Agent selection and threat actualization in contamination cases:

Predicting action from perpetrator behavior

Sarah C. Kilbane

Centre for Criminology, University of Greenwich, London, UK

Abstract

While existing research on the topic is sparse, previous works have shown that there is believed to be a substantial threat of intentional, malicious contamination of the supply chain by criminals and terrorists (CFSAN, 2001; WHO, 2008). Genuine contamination incidents have the potential to result in mass casualties, although empty threats are often enough to generate public fear and lead to considerable economic damage. While empty threats often appear indistinguishable from those which will result in contamination, it is thought that certain variables identified in perpetrator communications may be able to help separate empty threats from those which will be actualized. This research thus attempts to determine whether a perpetrator's reported choice of agent could offer functional predictions for the likelihood of actual contamination in future incidents. Findings indicate that chemical agents alone are more likely to be associated with genuine contamination, while the claimed use of biological agents alone as well as chemical, biological and radionuclear (CBRN) agents combined are more often associated with empty threats. The utility of these findings will be discussed, as well as suggestions for future research.

Keywords: contamination; product tampering; threat actualization; CBRN; Bayes' Theorem

Introduction

Over the past 20 years, a number of studies have identified the potential severity of outcomes in cases of product contamination, and for food and water contamination in particular (e.g., Center for Food Safety and Applied Nutrition [CFSAN], 2001; Sobel, Khan & Swerdlow, 2002; World Health Organization [WHO], 2008), with the probability of a malicious contamination event with at least 5,000 casualties estimated at between 10% and 30% in a given year, and thought to be increasing each year (Mohtadi & Murshid, 2009). Due to the diversity of products which can be targeted through contamination, as well as the globalization of the market, food is considered to be one of the most susceptible means available for those who wish to harm a great number of individuals (WHO, 2008) as this method of transmission has an effect on the entire population (Stinson, Kinsey, Degeneffe, & Ghosh, 2007).

In the event of a food terrorism incident, a widespread operation would not be necessary, as targeting only a few specific products or individuals would still likely result in the desired consequence of mass public fear and anxiety (WHO, 2008) as well as have substantial economic implications (Khan, Swerdlow, & Juranek, 2001). In addition, for attacks using chemical and biological weapons, the resulting publicity for those responsible or for their cause could be considered a "very compelling incentive" for terrorist organizations (Cornish, 2007, p.7). According to the WHO (2008), the effects of food terrorism can include impacts on public health services, the economy and trade, social and political implications, as well as disease and death. Additionally, an attack against the food supply of the US, or any other industrialized nation, could also distract the military from other potential threats (CFSAN, 2001), and public anxiety could also reduce trust in government, thus having a ripple effect on political stability (WHO, 2008). Finally, the psychological effects on the public can be severe in attacks involving chemical, biological,

and radionuclear agents, as following the 1995 sarin gas attacks in the Tokyo subway, more than 5000 individuals were found to have physical symptoms without any exposure to the sarin gas (Lemyre et al., 2005).

However, physical harm to consumers as a result of actual product contamination may not always be required – or even desired – to attain terrorist or criminal goals. In many instances threats and hoaxes involving the contamination of consumer products can be seen to achieve desired outcomes, with common motives including financial gain by conning the targeted company or the desire for personal or political attention (Logan, 1993). Additionally, extortion attempts do not necessarily require actual contamination to have taken place, but only a threat substantial enough to make consumers, and thus the victimized company, take notice (Cremin, 2001). Therefore, depending on the final goal of the individual or organization, the decision to use an empty threat may be a more rational choice than the actual contamination of a product, as the same outcome can be achieved with seemingly no technical skill, knowledge of or access to any contaminating agents. Indeed, it has been suggested that even the implication that chemical or biological agents have been used against the food supply could create havoc (Mohtadi & Murshid, 2009).

While physical harm is no longer a concern in cases of empty threats, affected companies may deal with a number of financial issues including the loss of consumer confidence and long-term damage to the brand (Cremin, 2001; Dalziel, 2009), as well as the cost of a recall if the threat is assumed to be a case of genuine contamination (Morgan, 1988). Indeed, when considering potable water sources as an example, even a threat of contamination could lead to as serious an incident as a genuine terrorist attack (Gleick, 2006). One particular contamination hoax involving the claimed adulteration of Mars Bars by animal rights activists in 1984 cost roughly £6 million for the company (Monaghan, 2000). Beyond economics and as with actual contamination incidents, empty threats using consumer products can cause widespread public fear, and may even lead to changes in consumer purchasing behavior (e.g., Mitchell, 1989; Yeung & Morris, 2001).

Therefore, both actual contamination incidents and empty threats present considerable challenges to law enforcement and targeted companies. Ideally, whether or not a product has been (or will be) genuinely contaminated should determine the response in such cases, as the ultimate outcome will dictate, for instance, whether a costly product recall should be issued. However, it is often the case that terrorist threats will need to be considered as legitimate precursors to action until proven otherwise, due to the potential high cost of incorrectly treating a genuine attack as innocuous (Tishler, 2016). The same can be said to be true for criminal attacks against the supply chain. This strategy, however, is not without its own risks. Of note here is the Chilean grape scare of 1989, in which grapes imported to the US and other countries were thought to be contaminated with cyanide. After initial tests showing small traces of cyanide, the US banned these grapes, with Chile reportedly losing $330 million as a result (Dalziel, 2009). However, further tests revealed no conclusive evidence of cyanide contamination, and so this case offers a clear example of how the economic damage from a case wrongly assessed as a genuine risk could be just as, if not more damaging than, an actual attack (Dalziel, 2009).

It is then crucial to be able to identify which cases are likely to result in genuine physical contamination, and which cases are likely to remain empty threats. As one of the requirements of such a threats is the need for attention (because the threat will not serve its function if no one is watching), and as the perpetrators of genuine contamination incidents will often benefit from public knowledge of their crime as well, it is important to consider what information can be taken from communications which are claimed to come from the perpetrator during such incidents.

