December 2018]
568
- 569 Alias, M., Mohd Rasdi, R., Ismail, M., & Abu Samah, B. (2013). Predictors of workplace
570 deviant behaviour: HRD agenda for Malaysian support personnel. *European Journal of*
571 *Training and Development*, 37(2), 161-182.
572
- 573 Alvarez, M. J., Alvarez, A., De Maggio, M. C., Oses, A., Trombetta, M., & Setola, R. (2010,
574 March). Protecting the food supply chain from terrorist attack. In *International Conference*
575 *on Critical Infrastructure Protection* (pp. 157-167). Springer, Berlin, Heidelberg.
576
- 577 Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: The
578 role of organizational injustice. *Organizational behavior and human decision processes*,
579 89(1), 947-965.
580
- 581 Bandal, S., Singh, A., Mangal, M., Mangal, A.K., & Kumar, S. 2017. Food adulteration:
582 Sources, health risks, and detection methods, *Critical Reviews in Food Science and Nutrition*
583 57(6): 1174-1189. <http://dx.doi.org/10.1080/10408398.2014.967834>.
584
- 585 BBC (2018), Poisoned baby food: German jailed for attempted murder, Available at:
586 <https://www.bbc.co.uk/news/amp/world-europe-45951642> [Accessed 23 October 2018]
587
- 588 BBC (2016), New Zealand man jailed for milk formula 1080 threat, Available at:
589 <https://www.bbc.co.uk/news/world-asia-35878645> [Accessed 10th October 2018].
590
- 591 Bendovschi, A. (2015). Cyber-attacks—trends, patterns and security countermeasures.
592 *Procedia Economics and Finance*, 28, 24-31.
593
- 594 Bogadi, N. P., Banović, M., & Babić, I. (2016). Food defence system in food industry:
595 perspective of the EU countries. *Journal für Verbraucherschutz und Lebensmittelsicherheit*,
596 11(3), 217-226.
597
- 598 BRC (British Retail Consortium) (2018), Global Standard Food Safety. Issue 8 TSO Books
599 ISBN 9781784903343
600
- 601 Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of
602 the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*
603 8(1): 1-20
604
- 605 Budiono, G. L., & Sawitri, N. N. (2017). Strategic Business Espionage: An Ethics and
606 Business Practices to Gain Opportunity or Community Problems. *Studies in Business and*
607 *Economics*, 12(1), 29-39.
608
- 609 Burger, R. (2012). EHEC O104: H4 in Germany 2011: Large outbreak of bloody diarrhea and
610 haemolytic uraemic syndrome by shiga toxin-producing E. coli via contaminated food.
611 Improving Food Safety Through a One Health Approach: Workshop Summary. Institute of
612 Medicine (US). Washington (DC): National Academies Press (US); 2012.

