Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

On the scale from ransomware to cyberterrorism: the cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine

Lora Pitman & Wendy Crosier

To cite this article: Lora Pitman & Wendy Crosier (2024) On the scale from ransomware to cyberterrorism: the cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine, Journal of Cyber Policy, 9:2, 179-199, DOI: 10.1080/23738871.2024.2377670

To link to this article: https://doi.org/10.1080/23738871.2024.2377670

Published online: 16 Jul 2024.

JOURNAL OF CYBER POLICY
2024, VOL. 9, NO. 2, 179–199
https://doi.org/10.1080/23738871.2024.2377670

Routledge
Taylor & Francis Group

On the scale from ransomware to cyberterrorism: the cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine

Lora Pitman [a] and Wendy Crosier[b]

[a]Department of Intelligence and Security Studies, Coastal Carolina University, Conway, SC, USA;
[b]Department of Political Science, University of Maine, Orono, ME, USA

ABSTRACT

This research explores the conditions under which ransomware can be considered as an act of cyberterrorism and whether the cases of JBS USA, Colonial Pipeline and the wiperware attacks against Ukraine in 2022 constitute such. These theoretical and practical issues are particularly important in light of the negotiations at the United Nations level for a binding treaty on cybercrime. To achieve these goals, we have undertaken the following steps in designing a model for the analysis of ransomware events. First, we searched for an agreed-upon definition for cyberterrorism in the academic literature. To do so, we compiled a dataset of one hundred peer-reviewed articles published in scholarly journals on the topic of cyberterrorism. We reported whether authors considered factors such as inducing a sense of fear/panic, the destruction of property or the threat of such, and/or killing/violence/coercion or the threat of such as necessary conditions for the definition of cyberterrorism. Second, we complemented academic views with the definitions of practitioners and policymakers. Third, we applied the model to test whether the three ransomware case studies fit the criteria for cyberterrorism. We found that based on the proposed framework, all case studies constitute acts of cyberterrorism, albeit to a different extent.

ARTICLE HISTORY
Received 10 March 2022
Revised 21 February 2024
Accepted 7 May 2024

KEYWORDS
Ransomware; cyberterrorism; cybercrime treaty; cyberattacks

Introduction

As of 2021, there were 4.66 billion internet-users (Johnson 2021). The rapid increase of internet use over the years has resulted in people being more connected. The issue is that it has made them more connected both to users with whom they want to be connected but also to those with whom they do not want to be, such as hackers, for instance. According to economic forecasts, financial damages caused by ransomware are significant. While ransomware as a concept is defined by IBM (2023) as 'a type of malware that locks a victim's data or device and threatens to keep it locked – or worse – unless

CONTACT Lora Pitman lpitman@coastal.edu
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

the victim pays a ransom to the attacker', there are some nuances that warrant more attention. Ransomware, in its basic form, indeed locks the victim's information, which gets released once the victim pays the demanded ransom. In a more recent and advanced form called wiperware, the victim's information is erased completely, regardless of whether the ransom is paid. The victim, at the same time, is unaware of the fact that their information will not be retrieved and still perceives the attacker's actions as ransomware, hoping that the data is not lost, and sometimes paying the ransom just to find out that their data has been erased. Therefore, at its core, wiperware represents a form of ransomware due to the similarities of the two – the impression the victim has that they can regain access to their data, and the message for ransom (present in both classic ransomware and wiperware cases). At the same time, wiperware is even more dangerous, as the victim perceives it as ransomware despite the intent of the attacker, which is claimed to be the only difference between both along with the scale of the damages (Warner 2022).

A careful look into the mechanism of ransomware is also needed as projections show that by the year 2031, losses will exceed $265 billion (Braue 2021). The same report shows that the cost of ransomware will not only increase in the coming years, but that it is the fastest growing type of cybercrime. It is increasingly often that businesses have become the targets of ransomware demands. When they are responsible for delivering public goods and services, an attack on them may result in repercussions for a significant number of people. This raises the question: when ransomware targets businesses providing critical products and services for a state, resulting in economic disruptions on a local, regional, state, federal or even international level, is it reasonable to discuss malware in the context of cyberterrorism?