Assessing Threats

As mentioned previously, there are many instances in which a perpetrator engaging in product contamination may make the choice to use an empty threat, and differentiating between cases that will progress to violence from those that will not is incredibly difficult. One method which may help in differentiating between an individual thinking about an action from someone actually intending on carrying out that behavior is to examine perpetrator implementation intentions. Implementation intentions offer specific detail on the when, where, and how someone will meet their intended goals (Sooniste, Granhag, Stromwall, & Vrij, 2014). As implementation intentions go beyond what a person *wants* to achieve and instead focuses on the *behaviors* needed to reach their goal, an individual who does not actually intend to follow through with an action will be unlikely to give appropriate detail on how the act would be carried out, thus failing to form true implementation intention (Sheeran, Milne, Webb, & Gollwitzer, 2005). Sooniste and colleagues (2014) found that participants telling the truth about an innocuous task were more concerned with explaining procedural details (i.e., the *how* of the act) in comparison to participants covering up ulterior criminal intentions ('liars'), who were more concerned about the reasoning behind the task (i.e., the *why* of the act). This may be due to the preoccupation on the part of the liars with convincing the target about their desire and intent to follow through with their stated actions (Sooniste et al., 2014).

Applying this research to contamination incidents, it is believed that those offering threats that will not progress to violence would provide communication lacking in methodological detail due to the fact that they do not actually intend to carry out the stated action. This could extend to a number of key pieces of information pertaining to *how* the act would be carried out, possibly including the location, the method of contamination, and the contaminating agent itself. This is not to say that threateners would not form implementation intentions at all, but rather that statements would be focused on covering up their lies rather than how the stated act would be carried out (Sooniste et al., 2014). However, it is worth emphasizing here that the 'truth-tellers' in the Sooniste

et al. (2014) study engaged in a non-criminal activity, which differs from the current study in which all individuals have taken part in some malicious act, even if just issuing an empty threat (Geurts, Granhag, Ask, & Vrij, 2016).

Following on from the previous work, Geurts and colleagues conducted an experiment involving the issuing of threats against a fictitious company. In their study the authors differentiate between *actualizers*, being defined as providing "a stated intention to cause harm that the threatener genuinely intends to carry out", and *bluffers,* who offer "a stated intention to cause harm that the threatener does not intend to carry out" (2016, p.53). In contrast to previous findings about implementation intentions, Geurts et al. (2016) found that bluffers tended to provide more details than actualizers when it came to the *how* of the act. In addition, bluffers revealed more *how* information when challenged about their threat, perhaps due to concern that their threat was not being taken seriously (Geurts et al., 2016). What may be crucial with these results is not what is possible for the perpetrator to say, but what is best for them to say, indicating that careful calculation may be used when delivering threats (Geurts et al., 2016). If this were to be true for those engaging in contamination threats, it would be expected that perpetrators might offer more *how* detail in an attempt to make their threat more believable. While the Geurts et al. (2016) study may offer a closer approximation to contamination cases as all participants issued threats with the potential to be criminal given the circumstances, it is not clear whether an experimental study using a student sample can be fully generalized to the current sample of actual crimes.

A threatening communication which is sent by the perpetrator claiming past or future product contamination may contain both *why* and *how* information. As questions have been raised from previous research of whether detailed *how* information is more likely to be indicative of bluffers or 'truth-tellers', this information will be given primary attention. In particular, the agent chosen by the perpetrator (i.e., their weapon) will be the focus of the

current analysis, as this piece of *how* information is frequently reported in the media and other available sources on contamination threats, and may tell a great deal about the perpetrator (e.g., their potential access to such agents) as well as their desired outcome. According to Jackson and Frelinger (2008, p.2), a perpetrator's weapon of choice implies "the scale and scope of their violence", and weapon choice has also been identified as important in understanding a perpetrator's apparent intended lethality (Wilson & Lemanski, 2013). In regard to chemical, biological and radiological weapons, the type of agent chosen may be indicative of factors such as the size of the chemical or biological industry in the country of attack or the perpetrator's religious ideology, although there may also be differences based on whether these incidents are empty threats or actual attacks (Tishler, 2013). Indeed, previous research on product contamination has revealed that different agents may be used in threats and authentic attacks, as those agents which are easiest to obtain, such as household poisons (Dalziel, 2009) and foreign objects (Graves, Smith & Batchelor, 1998), are most frequently used in attacks on the food supply, while more concerning and difficult to obtain biological agents may be more likely to be used in threats alone (Wilson & Kilbane, 2017). Additionally, it has been noted that the unease around biological agents could mean that they are important tools to use during threats (Cornish, 2007). However, before proceeding it is first necessary to determine how these particularly dangerous agents may be classified as such.

Identifying Agents of Concern

During contamination incidents there are typically four general categories of agent used; biological agents (e.g., bacteria, toxins, viruses and parasites), chemical agents (e.g., pesticides and heavy metals), radiological agents (e.g., polonium), and physical agents (e.g., glass, pieces of metal) (CFSAN, 2001). Agents that are easily dispersed, are very likely to cause serious illness or death, and require vigilance from public health organizations are often identified as being the most concerning, and include botulism and anthrax toxins (Sobel et al., 2002). However, the list of particularly concerning agents can be quite long depending on the source of this information, and even easily

obtained chemicals such as lead, mercury, and pesticides have been identified by the US Centers for Disease Control and Prevention (CDC) as agents which could be used by terrorists to attack the food supply (CFSAN, 2003). It is thus initially quite difficult to decide which agents should be given the most serious attention without additional details concerning the target chosen, the mode of transmission, and other situational variables.

However, if empty threats are to capitalize on public fear, as would certainly be the case with food and water terrorism, then it is not only the attitudes of public health officials and law enforcement which are important, but also which agents may be *perceived* as concerning to the general public. Such agents that have the greatest capacity to induce fear may fall under the category of CBRN, or 'chemical, biological, and radionuclear' agents. This term is most often used in the context of CBRN terrorism, with these likely to be the agents used should there be an attack on the food supply chain (Mohtadi & Murshid, 2009). Despite the fact that very few deaths have resulted from CBRN terrorism in the past (Ivanova & Sandler, 2007), several authors have noted the public fear which is likely to accompany the use of such agents. For instance, Cornish (2007, p.3) notes that if a CBRN attack was to take place in the UK, the effects could be partly 'self-inflicted' by the public, business and government officials, or even made worse by the media due to the panic that the use of such agents may foster. Indeed, CBRN agents have been described as "weapons of terror", the use of which would be likely to result in anxiety on both an individual and communal level, caused by the uncertainty concerning the given agent's effects on the population (Palmer, 2004, p.3).