613
614 Cohen, L. and Felson, M. (1979). Social change and crime rate trends: a routine activity
615 approach. *American Sociological Review* 44(4): 588-608
616
617 Collins Dictionary (nd), Saboteur – definition Available at:
618 <https://www.collinsdictionary.com/dictionary/english/saboteur> [Accessed 13 October 2018]
619
620 Cooney, T. P., Varelis, P., & Bendall, J. G. (2016). High-Throughput Quantification of
621 Monofluoroacetate (1080) in Milk as a Response to an Extortion Threat. *Journal of food*
622 *protection*, 79(2), 273-281.
623
624 Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes
625 industrial espionage. *Business Horizons*, 48(3), 233-240.
626
627 Crino, M. D. (1994). Employee sabotage: A random or preventable phenomenon?. *Journal of*
628 *Managerial Issues*, 311-330.
629
630 Dalziel, G.R. (2009), Food Defense Incidents 1950-2008: A chronology and analysis of
631 incidents involving the malicious contamination of the food supply chain. Report. Centre of
632 Excellence for National Security (CENS). S Rajaratnam School of International Studies,
633 Nanyang Technology University, Singapore.
634
635 Davidson, R. K., Antunes, W., Madslie, E. H., Belenguer, J., Gerevini, M., Torroba Perez,
636 T., & Prugger, R. 2017. From food defence to food supply chain integrity. *British Food*
637 *Journal*, 119(1), 52-66
638
639 Dawson, M. (2018). A Brief Review of New Threats and Countermeasures in Digital Crime
640 and Cyber Terrorism. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and*
641 *Applications* (pp. 173-180). IGI Global.
642
643 Detica (2011). The Cost of Cyber Crime. A Detica report in partnership with the Office of
644 Cyber Security and Information Assurance in the Cabinet Office. Detica Ltd. Guildford
645 Surrey.
646
647 Douthit III, H. L. (1987). *The Use and Effectiveness of Sabotage as a Means of*
648 *Unconventional Warfare-An Historical Perspective from World War I through Viet Nam* (No.
649 AFIT/GLM/LSMA/87S-20). AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB
650 OH SCHOOL OF SYSTEMS AND LOGISTICS.
651
652 Elad, D. (2005). Risk assessment of malicious biocontamination of food. *Journal of food*
653 *protection*, 68(6), 1302-1305.
654
655 EUROPOL (2017) European Union Terrorism Situation and Trend Report 2017. Available
656 at: https://www.europol.europa.eu/sites/default/files/documents/tesat2017_0.pdf [Accessed
657 10 October 2018]
658
659 Fan, C., Jun, B. H., & Wolfstetter, E. G. (2016). To spy or not to (fire the) spy: Impact and
660 stability of spying out rivals' play in Bertrand competition. Discussion Paper. Series No.
661 1609. December 2016
662

663 FDA (2018a) Mitigation Strategies to Protect Food Against Intentional Adulteration:
664 Guidance for Industry. U.S. Department of Health and Human Services Food and Drug
665 Administration Center for Food Safety and Applied Nutrition June 2018. Available at:
666 [https://www.fda.gov/downloads/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryI](https://www.fda.gov/downloads/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryInformation/UCM611043.pdf)
667 [nformation/UCM611043.pdf](https://www.fda.gov/downloads/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryInformation/UCM611043.pdf) [Accessed 15 December 2018]
668
669 FDA (2018b), Food defense, Available at:
670 <https://www.fda.gov/Food/FoodDefense/default.htm> [Accessed 21 September 2018]
671
672 Fisher, D. (1989) New cases of tainted baby food plague Britons. Available at:
673 http://articles.latimes.com/1989-04-28/news/mn-1925_1_baby-food-new-cases-heinz-baby
674 [Accessed 19 October 2018]
675
676 Fortune, R. (1852). *A Journey to the Tea Countries of China Including Sung-Lo and the*
677 *Bohea Hills; with a Short Notice of the East India Company's Tea Plantations in the*
678 *Himalaya Mountains: By Robert Fortune. With Map and Illustrations.* John Murray.
679
680 Fredrickson, N.R. (2014) Food Security: Food Defense and Biosecurity, *Encyclopedia of*
681 *Agriculture and Food Systems*, 3, 311-323
682
683 GFSI (2017) (Global Food Safety Initiative). GFSI Benchmarking requirements version 7.2
684 Available from: [https://www.mygfsi.com/certification/benchmarking/gfsi-guidance-](https://www.mygfsi.com/certification/benchmarking/gfsi-guidance-document.html)
685 [document.html](https://www.mygfsi.com/certification/benchmarking/gfsi-guidance-document.html) [Accessed 15 December 2018]
686
687 GFSI. (2014). (Global Food Safety Initiative). GFSI Position on mitigating the public health
688 risk of food fraud July 2014. Available from: [http://www.mygfsi.com/news-](http://www.mygfsi.com/news-resources/news/295-gfsi-position-paper-on-mitigating-the-public-health-risk-of-food-fraud.html)
689 [resources/news/295-gfsi-position-paper-on-](http://www.mygfsi.com/news-resources/news/295-gfsi-position-paper-on-mitigating-the-public-health-risk-of-food-fraud.html)
690 [mitigating-the-public-health-risk-of-food-](http://www.mygfsi.com/news-resources/news/295-gfsi-position-paper-on-mitigating-the-public-health-risk-of-food-fraud.html)
691 [fraud.html](http://www.mygfsi.com/news-resources/news/295-gfsi-position-paper-on-mitigating-the-public-health-risk-of-food-fraud.html). [Accessed 4 October 2018].
692
693 Gross, G (2012) Two Romainians plead guilty to Subway hack, Available at:
694 [https://www.computerworld.com/article/2492641/cybercrime-hacking/two-romanians-plead-](https://www.computerworld.com/article/2492641/cybercrime-hacking/two-romanians-plead-guilty-in-subway-hack.html)
695 [guilty-in-subway-hack.html](https://www.computerworld.com/article/2492641/cybercrime-hacking/two-romanians-plead-guilty-in-subway-hack.html) [Accessed 23 October 2018]
696
697 Hirschauer, N. and Zwoell, S. (2008). Understanding and managing behavioural risks: the case
698 of malpractice in poultry production. *European Journal of Law and Economics* 26: 27-60
699
700 Hirschi, T. (1969). *Causes of delinquency.* Berkeley: University of California Press.
701
702 Hollis, M.E. & Wilson, J.M. (2014). Who are the guardians in product counterfeiting? A
703 theoretical application of routine activities theory. *Crime Prevention and Community Safety*,
704 16(3): 169-188.
705
706 ISO 27001:2013. Information technology – security techniques Information Security
707 Management Systems – Requirements. Available at:
708 <https://www.iso.org/standard/54534.html>
709
710 ISO 28000: 2007. Specification for security management systems for the supply chain.
711 Available at: <https://www.iso.org/standard/44641.html>