Some recent cases of ransomware include JBS USA, one of the US's biggest meat producers, Colonial Pipeline, the largest US pipeline system, and the cluster of wiperware attacks against Ukraine in 2022. These cases show that it is no longer a phenomenon affecting only businesses. The damages have spread beyond the day-to-day operations of companies, seriously disrupting people's lives and the economy. The series of wiperware attacks against Ukraine in 2022 adds a political dimension to ransomware and poses even more questions to be considered by nations, especially in the context of the negotiations for a United Nations treaty on cybercrime (United Nations General Assembly 2020).

The magnitude and seriousness of the latest cases of ransomware, and the lack of clarity on when ransomware represents a case of cyberterrorism, are the factors that led us to formulate our research question – under what conditions should ransomware be considered an act of cyberterrorism. Because this is a relatively new topic in the field of cybersecurity and national/international security, the number of works addressing this issue is still limited. Therefore, to respond to our research question, we undertook several different steps in our methodology.

First, to assess whether a certain case can be viewed as an act of cyberterrorism, there needs to be an agreed-upon definition for *cyberterrorism*. Scholars vary considerably in their opinion, so we have sought a relative scholarly consensus on the definition. To clarify this approach, we collected only academic definitions for the concept of cyberterrorism. National/international definitions may differ from the academic ones, but proposing a model for defining cyberterrorism as a scholarly term is the first step towards a further potential harmonisation of legislation across borders. The model can then be considered by nations and international organisations and be made more suitable for the

specific needs and goals of these state and non-state actors as political entities. We coded how scholars use cyberterrorism in their peer-reviewed articles by identifying the specific attributes of the concept. To be more inclusive and because of the very fragile level of consensus among scholars on the topic, we also added the perspectives of some policy-makers and practitioners.

Second, we constructed a model with multiple variables in order to assess what would be required of ransomware for it to constitute an act of cyberterrorism. We then explored to what extent the JBS and Colonial Pipeline cases and the 2022 wiperware cluster of attacks against Ukraine constitute cyberterrorism.

Our paper contributes to the scholarly literature on cybersecurity and national/international security in the following ways. On the one hand, it demonstrates a lack of agreement among scholars on a definition for 'cyberterrorism' in a quantitative manner and addresses practical issues regarding how to identify elements of cyberterrorism in concrete cases. On the other, it proposes a model through which events can be labelled as ransomware only or as a ransomware case which also constitutes an act of cyberterrorism. Lastly, we enquire to what extent three of the recent cases of ransomware can be considered acts of cyberterrorism. The theoretical and practical implications from our study should inform policies both at the national level and at the UN level, as the latter is in the process of seeking to introduce a harmonised approach against cybercrime.

Review of the literature

Definitional issues

The concept of 'terrorism' varies with the jurisdictions of countries. It is often broadly defined, and the specific details of a case help determine whether or not it will qualify as an act of terrorism. In this regard, Embar-Seddon (2002) notes that 'a significant barrier to constructing a definition of cyberterrorism is the lack of a consistent definition of terrorism.' The need for an agreed-upon definition of cyberterrorism, and even terrorism, has been noted by researchers as part of NATO Cooperative Cyber Defence Centre of Excellence efforts (Dogrul et al. 2011). Failing to define it, the authors emphasise, may negatively affect the attempts of NATO members to coordinate cyber capabilities and effectively respond to cyberthreats. One problem hindering the harmonisation of the definition across legislations is also the question of how significant the act should be to constitute terrorism or cyberterrorism.