Despite the fact that CBRN attacks have been a regular topic of discussion in recent years, it is still difficult to identify a clear and accessible definition for this term. The need for such a clear definition is also echoed by Plamboeck et al., who note that a vast number of substances can be classified as CBRN (2016). For Plamboeck and colleagues, in the case of

chemicals this should exclude drugs, explosives and household chemicals, but does include chemical warfare agents (CWA) and toxic industrial chemicals (TIC). Therefore, and despite what its acronym implies, not all chemicals would be considered as CBRN agents. Additionally, many agents, and especially those which are radiological or chemical such as ammonia, chlorine, sulfur or formaldehyde, may have multiple legitimate uses in certain industries (Cornish, 2007), and so scenarios exist in which specific CBRN agents from each of these categories may be obtained relatively easily.

Cornish (2007) offers even more detail on what agents may be considered CBRN by outlining a number of different chemical weapon categories (i.e., nerve agents, blood agents, blister agents, choking agents, vomiting agents, incapacitants and irritants) as well as the three category system (A, B and C) used by the US CDC to identify biological weapons. In these three categories those of greatest concern fall within Category A, those which are expected to result in fewer illnesses and deaths are in Category B, and those which are not thought to present a high risk are in Category C (Rotz, Khan, Lillibridge, Ostroff, & Hughes, 2002). While such classifications do make it easier to identify agents of particular concern, the CDC's Category B includes as bioterrorism agents 'food-borne agents', which is again a relatively indistinct category, making it difficult to identify those biological threats to food which are of the greatest concern to public health, and to differentiate between intentional and unintentional contamination. Cornish (2007) also identifies that uranium-235 and plutonium-239 are of the highest concern when it comes to radiological agents, although other radiological agents which may be used in terrorist incidents are mentioned by the author as well. While there is no definitive list of what constitutes a CBRN agent, the agents mentioned in Cornish (2007) offer a good starting point to work from.

As can be seen, the term 'CBRN' has often been defined in vague terms, but has generally been used as a stand-in for concerning and dangerous contaminating agents. For this paper then, a specific definition of 'CBRN' agents is proposed in an attempt to identify those agents in this sample

likely to both (a) cause the most fear among would-be targets and victims, and (b) have the potential for causing a great deal of physical harm. In order to identify particularly concerning chemical agents, Schedules 1, 2 and 3 of toxic chemicals and their precursors from the Chemical Weapons Convention (CWC) from the Organisation for the Prohibition of Chemical Weapons is used. The CWC Schedules have been consulted due to a lack of specific chemical components listed in Cornish (2007). However, as with Cornish (2007), the 'biological' component can be fulfilled by any agent considered to be a bioterrorism agent by the US CDC. Finally, an item is considered to be in the 'radionuclear' category if it is a radioactive element. Thus 'CBRN' is used here as an exclusionary category, containing only specific and particularly threatening chemical, biological, and radionuclear substances. However, more comprehensive agent categories will also be considered in the current analysis, including all chemical agents, all biological agents, all radiological agents, all foreign bodies, and the claimed use of 'poison' alone.

Research Aims

When a threat is received by the authorities, the media, or a victimized company, the recipient of such threats must have a plan in place in order to effectively respond. As stated by Geurts et al. (2016), it is vitally important to differentiate between those who plan to carry out their threats (i.e., actualizers) as opposed to those who offer threats but do not plan to carry them out (i.e., bluffers). While it is expected that the amount of detail a perpetrator supplies in regards to their agent of choice will (at least in part) indicate their true intention, it is not clear whether this will be consistent with the work of Sooniste et al. (2014) with less practical (*how*) detail being provided by threateners, or the work of Geurts et al. (2016) where bluffers offerred more such detail. However, it is believed that being able to name a specific contaminating agent could suggest existing knowledge on the part of the perpetrator, and thus the ability to follow through with the threat. As a result, in considering the agent reportedly named by the perpetrator, it is expected that:

H1 – Specifically named agents will be more strongly associated with actual contamination than cases involving vague threats of 'poison'

In addition, this work will also assess whether certain agent categories are more likely to be associated with actual contamination rather than empty threats alone, as well as the likelihood of encountering a genuine act of malicious contamination when a CBRN agent is claimed to have been used. Based on previous research it is expected that the most concerning agents, including biological, radionuclear and CBRN agents, will more often be associated with empty threats as opposed to actual contaminations, leading to the following hypothesis:

> *H2 – Particularly concerning agents, including biological, radiological and CBRN agents, will be more strongly associated with empty threats than chemical agents, foreign bodies and non-CBRN agents.*

Method

The Sample

The sample for this study consisted of all known malicious contamination incidents occurring worldwide from 1970 to 2011 in which there was some form of communication made on behalf of the perpetrator (n=77). This sample was taken from a larger dataset of malicious contamination incidents (n=384), composed of intentional poisonings, product tamperings, and incidents which fell in between these two categories. Poisonings and product tamperings can be said to exist on either end of a spectrum and have been fully defined elsewhere (Wilson & Kilbane, 2017), although poisonings are generally seen as being carried out by someone known to the victim, with the contamination occurring in the home with an open consumable, while product tamperings may involve a commercial target and unspecified victims, with a packaged consumable being

contaminated. While perpetrator communication itself is identified as a variable typically indicative of product tampering (Wilson & Kilbane, 2017), and incidents of product tampering were most numerous in this sample (n=69), there were also several cases of poisoning (n=7) and one intermediate case in this sample as well. Both poisoning and product tampering cases were included here as these acts are thought to occur on a continuum, and so considering such acts together provides a more complete understanding of the full spectrum of malicious contamination incidents.

A malicious contamination incident was considered to be a plot, threat, or an actual case of a consumer product or other consumable item being knowingly and intentionally contaminated. The contamination could occur at any point along the production chain and could involve any consumer product. However, cases believed to be accidental contaminations or contamination as a result of corporate negligence were not included in the sample. Sexual assault cases in which the victim was first drugged were also excluded as they were not captured by the search criteria and were thought to cover a different type of phenomenon. In addition, each of the 77 incidents in this sample could be considered as either a single attack on a specific individual or individuals using a consumer product, or a campaign of multiple attacks or threats on a consumer product being carried out using the same method and a common motive. Here campaigns were coded as single incidents due to the difficulty in separating out individual communications during the reporting of such cases. While this cross-sectional examination does not allow for the progression of threats to violence to be examined, it does make it possible to observe the association between communication-related variables and eventual contamination outcomes (i.e., whether or not a product will actually be contaminated).