712 Koc, M., Jernigan, C., & Das, R. (2007). Food security and food sovereignty in Iraq: The
713 impact of war and sanctions on the civilian population. *Food, Culture & Society*, 10(2), 317-
714 348.

715

716 Kowalska, A., Soon, J.M., & Manning, L. (2018), A study on adulteration in cereals and
717 bakery products from Poland including a review of definitions *Food Control*, 92, 348-356
718

719 Kreft, H., & Crowson, I. (2018), Kerry Foods statement: ‘No evidence’ terror plotter
720 poisoned ready meal sauces in Burton factory, Staffordshire Live, Available at:
721 [https://www.staffordshire-live.co.uk/news/burton-news/kerry-foods-statement-no-evidence-](https://www.staffordshire-live.co.uk/news/burton-news/kerry-foods-statement-no-evidence-1033646)
722 [1033646](https://www.staffordshire-live.co.uk/news/burton-news/kerry-foods-statement-no-evidence-1033646) [Accessed 10 October 2018]
723

724 Krischer, M. M., Penney, L. M., & Hunter, E. M. (2010). Can counterproductive work
725 behaviors be productive? CWB as emotion-focused coping. *Journal of occupational health*
726 *psychology*, 15(2), 154.
727

728 Khursheed, A., Kumar, M., & Sharma, M. (2016) Security Against Cyber Attacks in Food
729 Industry. *International Journal of Control Theory and Applications*, 9(17) 2016, pp. 8623-
730 8628
731

732 Licea, M. (2017), Man charged with poisoning baby food in extortion plot. Available at:
733 <https://nypost.com/2017/09/30/man-charged-with-poisoning-baby-food-in-extortion-plot/>
734 [Accessed 18 October 2018]
735

736 Lord, J. (2015). Undercover under threat: Cover identity, clandestine activity, and covert
737 action in the digital age. *International Journal of Intelligence and Counterintelligence*, 28(4),
738 666-691.
739