Terrorism is broadly described as an act of violence or the threat of such, using intimidation tactics aimed at a large number of people, different from the direct victims themselves (Enders and Sandler 2011). These acts can be in pursuit of social, political, economic or religious goals. With the emergence of the phrase 'cyberterrorism', the definitional issues have become even more complicated. It is insufficient to say that a cyber incident becomes an act of cyberterrorism if it is conducted by a terrorist organisation (e.g. non-state actors such as the Islamic State of Iraq and Syria (ISIS) or the Lazarus Group). While some of the perpetrators of cyberterrorism are non-state actors, contributing to the agenda of state actors, deciding whether or not an act is a form of cyberterrorism should be based on the act as opposed to focusing only on the perpetrator (Thackrah 1987). This is especially true, since many terrorist attacks in physical space remain

unattributed to a particular entity (National Consortium for the Study of Terrorism and Responses to Terrorism (START) 2021). The task of tracking the plans of perpetrators and preventing future violence or threats has been complicated by new ransomware tactics and transactions through bitcoin or other digital currencies (Lee and Choi 2021). The issue becomes even more exacerbated when ransomware results in major damages and consequences that are not identifiable to a known terrorist organisation but to another entity. The question that naturally arises is whether a cyber incident becomes an act of cyberterrorism if the intent behind the attack is pursuant to a political or ideological goal rather than just financial gain (Beaman et al. 2021; Connolly and Wall 2019; Nershi and Grossman 2023; Yuryna Connolly et al. 2020).

Some authors have taken a logical approach to deriving a definition for cyberterrorism by employing the concept of traditional terrorism and making it accommodate the conditions of cyberspace. In particular, Rogers (2003, 78) describes it as an activity by 'an individual who uses computer/network technology to control, dominate, or coerce through the use of terror in furtherance of political or social objectives'. Rogers continues that it is not sufficient for an operation to have just a government or a military unit as a target, but the intention to affect both the unit and the public. Furnell and Warren (1999) argue that there are not many distinguishable characteristics of traditional hackers and cyberterrorists, outside their agenda. Regarding the consequences from a cyberterrorist act, Desouza and Hensgen (2003) discuss that the common perception among scholars is that cybercrime is classified as an act of cyberterrorism when there are material consequences in the physical world. They argue that it should be viewed as sufficient cause for classification if these consequences appear solely in the digital world, as some of the most powerful economies conduct a very significant number of transactions exclusively in cyberspace. While both studies should be taken into consideration, it is important to note that the cyberthreat landscape has changed considerably ever since, along with the opportunities to obtain more information, for the perpetrators through cyber intelligence collection methods (Uthoff 2022). A more recent work, presenting a series of surveys among policymakers and scholars by Macdonald et al. (2019, 7) emphasises the following trend regarding terrorism and cyberterrorism: 'the definitional issues around terrorism in general remain as important as five years ago and are no closer to being resolved, but also that a specific definition of cyberterrorism is *more necessary* now than it was then.' While academics and policymakers are still trying to find an answer to the question about the nature of cyberterrorism, Macdonald and colleagues identified some elements on which most scholars have agreed, which will be outlined in the following section. We complemented these elements with additional scholarly views and with our own more recent exploration, which will be summarised in the segment after the literature review.

Elements of the definition

Macdonald, Jarvis and Lavis (2019) concluded that there was a relative consensus among the respondents in the survey regarding three core elements of cyberterrorism: (1) the political motive of the attack; (2) the digital means and/or the target through which the attack was conducted; and (3) the aim to instil fear with the attack as an intention. Among the other elements that were considered but did not gather enough consensus from the surveyed scholars and practitioners was whether the acts should manifest as

concrete harm to property or people (Macdonald et al. 2019). The discussion below aims to specify how different elements of the definition of cyberterrorism can be identified and applied in practice.