Using the inclusion criteria for each case described above, malicious contamination incidents were identified from existing databases (Carus, 2002; Dalziel, 2009) and through

online newspaper searches. International, national and regional newspapers were searched using LexisNexis, ProQuest and ProQuest Historical, as well as Google and Google News search engines, and the US FDA's criminal investigation press releases. General search terms included *'product tampering', 'tamper', 'tampering', 'poison', 'poisoning', 'contamination',* and *'contaminate',* as well as the names of the perpetrators and victims when this information was known.

Once all known contamination incidents during the timeframe were compiled, a number of behavioral variables were coded as being either present or absent in each case, with news reports, academic journal articles, and government publications as described above being the sources of qualitative case data. For the current analysis, each incident was coded based on whether the chosen product was found to be contaminated or not (i.e., whether the case was an actual contamination or an empty threat), which agent was used or claimed to have been used (i.e., chemical, biological, radiological, foreign body, or 'poison'), who was contacted (i.e., the authorities, the media, or the targeted company), which method of communication was used (i.e., phone, letter, or email), and whether any demands were made (i.e., monetary or otherwise). In addition, cases were categorized based on whether they lacked the potential to cause any harm (i.e., a hoax case), and whether any illnesses or deaths resulted from the incident. With the exception of the name of the agent used as reported in the source material, all variables were coded dichotomously (the behavior being absent or present). An interrater reliability analysis was conducted on 18% of the data (n=14) with a second independent researcher familiar with the topic. This analysis yielded a significant kappa value (κ=.822, $p<.001$) indicating strong consistency.

While reducing descriptive, qualitative data into dichotomous data does have its shortcomings, this is a common technique in forensic psychology (e.g., Almond, Duggan, Shine, & Canter, 2005; Canter & Heritage, 1990; Donohue & Taylor, 2003; Dixon, Hamilton-Giachritsis, & Browne, 2008), and allows for statistical analyses to be conducted on the data. It must also be acknowledged that, unlike some past studies which have relied on direct communications (e.g.,

Geurts et al., 2014; Sooniste et al., 2014), the data here reflect what was reported of perpetrator communications in the media rather than the content of the actual communications themselves. This was due to the inability to gain access to actual threatening communications in contamination cases. Indeed, access to primary sources of data in these cases has previously been identified as a significant problem (Cremin, 2001; Dalziel, 2009). While such open-source intelligence may be lacking in detail (Egan et al., 2016), it makes for a necessary starting point when data from law enforcement or targeted companies is inaccessible, as is often the case with contamination cases.

Bayes' Theorem

In order to determine the likelihood of actual contamination taking place (as opposed to an empty or unactualized threat) when a specific threat is made, Bayes' Theorem will be used. This method allows for probabilities of future likelihood to be determined based on past observations. Bayes' Theorem can be defined as:

$$\Pr(A|X) = \frac{\Pr(X|A)\Pr(A)}{\Pr(X)}$$

The equation is then solved for Pr(A|X), or the posterior probability, which in this specific case is the probability of an item being actually contaminated (A) given a chosen agent (henceforth denoted as 'Y') is claimed to be used (X). The value of (X|A) is then the probability of an agent Y being used given the product in question has actually been contaminated, with Pr(A) and Pr(X) representing both the probability of a product actually being contaminated and the probability of an agent Y being used respectively. Once values have been identified for these variables the equation can be solved, with the value for Pr(A|X) then used to estimate the likelihood of an actual contamination occurring in the future given the claimed use of the selected variable. As little empirical research has been conducted in this area previously, the values for each of the variables on the right side of the equation will be based on the current dataset of contamination incidents.

Bayesian statistics may be used in the social sciences instead of traditional, frequentist null hypothesis testing, in part because the latter can be plagued by both false positives and false negatives. While Bayesian inference does not eliminate these errors, it relies on past information to obtain real-world probabilities. The use of Bayes' Theorem then allows for new information to be incorporated into existing models, with prior probabilities being updated as more information becomes available. Bayesian techniques have been previously used in modeling terrorism risk (Ezell, Bennett, von Winterfeldt, Sokolowski, & Collins, 2010; Horowitz & Haimes, 2003), developing accurate criminal profiles in cases of single victim homicides (Baumgartner, Ferrari, & Palermo, 2008), predicting recidivism for sexually violent offenders (Wollert, 2006) and crime linkage (de Zoete et al., 2014). In addition, Bayesian methods have also been recommended for use in risk prediction for forensic psychiatric patients (Duggan & Jones, 2017) and in Behavioural Investigative Advising (Allen, 2014).

Results

Communication and Agent Categories

In the 77 malicious contamination incidents in which communication was made by the perpetrator, the most common recipient was the targeted company (n=54; 70.1%), followed by the media (n=18; 23.4%) and the authorities (n=10; 13.0%), with 10 cases in which more than one type of recipient was contacted, and five where the recipient was not listed (see Table 1). Most commonly these communications were in the form of a posted letter (n=47; 61.0%) or a phone call (21; 27.3%), but communication was also made by email or some other online method (n=5; 6.5%). In 43 of the incidents (55.8%) the perpetrator demanded money, and in six additional cases (7.8%) there was some non-monetary demand made. One example of such a case involved an unknown perpetrator threatening to poison the products of an Australian biscuit maker unless a polygraph

test was administered to police officers involved in a 1991 murder conviction ("Biscuit maker drops stock", 1997).

Just over half of the cases in this sample (n=41; 53.2%) involved genuine contamination of the claimed product, with the perpetrator communication serving as an authentic warning or an actualized threat. While none of these actual contamination incidents resulted in any deaths, 19.5% (n=8) of such genuine contaminations led to at least one injury, and a further 51.2% (n=21) were potentially harmful in nature, with the remainder of cases (n=12; 29.3%) involving contamination with a harmless agent, such as dye or an agent which could not be transmitted to humans through the stated mechanism of delivery. One such example involved threats to introduce plutonium into the water supply of New York City unless charges were dropped against the 'Subway Vigilante' Bernhard Goetz (Weatherby, 1985). While a greater concentration of plutonium was found in a sample of the drinking water at the time, analysts could not determine at which point the water had been contaminated (Bogen et al., 1988). However, plutonium is unlikely to cause much damage when disseminated in a public water source as it will be diluted to harmless amounts (Durante & Manti, 2002), and so the potential for physical harm in this case was virtually non-existant. Such hoaxes are thus included here as they indicate that the perpetrator had the means and the ability to contaminate the product, even if no harm could result.