740 Manhire, T. (2015) New Zealand prime minister says poison threat to milk powder
741 ‘ecoterrorism’. The Guardian 10th March 2015. Available at:
742 [https://www.theguardian.com/world/2015/mar/10/new-zealand-prime-minister-poison-threat-](https://www.theguardian.com/world/2015/mar/10/new-zealand-prime-minister-poison-threat-milk-powder-ecoterrorism)
743 [milk-powder-ecoterrorism](https://www.theguardian.com/world/2015/mar/10/new-zealand-prime-minister-poison-threat-milk-powder-ecoterrorism) [Accessed 11 October 2018]
744

745 Manning, L., & Soon, J. M. (2016). Food safety, food fraud, and food defense: a fast
746 evolving literature. *Journal of food science*, 81(4), R823-R834.
747

748 Manning, L & Soon, J.M, (2014). Developing systems to control food adulteration, *Food*
749 *Policy*, 49(1), 23-32
750

751 Manning, L., Baines, R. N., & Chadd, S. A. (2005). Deliberate contamination of the food
752 supply chain. *British Food Journal*, 107(4), 225-245.
753

754 McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key*
755 *findings and implications. Home Office Research report*, 75. Chapter 1 Cyber- dependent
756 crimes. Available at: <http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf>
757 [Accessed 23 October 2018]
758

759 McGuire, M. (2012). *Organised Crime in the Digital Age*. London: John Grieve Centre for
760 Policing and Security.
761

762 McIntyre, L., & Monaghan, J. (2016). Microbiological Outbreak in Sprouted Seeds. In
763 *Foodborne Diseases* (pp. 50-75). CRC Press.
764

765 Meulenbelt, S. (2018). Assessing chemical, biological, radiological and nuclear threats to the
766 food supply chain. *Global Security: Health, Science and Policy*, 3(1), 14-27.
767

768 Mitenius, N, Kennedy SP, & Busta FF. (2014). Chapter 35— Food defense, food safety
769 management: a practical guide for the food industry. In: Motarjemi Y, & Lelieveld H, editors.
770 1st Edition Academic Press, Elsevier ISBN 9780123815040. p 937–58.
771

772 Mohammed, D. (2017). US Healthcare Industry: Cybersecurity Regulatory and Compliance
773 Issues. *Journal of Research in Business, Economics and Management*, 9(5), 1771-1776.
774

775 Monke, J. (2007). Agroterrorism: Threats and preparedness. Library of Congress
776 Washington DC CONGRESSIONAL RESEARCH SERVICE. March 12. 2007

777 Nestle, M. (2003), *Safe Food: Bacteria, Biotechnology and Bioterrorism*, University of
778 California Press Ltd, London.

779 Neethirajan, S., Ragavan, K. V., & Weng, X. (2018). Agro-defense: Biosensors for food from
780 healthy crops and animals. *Trends in Food Science & Technology*, 73, 25-44

781 NZHerald (2017), 1080 blackmailer Jeremy Kerr jailed for eight and a half years. Available
782 at: https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11610428 [Accessed
783 16 October 2018]

784 O'Halloran, S. (2014) DuPont industrial espionage case ends with convictions. Food Eng.
785 Available at: [http://www.foodengineeringmag.com/articles/92018-dupont-industrial-
786 espionage-case-endswith-convictions](http://www.foodengineeringmag.com/articles/92018-dupont-industrial-espionage-case-endswith-convictions). [Accessed 18 October 2018]
787

788 Olson D. (2012), *Agroterrorism Threats to America's Economy and Food Supply*, "FBI Law
789 Enforcement Bulletin" February 2012.
790

791 PAS 96. (2017) *Guide to protecting and defending food and drink from deliberate attack*.
792 BSI, London
793

794 Pease, K. (2006). Rational choice theory. In, McLaughlin, E. and Muncie, J. (eds.). *The Sage
795 Dictionary of Criminology*. London: Sage.
796

797 Reynald, D. M. (2009). Guardianship in action: Developing a new tool for measurement.
798 *Crime Prevention and Community Safety*, 1(1), 1-20.
799