While there seems to be wide agreement that terrorism and cyberterrorism involve a political/ideological reason for committing the acts, few authors actually identify what expressions these motives can have, especially if the perpetrator is not a known terrorist organisation. Moreover, one of the most difficult elements of any crime is to prove intent, especially in cyberspace where the anonymity of the perpetrator can hinder such an effort. This opens up the possibility of not labelling many cybercrimes as terrorist acts, not prosecuting them as such, and not sentencing the offenders as harshly as they would have been if their act was identified as cyberterrorism. In order to compensate for this, a useful set of intent-determining features needs to be adopted when it comes to cyberterrorism. This could be modelled on how intent is proved for traditional crimes – 'shown by circumstantial evidence such as the acts or knowledge of the defendant' (Legal Information Institute 2020). For instance, this could be if the perpetrator knew (or it could have been reasonably expected that they should have known) that with their act they could fulfil the other elements of the cyberterrorist act: the use of a device to inflict severe, large-scale damages to property or people which will also instil a great amount of fear. Particularly relevant in cyberterrorism are acts through which a state and its people are coerced or intimidated by significant economic disruptions, which can cause fear and terror (Yunos and Sulaman 2017). An additional useful distinction between ransomware and cyberterrorism would be if the target is a major company/government entity providing critical services to the population (healthcare, food, water, petrol or other essential services and resources). In this example, the cybersecurity threat may reach the dimensions of a cyberterrorism case, assuming a critical service is deliberately impacted by the perpetrator(s) knowing what the scale of the damages will be if the ransom is not paid. The issues with both cyberattacks and cyberterrorism cases pertain to cybersecurity, but the difference lies in the perpetrator's intent, motivation, understanding and acceptance of the fear/terror and large-scale damages that the act will provoke. A study by Plotnek and Slay (2021) showed that scholars mostly rely upon the effect of the attack, the type of the target and the means through which it was conducted to emphasise their definitions of cyberterrorism – all of which can be relatively easy to prove, despite the elusiveness provided by cyberspace for illegal cyber activities. Results from a study based on focus groups of government officials, conducted in collaboration with the Southeast Asia Regional Center for Counter Terrorism, showed similar consensus regarding the elements necessary in constituting cyberterrorism – motivation, effect, target, method and domain (Ahmad et al. 2012). Regarding the motivation of the perpetrators to instil fear and panic, a study by the research team led by Backhaus et al. (2020) found that the negative emotions experienced by people as a result of a cyberattack do not differ from the emotions triggered by a non-cyber terrorist attack. In addition, the team of researchers confirmed their hypothesis that these emotional responses are not based on whether or not there are any casualties (Backhaus et al. 2020), thus highlighting that in cyberterrorism, the harm to people and property, not lethality, may be a sufficient element for a cybercrime to qualify as an act of cyberterrorism.

The adapted cyberterrorism model: searching for a consensus

When it comes to cyberterrorism, motivation (the reason driving the perpetrators to commit certain acts) and intention (the desired consequences of committing an act) are both a psychological element on which most scholars seem to agree. Some of them derive it from the concept of terrorism. Egloff (2021) argues that the intent in cases of terrorism, and by extension cyberterrorism, is to cause terror to multiple targets. At the same time, he notes that the motivation is to achieve political goals. In their study about the motivations behind cyberterrorist attacks, Yunos and Sulaman (2017, 8) expand this notion, claiming that 'several attributes can be associated with motivation, amongst which are political, economic, social, and ideological.'

However, Tilly (2004, 7) cautions against relying too much on intent as a factor in a cyberterrorism definition as 'solid evidence on intentions and motivations rarely becomes available for collective violence.' Egloff (2021) views this as a valid, but insufficient reason why definitions should exclude intent. The reasoning behind the approach adopted in this paper is an amalgamation of both these perspectives. Intent and motivation are indeed an integral part of any model on terrorism, and cyberterrorism by extension, but the sometimes high level of uncertainty behind a perpetrator's intent, and mostly their motivation, in cyberspace, call for a more pragmatic assessment of whether a case is indeed cyberterrorism or not. This pragmatic approach requires a closer look at the information that is known about a specific case, such as the target, the method and the context of the attack, as they all may contain clues for both the intent and the motivation of the perpetrator.

Therefore, aside from motivation, we explored whether there is a scholarly consensus on the other elements of cyberterrorism, as described in the literature. To do so we created a dataset of 100 academic articles on the topic of 'cyberterrorism' that were published between 1997 and 2021 in 78 peer-reviewed journals and were identified through Google Scholar in a consecutive order until reaching the sample of 100 articles. We coded whether scholars mention common features that appear in the concept of 'terrorism', such as whether the act seeks to induce feelings of fear/panic in the victim(s) (intent), whether destruction of property or the threat of such is a necessary component, whether there should be an actual death caused or a threat of killing/violence/coercion, and/or indicating intent to 'influence' (Terzi 2019). This model is built after Terzi's (2019, 226), which includes the elements of 'cause, instrument, aim and intent'. Since political motivation was a widely agreed-upon element in previous studies, it was not included in the results of our coding, in which we searched for scholarly consensus (Table 1). A note about the distinguishable differences between these categories is also in order. First, inducing fear/panic pertains to the intentional and sought effect of inflicting emotional distress on the victims. It overlaps to some

Table 1. Scholarly agreement about some elements of the cyberterrorism definition.