Of the information contained in such communications in addition to demands, this often included the chosen product or products, whether the item had been contaminated already or might be in the future, and the contaminating agent selected. As mentioned, the agents could be broadly split into categories of chemical agents (n=38; 49.4%), biological agents (n=19; 24.7%), radiological agents (n=1; 1.3%), or foreign bodies (n=8; 10.4%), although more than one agent could be used in a single communication, as occurred in five cases (see Table 1). In eight cases the specific agent was

either unspecified, unknown or unreported, and in 10 cases (13.0% of incidents) only a vague description was included using words like ‘poison’ or ‘contaminate’. In 89.6% of communications in this sample an agent was mentioned in the communication, even if only through use of a vague term as described above. Agent categories are considered here as it would be unmanageable to determine base rates for all 40 different agents claimed to have been used in the cases in this sample.

TABLE 1 ABOUT HERE

As can be seen in Table 2, the likelihood of actual product contamination based on the agent mentioned in the perpetrator communication (Pr(A|X)) differs for each agent type. Again, Pr(A) represents the overall likelihood of actual contamination in the sample, Pr(X) the likelihood of such an agent being used in all cases, and Pr(X|A) the probability of such an agent being used given actual contamination occurring. From this information the equation can be solved for Pr(A|X), with this column showing the probability of an attack taking place given the agent identified has been mentioned by the perpetrator. Claimed uses of radiological agents, foreign bodies, and multiple different agents were associated with a high likelihood of genuine contamination (>80%), while the use of a vague phrase like ‘poison’ was only associated with less than a 10% chance of such an outcome. However, it is worth noting that only one case of a radiological agent being claimed to be used was identified in this sample, and as a result the probably would be likely to change if additional cases of radiological threats were incorporated.

TABLE 2 ABOUT HERE

For the two most prevalent agent types, the probability of actual contamination was 76.1% for chemical agents compared to 26.3% for biological agents. However, as both the designations for ‘biological agent’ and ‘chemical agent’ are relatively broad, describing agents with variable degrees

of harmfulness, a more specific designation is needed to fully understand the probability of threat actualization when the most concerning agents are selected.

CBRN Agents and Contamination

Here CBRN agents (as defined above) were considered those agents classified as chemical weapons, bioterrorism agents, or radiological elements. A complete list of the CBRN agents reported in this sample can be found in Table 3, along with the number of cases in which each agent was used or claimed to have been used. Only six incidents were identified as claiming the use of CBRN agents in this sample, with five of these involving bioterrorism agents, and the remaining incident involving radioactive plutonium. With the exception of ricin which is listed under Schedule 1 of the CWC, no other chemical weapons were used or were claimed to have been used in this sample.

TABLE 3 ABOUT HERE

As previously mentioned and as can be seen with Pr(A) in Table 4, when communication is received during a malicious contamination incident there is just over a 50% chance that the product identified will actually be contaminated, with the opposing probability of an empty threat represented by Pr(A'). However, the probability that a case will involve a CBRN agent – whether as a hoax or an actual contamination – is much lower, at 7.8%. Using Bayes' Theorem, the likelihood of an item actually being contaminated when a CBRN threat is received is 33.4%, which is a reduction from the likelihood of actualization for all communication cases (Pr(A)). Therefore, when a perpetrator issues a contamination threat involving a CBRN agent, it is more likely that this is an empty threat.

TABLE 4 ABOUT HERE

Discussion

By examining malicious contamination cases in which communication was made by the perpetrator, the highest likelihood of actual contamination was found with the claimed use of radiological agents (98%), foreign bodies (88%) and chemical agents (76%), while the claimed use of biological agents indicated only a 26% chance of actual contamination. These results were found to lend support to the second hypothesis, with the exception of radiological agents, which were expected to be more strongly associated with empty threats than actual contamination. This may be due to the fact that very few radiological cases were found in this sample, with the potential for the inclusion of additional radiological cases to substantially change the predicted outcome. Therefore, the results provided by this paper for radiological agents should be used with caution until more data can be collected on such cases. As for chemical and biological agents, it may be that chemical agents, which can include easily accessible household poisons, such as pesticides and cleaning products, are selected due to both their availability and their potential to cause harm. Biological agents on the other hand are often more difficult to access and may also be more fear inducing, indicating that they could be more useful during empty threats as opposed to genuine attempts to harm consumers.

For CBRN agents specifically a 33% likelihood of actual contamination was found. As mentioned, it may be that frightening yet difficult to obtain biological and CBRN agents are more likely to be used in threats than actual contamination incidents due to their ability to create a great deal of fear among the general public. This is consistent with the work of Carus (2002) in that while biological pathogens and toxins may be used quite frequently during threats, the perpetrators are rarely in possession of such agents. Cornish also reiterates this point when it comes to biological weapons (BW), stating “[i]n the terrorist’s mind, even the language or threat of a BW attack could offer a high level of celebrity and media/public interest” with the possibility for terrorists to exploit psychological vulnerability using only a series of threats (Cornish, 2007, p.13). However, it is important to note here that only six CBRN agents were identified in the current sample, and so as

described above in the case with radiological agents, additional data could change this likelihood of contamination considerably.

As Duggan and Jones (2017) note, the use of Bayes' Theorem will never result in a definitive 'yes' or 'no' answer, or in this case whether a product will or will not be contaminated. However, using this technique during investigations can help those responsible for assessing threats make decisions which are informed by existing evidence. While the results of this study provide the first known base rates for contamination outcomes based on agents used or claimed to have been used, the relatively small sample size should not be ignored. Therefore, it is hoped that this study will serve as the foundation for further data collection in this area, and that the usefulness of such predictions will increase along with an increasing number of observations.