800 RKI (Robert Koch Institute). (2012). EHEC O104:H4 Outbreak in Germany, 2011 Available
801 at:
802 [https://www.rki.de/EN/Content/infections/epidemiology/outbreaks/EHEC_O104/ehec_O104
803 _inhalt_en.html](https://www.rki.de/EN/Content/infections/epidemiology/outbreaks/EHEC_O104/ehec_O104_inhalt_en.html) [Accessed 13 October 2018]
804

805 Rojas, N. (2017) Man puts lethal poison into baby food to blackmail supermarkets in €10
806 million extortion plot. Available at: [https://www.ibtimes.co.uk/man-puts-lethal-poison-into-
807 baby-food-blackmail-supermarkets-10m-extortion-plot-1641233](https://www.ibtimes.co.uk/man-puts-lethal-poison-into-baby-food-blackmail-supermarkets-10m-extortion-plot-1641233) [Accessed 13 October 2018]

808
809 Sigley, G. (2015). Tea and China's rise: tea, nationalism and culture in the 21st century.
810 *International Communication of Chinese Culture*, 2(3), 319-341.
811
812 Smith, L. (2016) , £2 million blackmail plotter claimed he had laced supermarket food with
813 cyanide. Available at: [https://www.mirror.co.uk/news/trials/2million-blackmail-plotter-](https://www.mirror.co.uk/news/trials/2million-blackmail-plotter-claimed-laced-8751269)
814 [claimed-laced-8751269](https://www.mirror.co.uk/news/trials/2million-blackmail-plotter-claimed-laced-8751269) [Accessed 16 October 2018]
815
816 Soon, J.M., Manning, L. & Smith, R. (2019) Advancing understanding of pinchpoints and
817 crime prevention in the food supply chain, *Crime Prevention and Community Safety*, 21(1)

818 Spector, P. E., & Fox, S. (2005). The stressor– emotion model of counterproductive work
819 behaviour. In S. Fox & P. Spector (Eds.), *Counterproductive work behavior: Investigations*
820 *of actors and targets* (pp. 151–174). Washington, DC: American Psychological Association.
821
822 Spink, J., Moyer, D. C., & Rip, M. R. (2016). Addressing the risk of product fraud: a case
823 study of the Nigerian combating counterfeiting and sub-standard medicines initiatives.
824 *Journal of Forensic Science & Criminology*, 4(2), 1-13.
825
826 Spink, J., Moyer, D.C. Park, H. Wu, Y. Fersht, V. Shao, B., Hong, M., Paek, S.Y., & Edelev,
827 D. (2015), Introduction to Food Fraud including translation and interpretation to Russian,
828 Korean and Chinese languages. *Food Chemistry*. 189: 102-107.
829
830 Spink, J., Moyer, D.C, Park, H. & Heinonen, J.A (2013), Defining the types of counterfeiters,
831 counterfeiting and offender organizations, *Crime Science*, 2:8
832
833 Spink, J. & Moyer, D.C. (2011a). Backgrounder: Defining the Public Health Threat of Food
834 Fraud, in Research Grants, National Center for Food Protection and Defense (NCFPD),
835 Minneapolis, MN, p. 7, Available from: www.ncfpd.umn.edu (Accessed 4 October 2018).
836
837 Spink, J., & Moyer, D. C. (2011b). Defining the public health threat of food fraud. *Journal of*
838 *Food Science*, 76(9), R157-R163.
839
840 Stones, M. (2018), Kerry worker convicted of terrorism 'posed risk to factory' *Food*
841 *Manufacture* 10th January 2018 Available at:
842 [https://www.foodmanufacture.co.uk/Article/2018/01/10/Kerry-worker-convicted-of-terror-](https://www.foodmanufacture.co.uk/Article/2018/01/10/Kerry-worker-convicted-of-terror-offences-threatened-factory)
843 [offences-threatened-factory](https://www.foodmanufacture.co.uk/Article/2018/01/10/Kerry-worker-convicted-of-terror-offences-threatened-factory)
844
845 Taylor, L. & Walton, P. (1971). Industrial sabotage: motives and meanings. In S. Cohen, (ed.)
846 *Images of Deviance*, pp.219-45 Harmondsworth: Penguin
847
848 The Independent (1999), Food Scare Scandals Available at:
849 <https://www.independent.co.uk/news/food-scare-scandals-1100385.html> [Accessed 12
850 October 2018]
851
852 Török, T.J., Tauxe, R.V., Wise, R.P., Livengood, J.R., Sokolow, R., Mauvais, S., Birkness,
853 K.A., Skeels, M.R., Horan, J.M., & Foster, L.R., 1997. A large community outbreak of
854 salmonellosis caused by intentional contamination of restaurant salad bars. *JAMA* 278 (5),
855 389–395.
856