Element	Mentioned	Not mentioned
Inducing fear/panic (intent)	59% (N = 59)	41% (N = 41)
Unlawful possession, handling, use and/or destruction of physical and/or digital property	51% (N = 51)	49% (N = 49)
Death/harm/coercion of people	56% (N = 56)	44% (N = 44)

extent with the third category of the death/harm/coercion of people, as emotional distress is indeed harmful, but in the third category it is the physical effects which are taken into consideration, as opposed to the emotional/mental ones. Second, the unlawful possession, handling, use and/or destruction of physical and/or digital property should be distinguished from the third category, and harm in particular, where there are direct consequences for the individual, as opposed to indirect harm, caused by the unlawful possession, handling, use and/or destruction of physical and/or digital property. There is some overlap between the latter and the category of fear/panic, as the events envisioned in the previous sentence can inevitably cause some fear and panic, but the emphasis of the first category of elements falls on the intention of the perpetrator to cause fear/panic on purpose, as opposed to this being a natural result from the elements in the second category (e.g. destruction of physical and/or digital property).

As intent and motivation are difficult to determine in cyberspace, we have examined one additional element that was highlighted by practitioners which can also indicate possible intent – the scale of the act. Tyler Shields, the CMO of JupiterOne, a cyber asset management company, says: 'Ransomware isn't something that can be labelled with a broad stroke … If someone attacked a small dental office with ransomware, it's most certainly not an act of terrorism. However, if they take down critical infrastructure such as an oil pipeline or water system then it is. It's more about the target of the attack and the meaning and intention than it is about the type of attack' (*Security Magazine* 2021). A group of researchers from US-based Sandia National Laboratories, a subsidiary of the Lockheed Martin Corporation, connect the figure of the cyberterrorist with their intent to cause a 'large-scale disruption of computer networks' (Mateski et al. 2012, 11). TechTarget, a network offering technology-related online content, links cyberterrorism to the presence of 'significant attacks', as interpreted by the US Center for Strategic and International Studies (2022). According to the latter, this includes government units, defence companies, high-profile tech companies and crimes with financial losses higher than $1 million (Sheldon and Hanna 2022). A report by the Cambridge Centre for Risk Studies underlines the need for a scale of personal and property damage in order to assess a cyberterrorist event (Evan et al. 2017).

Considering the previous studies and literature on the topic of cyberterrorism, we have built a model assessing when ransomware constitutes as an act of cyberterrorism, based on elements agreed upon by scholars and practitioners. However, a few clarifications are in order. It seems that there is a consensus in the field pertaining to intent (inducing fear/terror) and motivation (political or ideological, broadly defined) as necessary factors in the definition of cyberterrorism, despite different nuances. As previously mentioned though, they are both also inherently psychological phenomena, difficult to prove in the courtroom even in cases of crimes committed in the physical space. This task becomes even more complicated for crimes in cyberspace, where the perpetrator may never be identified, particularly if they are a part of an organised group. The motivation of the offender(s) involved in ransomware may also range from financial gains to political and ideological ambitions and goals, mapped by different entities. When ransomware is part of a cyberterrorism case, however, there needs to be 'a wider psychological impact beyond the immediate victims' in terms of the intent (Richards 2014, 221).

Richards (2014) also highlights an issue related to both terrorism and cyberterrorism that is still ongoing today. In particular, he calls the effort to conclude what falls within the concept of terrorism 'extremely difficult … because it is hard to know what the intent or purpose is behind the act of violence' (p. 230). Regardless, he strongly encourages the scholarly field to continue pursuing this task, as not doing so would be 'an abdication of academic responsibility, not just because it would leave terrorism studies without a sufficient conceptual and theoretical foundation but because it would leave policy-makers bereft of academic input to inform their own endeavours in defining the term' (p. 219).