Despite the low likelihood of actual contamination, there was still found to be roughly a 1 in 4 chance that claimed use of a biological agent, and a 1 in 3 chance that claimed use of a CBRN agent, would result in actual contamination. Due to the probability of contamination in such instances and the potential severity of outcomes should a contaminated item reach consumers, more attention should be paid to what other factors could be useful in identifying genuine cases of contamination. This is particularly important for other pieces of *how* information which could be gleaned from perpetrator communications, such as who the recipient of the contact is (e.g., the police, the targeted company, the media, etc.) or the language of the threat (e.g., whether this involves a future threat that '*something will be poisoned*' or a claim that an item '*has already been poisoned*'). In the future, these additional elements of perpetrator communications could be used to create a model which incorporates multiple variables, and thus offers more predictive utility than the relatively simple probabilities identified in this study.

Consistent with the first hypothesis, considering only those cases where a vague description of 'poison' was noted, less than 10% of these cases resulted in actual contamination. In comparison to the claimed use of multiple different agents, which was associated with an 80% likelihood of contamination, this seems to suggest that fewer *how* details about the claimed agent (e.g., threatening with 'poison' rather than a specific agent) may be more strongly associated with bluffing, which is not consistent with the findings of Geurts et al. (2016). Instead, it may be that perpetrators who offer less detail regarding their agent choice may do so as they have not fully formed implementation intention around the actual act of contamination, and may instead be focusing on the delivery of the threat itself. However, it should be reiterated that the current study did not directly compare the language used by actualizers and bluffers as the content of perpetrator communications were not always available, and so further research would need to be conducted using the content of perpetrator threats before any firm conclusions could be drawn.

It is also worth noting that the probabilities of actual contamination in this sample also contain some hoax cases, or instances where a product was contaminated but would not result in any harm to consumers (e.g., the case of plutonium in a public water supply as previously mentioned). Because of this, the probability of contamination here does not fully equate to the immediate risk of harm, but instead the ability for a perpetrator to contaminate a product. Therefore, when a threat is received, the language used to describe the chosen agent and the specific method of delivery should be carefully considered to determine whether the contamination threat described by the perpetrator is even feasible. For instance, it is believed that someone with access to an agent like *S. typhi* would be able to identify the bacterium by name, and would understand that this is the agent of contamination, rather than 'typhoid', which is instead the disease caused by this agent. In addition to using diseases as agents such as 'typhoid' or 'botulism', this is also pertinent in instances where the claimed agent cannot be spread through food or water as is the case with HIV, which was claimed to have been used in several cases in this sample during

the height of public fear and misinformation surrounding HIV transmission. Such claims may show a level of ignorance on the part of the perpetrator when it comes to the use of these agents, and would likely fail what Tunkel (2010) refers to as the 'reality test'. This concept was initially applied to bomb threats without further action, with threats failing such a test unlikely to involve logical, actionable threats (Tunkel, 2010). Therefore, it would be helpful in the future not only to consider the amount of *how* or *why* detail provided, but also the accuracy of the actual threat described when threatening communications are available. This also emphasizes the importance of involving those with specific knowledge of chemistry, biology, or a related discipline when attempting to determine the likelihood of contamination threats being actualized.

It is also worth noting that 'threat' and 'actualization' in contamination cases may not be distinct and opposing categories. As mentioned, threats may result in consumer fear and economic damage even if no product is ever contaminated. In addition, genuine contamination may involve different levels of seriousness, as the use of a harmless dye may not result in any casualties, while a small amount of household poison may be more serious, and the use of a chemical or biological weapon would be of the highest concern. Therefore, while this paper has considered actualization to be coded dichotomously as either present or absent, future research should focus on the scale of potential harm involved in contamination incidents.

As with terrorist incidents specifically, coding event data comes with a number of limitations, including determining attribution (Mickolus, 2002). For instance, when identifying threats it can often be extremely difficult to be certain of where a threat has originated, as even if a group claims responsibility this does not necessarily mean that they are responsible. While the language of threats has been identified as important, the specific transcript of each threat is not available in the majority of cases when relying on open

source data, and so it is not possible to conduct an in-depth analysis of what was said by each perpetrator. Threats were also coded together when a campaign was involved, and so some of what was reported as having been said may have occurred across a number of different individual communications. This limits the ability to determine, in cases where contamination occurred, exactly *when* it occurred but also *what* may cause a threat to progress to actuation. Where available, it would be valuable in the future to examine each set of communications over time to determine how a trajectory to violence may materialize in such cases, especially as demands are likely to change over the course of an extortion attempt (Cremin, 2001). Additionally, in the cases in which there was direct communication (e.g., a telephone contact) it is not known what was asked of the perpetrators, or how this may have affected their threats or demands. However, due to the nature of the available data, any future study looking to examine the context of such threats would require cooperation from the holders of more detailed data, including law enforcement and companies which have been previously targeted.

The nature of the data means that, while cases were recorded from many different countries worldwide, there is likely a bias towards English-speaking countries generally, and towards the US and UK specifically, with these countries most frequently appearing as the incident location in the data. As a result, there could be issues with the generalizability of these results. In addition, as data were collected over the span of more than 40 years, it is possible that temporal issues also have an effect on these results. One such example could be the fact that less than 7% of communications in this sample were made via the Internet, although it is acknowledged that a more recent sample would likely include a larger percentage of online communications. Indeed, in a sample of violent lone actors examined over 23 years, Gill et al. (2016) found that offenders were more likely to make use of the Internet in recent cases, although most offender behaviours observed in such cases were not found to differ significantly based on time period.

The use of open source data could also mean a bias in the data towards the most sensational cases, with more cases being included that involve particularly frightening agents, such as ricin, rather than, for instance, rat poison. Additionally, this could also mean a bias in the data towards more successful attacks, as unsuccessful attacks may be less likely to gain publicity in the media, due to the fact that they are generally less sensational and thus less newsworthy. This is consistent with previous works which have found that the media may underreport hoax cases (see Tishler, 2016). Other potential gaps in the data have been identified previously when studying contamination (Cremin, 2001; Wilson & Kilbane, 2017), and so it is imperative that any method of data analysis used with such a sample allow for the inclusion of new information as it become available. Indeed, the use of Bayes' Theorem means that as more information is discovered the calculated posterior probability becomes the prior probability for subsequent analyses (Duggan & Jones, 2017), allowing for more accurate predictions to be ultimately made.