857
858 UK Cyber Security Breaches Survey (2018). Available at:
859 <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018> [Accessed 23
860 October 2018]
861
862 US Code Title 22 Chapter 38 2656f – Annual country reports on terrorism Available at:
863 <https://www.law.cornell.edu/uscode/text/22/2656f> [Accessed 15 December 2018]
864
865
866 US Federal Food, Drug and Cosmetic Act. Section 342. Available at:
867 <https://www.law.cornell.edu/uscode/text/21/342> [Accessed 15 December 2018]
868
869 Van Arnam, R. C. (2001). Business war: Economic espionage in the United States and the
870 European Union and the need for greater trade secret protection. *NCJ Int'l L. & Com. Reg.*,
871 27, 95.
872
873 Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African*
874 *Journal of Information and Communication (AJIC)*, 20, 113-132.
875
876 van Ruth, S.M., Huisman, W. & Luning, P.A., (2017). Food fraud vulnerability and its key
877 factors. *Trends in Food Science & Technology*, 67, pp.70-75.
878
879 Vidalis, S., & Angelopoulou, O. (2014). Assessing identity theft in the Internet of Things.
880 *Journal of IT Convergence Practice*. 2(10), 15-21
881
882 Walklate, S. (2007). *Understanding criminology*. Buckingham: Open University Press.
883
884 Wiśniewska, M. Z. (2015). HACCP-based food defense systems. *Journal of Management and*
885 *Finance*, 13, 106-119.
886
887 World Health Organization (2002). *Terrorist threats to food: guidance for establishing and*
888 *strengthening prevention and response systems*. Food Safety Programme. World Health
889 Organization. ISBN 9241545844
890
891 Yoe, C. & Schwartz J.G. (2010), *Incorporating Defense into HACCP*, “Food Safety
892 Magazine” August/September 2010 Available at:
893 [https://www.foodsafetymagazine.com/magazine-archive1/augustseptember-](https://www.foodsafetymagazine.com/magazine-archive1/augustseptember-2010/incorporating-defense-into-haccp/)
894 [2010/incorporating-defense-into-haccp/](https://www.foodsafetymagazine.com/magazine-archive1/augustseptember-2010/incorporating-defense-into-haccp/) [Accessed on 10th October 2018]
895
896
897

898 **Table 1 Examples of Intentional Food Supply Chain Contamination 1950-2008 (Adapted**
 899 **from Dalziel, 2009)**
 900

Stage of supply chain	Total confirmed cases	Agents used	Fatalities	Injuries	Notes
Water Supply	7	Pesticide, Insecticide, Cyanide, Sheep dip, VX, Sarin	3	<100	Multiple additional unconfirmed incidents
Pre-harvest	365	Glyphosate, plant toxin, cyanide, cattle feed as a vehicle, rodenticide	0	0	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.
Post harvest, and manufacturing	3	Mercury, glass, needles, rat poison	0	125	Numerous unconfirmed incidents
Retail and food service	89	Acetone, Arsenic, Atropine, Cyanide, Herbicide, Insecticide, Pesticide, Physical contaminants incl. rodenticide, Rohypnol, Salmonella Typhimurium, Thallium	123	3394	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
Consumer/Home	265	Multiple	265	670	Many cases were intentional homicide focused on specific individuals (victims) often family members.