Considering intent and motivation as building blocks in the definition, although difficult to prove, some other elements which can signify the offender's motivation should be also kept in mind – acts with large-scale effects, with the intent of provoking fear and panic among a certain population, as a consequence of killing, harming, coercing people, and unlawfully handling, using and destroying physical/digital property. Some of these elements can mutually amplify each other (e.g. scale and harm), so it must be underscored that these categories of elements are not existing in vacuum. They influence each other and the distinction between them is predominantly theoretical, as in practice their effects should be considered altogether. Lastly, it needs to be noted that actual acts which were carried out should not only be the ones considered as acts of cyberterrorism, but also credible threats that are made by fulfilling the conditions in the adapted model we propose, illustrated in Figure 1.

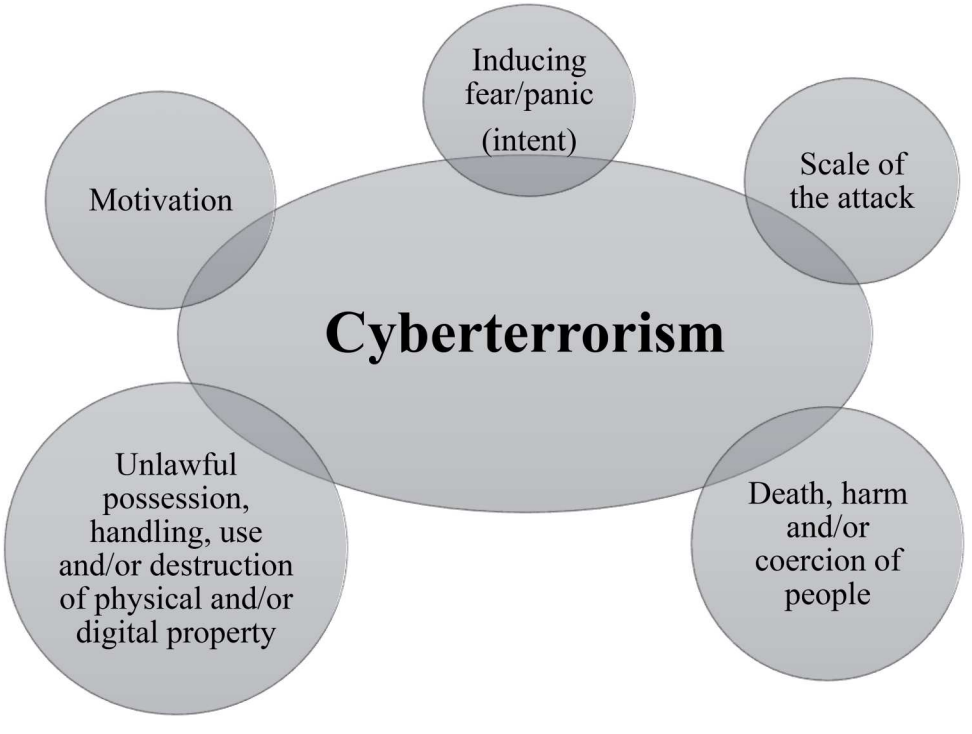

Figure 1. Adapted model for identifying ransomware cases as acts of cyberterrorism.

The case of colonial pipeline

There were 57 years of ceaseless operation before Colonial Pipeline's first complete shutdown in response to a ransomware attack (Reeder and Hall 2021). A group of hackers, identified as DarkSide, a Russian hacking group, gained access to Colonial Pipeline's virtual system on 29 April 2021. The company failed to require a two-step verification protection on personal computers/emails, allowing the hackers to sign on after attaining a worker's password (Turton and Mehrotra 2021).