Conclusion

While CBRN terrorist events may be an increasingly serious issue with the potential to cause catastrophic destruction (Mohtadi & Murshid, 2009), it still appears that such concerning agents are more likely to be used in empty threats as opposed to actual contamination incidents. However, due to the possibility of such a high number of casualties when one of these fear-inducing agents is used, it is crucial that more is done to separate authentic threats from those which will not be actualized. This should involve both the examination of other variables taken from threatening perpetrator communications, but also the close examination of the threats themselves to determine whether they are realistic. While these results provide a starting point for understanding the relationship between agent choice and likelihood of contamination, further research and additional data would allow for more robust predictions to be made, which could then be used by law

enforcement to enhance their decision making when threats are received against the supply chain.

References

Allen, J. C. (2014). Investigative advising: a job for Bayes. *Crime Science*, *3*(1), 7.

Almond, L., Duggan, L., Shine, J., & Canter, D. (2005). Test of the arson action system model in an incarcerated population. *Psychology, Crime & Law, 11*(1), 1-15.

Wilson, M. A., & Kilbane, S. C. (2017). Criminal Poisoning and Product Tampering: Toward an Operational Definition of Malicious Contamination. *Deviant Behavior, 38*(10), 1141-1159.

Baumgartner, K., Ferrari, S., & Palermo, G. (2008). Constructing Bayesian networks for criminal profiling from limited data. *Knowledge-Based Systems, 21*(7), 563-572.

Biscuit maker drops stock. (1997, February 22). *The Times*.

Bogen, D. C., Krey, P. W., Volchok, H. L., Feldstein, J., Calderon, G., Halverson, J., et al. (1988). Threat to the New York City water supply - plutonium. *Science of the Total Environment, 70*, 101-118.

Canter, D., & Heritage, R. (1990). A multivariate model of sexual offence behaviour: Developments in 'offender profiling'. *The Journal of Forensic Psychiatry, 1*(2), 185-212.

Carus, W. (2002). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900.* Amsterdam: Fredonia Books.

Center for Food Safety and Applied Nutrition (2001). *Food Safety and Security: Operational Risk Management Systems Approach.* US Food and Drug Administration.

Center for Food Safety and Applied Nutrition (2003). *Risk Assessment for Food Terrorism and Other Food Safety Concerns.* US Food and Drug Administration.

Cornish, P. (2007). *The CBRN System: Assessing the threat of terrorist use of chemical, biological, radiological and nuclear weapons in the United Kingdom.* The Royal Institute of International Affairs.

Cremin, B. (2001). Extortion by Product Contamination. *American Behavioral Scientist , 44*(6), 1042-1052.

Dalziel, G. R. (2009). *Food Defence Incidents 1950-2008: A chronology and analysis of incidents involving the malicious contamination of the food supply chain.* Nanyang, Singapore: Centre of Excellence for National Security.

de Zoete, J., Sjerps, M., Lagnado, D., & Fenton, N. (2015). Modelling crime linkage with Bayesian networks. *Science and justice*, *55*(3), 209-217.

Dixon, L., Hamilton-Giachritsis, C., & Browne, K. (2008). Classifying partner femicide. *Journal of Interpersonal Violence, 23*, 74-93.

Donohue, W., & Taylor, P. (2003). Testing the Role Effect in Terrorist Negotiations. *International Negotiation, 8*, 527-547.

Duggan, C., & Jones, R. (2017). Managing uncertainty in the clinical prediction of risk of harm: Bringing a Bayesian approach to forensic mental health. *Criminal Behaviour and Mental Health*, *27*(1), 1-7.

Durante, M., & Manti, L. (2002). Estimates of radiological risk from a terrorist attack using plutonium. *Radiation and Environmental Biophysics, 41*, 125-130.

Egan, V., Cole, J., Cole, B., Alison, L., Alison, E., Waring, S., et al. (2016). Can You Identify Violent Extremists Using a Screening Checklist and Open-Source Intelligence Alone? *Journal of Threat Assessment and Management, 3*(1), 21-36.

Ezell, B., Bennett, S., von Winterfeldt, D., Sokolowski, J., & Collins, A. (2010). Probabilistic Risk Analysis and Terrorism Risk. *Risk Analysis, 30*(4), 575-590.

Geurts, R., Granhag, P., Ask, K., & Vrij, A. (2016). Taking Threats to the Lab: Introducing an Experimental Paradigm for Studying Verbal Threats. *Journal of Threat Assessment and Management, 3*(1), 53-64.

Gill, P., Horgan, J., Corner, E., & Silver, J. (2016). Indicators of lone actor violent events: The problems of low base rates and long observational periods. *Journal of Threat Assessment and Management*, *3*(3-4), 165.

Gleick, P. (2006). Water and terrorism. *Water Policy, 8*, 481-503.

Graves, M., Smith, A., & Batchelor, B. (1998). Approaches to foreign body detection in foods. *Trends in Food Science & Technology, 9*, 21-27.

Horowitz, B., & Haimes, Y. (2003). Risk-Based Methodology for Scenario Tracking, Intelligence Gathering, and Analysis for Countering Terrorism. *Systems Engineering, 6*(3), 152-169.

Ivanova, K., & Sandler, T. (2007). CBRN Attack Perpetrators: An Empirical Study. *Foreign Policy Analysis, 3*, 273-294.

Jackson, B. A., & Frelinger, D. R. (2008). Rifling Through the Terrorists' Arsenal: Exploring Groups' Weapon Choices and Technology Strategies. *Studies in Conflict & Terrorism*, *31*(7), 583-604.

Khan, A., Swerdlow, D., & Juranek, D. (2001). Precautions against Biological and Chemical Terrorism Directed at Food and Water Supplies. *Public Health Reports , 116*, 3-14.

Lemyre, L., Clement, M., Corneil, W., Craig, L., Boutette, P., Tyshenko, M., et al. (2005). A Psychosocial Risk Assessment and Management Framework to Enhance Response to CBRN

Terrorism Threats and Attacks. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, 3*(4), 316-329.

Logan, B. (1993). Product Tampering Crime: A Review. *Journal of Forensic Sciences , 38*(4), 918-927.

Mickolus, E. (2002). How Do We Know We're Winning the War Against Terrorists? Issues in Measurement. *Studies in Conflict & Terrorism, 25*, 151-160.