901

902 **Table 2. Examples of questionable espionage tactics (Adapted from Crane, 2005)**

903

Questionable tactics
Breaking and entering into a competitor's premises to steal information or installing recording devices.
Contacting competitors with fake identity such as a potential customer or supplier
Covert surveillance through spy cameras.
Hiring private detectives to track competitor's staff.
Infiltrating competitor organisations with industrial spies.
Interviewing competitors' employees for a bogus job vacancy.
Pressuring the customers or suppliers of competitors to reveal sensitive information about their operations.
Searching through a competitor's rubbish.

904

905 **Table 3. Types of cyber attack (Adapted from Detica, 2011; McGuire and Dowling, 2013; Bendovschi, 2015; Khursheed, Kuma &**
 906 **Sharma, 2016; Van Niekerk, 2017)**
 907

Type of attack	Security risk
Brute force attack describes repeated attempts to gain access to protected information (e.g. passwords, encryption, etc.) until the correct key is found, and security is breached. Social engineering is the general term that describes techniques used to gain unauthorised access to information through human interaction	This type of attack allows unauthorised access to sensitive information.
Data corruption to cause disruption to services and activities	Data could be corrupted or lost.
Data exposure often in an attempt to show unethical behaviour or conduct	This type of attack has seen information being published by Wikileaks and others
Defacement of websites often with political or ideological slogans	Websites can be defaced with political and ideological slogans or legitimate links might be redirected to pornographic websites e.g. the 1996 attack on the US Department of Justice homepage.
Distributed Denial of Service (DDoS) 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	DDos attacks on Estonia (2007) and Myanmar (2010) caused significant disruption with Myanmar cut off from the Internet for more than 10 days.
Financial attack to steal money from accounts or fraudulent emails or links to fake tax revenue forms	In 2012, Subway’s credit-card payment terminals were attacked with more than 146,000 compromised cards and more than \$10 million in losses
Malware is a generic term describing types of malicious software. Examples of malware are: viruses, worms, trojans, spyware, ransomware, adware and scareware/rogware.	Malware is used by the attacker to compromise the confidentiality, availability and integrity of data. <i>Spyware</i> is software that invades users’ privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited [that] may then be transmitted to third parties (McGuire and Dowling, 2013:5)
Man in the middle (MitM) attack 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.	This type of attack allows not only access to unauthorised access to sensitive information, but also the opportunity to alter the information/ message between sending and receipt.
Phishing is a technique that aims to steal confidential information from users by masquerading as a trusted source (e.g. website)	An example would be the sending of bogus money transfer requests or emails targeted at individuals – “spoofing” i.e. misleading individuals into entering details into a counterfeit website; “pharming” redirecting website traffic from a legitimate to a fraudulent website. Botnets are clusters of computers that send out spam, phishing emails automatically after being infected by malicious software.
Scareware 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	. The software may be ineffective or partially effective before infecting the computer with its own viruses. The attackers may request payment to clean up the computer.
System penetration to steal information or other espionage activities	The US supermarket Target was attacked over the Thanksgiving season where 40 million credit and debit card data was stolen

908
909

Table 4: Typology of cyber criminals (Adapted from McGuire, 2012; Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014).

Sub-group	Sub-type	Description
Type 1 – online offending	Swarms	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.
	Hubs	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
Type 2 – Hybrids with online and offline offending	Clustered hybrid	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.
	Extended hybrid	Not as centralised as a clustered hybrid. More subgroups and associates but still with a level of coordination
Type 3 – Mainly offline but undertake some activity online	Hierarchies	Traditional criminal groups who transpose some activities online e.g. increasing scope of extortion activities.
	Aggregate groups	Loosely organised, temporary groups with opaque purpose that use digital technology in a disorganised way to support other activities

910
911