Mitchell, M. (1989). The impact of external parties on brand-name capital: The 1982 Tylenol poisonings and subsequent cases. *Economic Enquiry, 27*(4), 601-618.

Mohtadi, H., & Murshid, A. P. (2009). Risk Analysis of Chemical, Biological, or Radionuclear Threats: Implications for Food Security. *Risk Analysis, 29*(9), 1317-1334.

Monaghan, R. (2000). Single-Issue Terrorism: A Neglected Phenomenon? *Studies in Conflict & Terrorism, 23*, 255-265.

Morgan, F. (1988). Tampered Goods: Legal Developments and Marketing Guidelines. *Journal of Marketing, 52*, 86-96.

Palmer, I. (2004). The Psychological Dimension Of Chemical, Biological, Radiological And Nuclear (CBRN) Terrorism. *Journal of the Royal Army Medical Corps, 150*, 3-9.

Plamboeck, A., Stoven, S., Davidson, R. D., Fykse, E., Griffiths, M., Nieuwenhuizen, M., et al. (2016). Laboratory analysis of CBRN-substances: Stakeholder networks as clue to higher CBRN resilience in Europe. *Trends in Analytical Chemistry, 85*, 2-9.

Rotz, L., Khan, A., Lillibridge, S., Ostroff, S., & Hughes, J. (2002). Public Health Assessment of Potential Biologicla Terrorism Agents. *Emerging Infectious Diseases, 8*(2), 225-230.

Sheeran, P., Milne, S. E., Webb, T. L., & Gollwitzer, P. M. (2005). Implementation intentions. In M. Conner, & P. Norman (Eds.), *Predicting health behavior* (p. 276-323). Buckingham, UK: Open University Press.

Sobel, J., Khan, A. S., & Swerdlow, D. L. (2002). Threat of a biological terrorist attack on the US food supply: the CDC perspective. *The Lancet, 359*, 874-880.

Sooniste, T., Granhag, P. A., Stromwall, L. A., & Vrij, A. (2014). Discriminating between true and false intent among small cells of suspects. *Legal and Criminological Psychology, 21*(2), 344-357.

Stinson, T. F., Kinsey, J., Degeneffe, D., & Ghosh, K. (2007). Defending America's Food Supply Against Terrorism: Who is Responsible? Who Should Pay? *Choices, 22*(1), 67-71.

Tishler, N. (2013). C, B, R, or N: The Influence of Related Industry on Terrorists' Choice in Unconventional Weapons. *Canadian Graduate Journal of Sociology and Criminology, 2*(2), 52-72.

Tishler, N. (2016). *Taking Hoaxes Seriously: Characteristics of Terrorism Hoaxes and their Perpetrators.* Canadian Network for Research on Terrorism, Security and Society.

Tunkel, R. F. (2010). Bomb Threat Assessments Fact Sheet. *Arkansas Safe Schools Initiative Division*.

Weatherby, W. J. (1985, August 5). New York hums in the rain / Rain storms eventually ease the problems of water rationing. *The Guardian*.

World Health Organization. (2008). *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems.* World Health Organization, Department of Food Safety, Zoonoses and Foodborne Diseases. Geneva: World Health Organization.

Wilson, M. A., & Lemanski, L. (2013). Apparent intended lethality: Toward a model of intent to harm in terrorist bomb attacks. *Dynamics of Asymmetric Conflict, 6*(1-3), 1-21.

Wollert, R. (2006). Low base rates limit expert certainty when current actuarials are used to identify sexually violent predators: An application of Bayes's theorem. *Psychology, Public Policy, and Law*, *12*(1), 56.

Yeung, R., & Morris, J. (2001). Food safety risk: Consumer perception and puchase behaviour. *British Food Journal, 103*(3), 170-186.

Table 1

Frequencies of different variable categories for actual contaminations and empty threats

Variable category	Variable	Actual contamination (n=41)	Empty threat (n=36)	Totals

Recipient				
	Authorities	7	3	10
	Targeted company	30	24	54
	Media	12	6	18
	Multiple recipients	8	2	10
	Unreported	0	5	5
Type of communication				
	Letter	23	24	47
	Phone call	14	7	21
	Online	3	2	5
	Multiple types	7	5	12
	Unreported	8	8	16
Demands				
	Monetary	20	23	43
	Non-monetary	4	2	6
Agent				
	Chemical	29	9	38
	Biological	5	14	19
	Radiological	1	0	1
	Foreign body	7	1	8
	Multiple agents	4	1	5
	'Poison'	1	9	10
	'CBRN'	2	4	6

Note. Agent categories are not mutually exclusive.

Table 2

Individual probabilities of Bayes' Theorem for each type of agent claimed to have been used

Agent	n	Pr(A)	Pr(X)	Pr(X|A)	Pr(A|X)

Chemical	38	.532	.494	.707	.761
Biological	19	.532	.247	.122	.263
Radiological	1	.532	.013	.024	.982
Foreign body	8	.532	.104	.171	.875
Multiple agents	5	.532	.065	.098	.802
'Poison'	10	.532	.130	.024	.098

Note. When a threatening communication is received, Pr(A) is the probability of an item being actually contaminated, Pr(X) is the probability that the indicated agent will be used or claimed to be used, Pr(X|A) is the probability that the indicated agent is used given the product in question has actually been contaminated, and Pr(A|X) is the probability that actual contamination will occur given the indicated agent is used or claimed to have been used.

Table 3

Frequency of specific CBRN agents claimed to have been used

Agent claimed	n	Identification criteria
Ricin	1	CDC Category B; CWC Schedule 1
Escherichia coli	2	CDC Category B
Shigella dysenteriae	1	CDC Category B
'Typhoid'	1	CDC Category B
Plutonium	1	Radiation emitting material

Table 4

Individual probabilities and descriptions for the different components of Bayes' Theorem for CBRN agents

Component	Description	n	Probability
Pr(A)	Probability of an actual contamination	41	.532
Pr(X)	Probability of a CBRN agent used	6	.078
Pr(A')	Probability of no contamination (empty threat)	36	.468
Pr(X|A)	Probability of a CBRN agent being used given an actual contamination	2	.049
Pr(X|A')	Probability of a CBRN agent being used given an empty threat	4	.111
Pr(A|X)	Probability of actual contamination given the claimed use of a CBRN agent		.334