On 6 May 2021, at 5am, an operator in Colonial Pipeline's control room found a message on a computer monitor: a demand for an undisclosed amount in the millions (Reeder and Hall 2021). According to the CEO Joseph Blount, the 'shutdown process' commenced at 5:55am and by 6:10am the 5,500 miles of oil pipeline had ceased operations (Wilkie 2021). Blount stated that the same day as the attack against the company, responsible for critical infrastructure, he contacted the FBI in Georgia and California, as well as prosecutors in California and the US Capital (Perez et al. 2021). The next day, 7 June 2021, Laurel Beeler, a Magistrate Judge of San Francisco, signed a warrant for the seizure of property for 21 June 2021 (US Department of Justice 2021) to begin the process of retrieving the estimated 4.4 million in cryptocurrency that Blount would pay to the hackers' account several days after communication began (Smith 2021). Much of the information about the attack was gleaned by the US Senate Committee on Homeland Security and Governmental Affairs' interview with Joseph Blount on 8 June 2021. Sen. Gary Peters, chairman of the committee, stated to Blount: 'I am alarmed that this breach ever occurred in the first place and that communities from Texas to New York suffered as a result' (Owen and Cathey 2021). It was this investigation that brought to light how the hackers were able to access the company's infrastructure so easily.

Meanwhile, resulting from the cyberattack and its large-scale consequences, on 3 June 2021, the Ransomware and Digital Extortion Task Force was formulated by the US Department of Justice (Reeder and Hall 2021). The task force was able to locate and retrieve 63 of 75 bitcoins paid to DarkSide, worth an estimated $2 million. Although Colonial Pipeline was fast to initiate communication with the correct authorities, they did not give a full description of technical events to the Department of Homeland Security (Ellis 2021). The entirety of Colonial Pipeline's distribution system was shut down for days after the attack. One week after the first contact, Colonial Pipeline was able to disconnect DarkSide from its system by dismantling payment and communication operations, as well as its operational technology network (Jasper 2021).

Colonial Pipeline, responsible for approximately 45 per cent of the refined oil products supply of the US East Coast, was able to reinstate operations on 13 May 2021, in full, bringing relief to frantic customers along the entire eastern seaboard of the country (Turton and Mehrotra 2021). The company moved forward, hiring on 12 May 2021 Drago, an industrial cybersecurity protection firm, and Black Hills Information for cybersecurity prevention. It took Colonial Pipeline several more months, until 16 August 2021, when the company notified employees, past and present, as well as their family members, that they have also been victims of the data breach. An estimated 5,810 people were potentially affected (Fung 2021).

The Colonial hack had lasting costs psychologically, organisationally and financially. For weeks in May 2021, the evening news broadcasted images of panicking consumers

rushing petrol stations in response to the Colonial Pipeline shutdown. Photos of hand-made signs warning of petrol outages at pumps frequently appeared on social media. The 'panic buying' (Nawaz 2021) triggered by this cyberattack is another example of the magnitude of psychological effects that led to an even more scarce petrol supply. Georgia's governor suspended the petrol tax in the state in an effort to help with the increasing prices and North Carolina's governor declared a state of emergency (Rapier 2021). Three more states were also seriously affected by the ransomware attack and the petrol outages – Virginia, South Carolina and Florida.

The US Department of Transportation, in response to the resource rush, delivered a temporary emergency order which permitted truckers to ignore safety protocols and work overtime in an attempt to increase petrol deliveries (Ainsley and Collier 2021). It was estimated that half a billion gallons, or 12,500 tanker deliveries were postponed by the event (Popken 2021). The south-eastern region of the US saw one the largest increases in fuel costs, which were ultimately passed down to the consumer.

The case of JBS

It was reported that in 2017 and 2018, JBS employees spoke of a security audit of the company that identified potential breach points in the design of their system and suggested implementing endpoint detection tools (Gallagher and Alyza 2021). Similarly, information was given that implicated the company's leadership in overlooking the audit results and dismissing them as too costly. This audit was initiated by the US branch of the company, but the complexity of the system could also have an impact on international operations as well (Gallagher and Alyza 2021). On 31 May 2021, JBS Brazil announced that they had been a victim of cyber ransom, but were able to maintain operations in several facilities. However, plants in Australia and the USA were both shuttered for at least one day (Collier 2021; Durbin 2021).

Similarly to the Colonial Pipeline attack, the majority of detail about the JBS ransomware case came from the CEO's willingness to report it. Andre Nogueria shared what he had learnt of the attack at 5am on 30 May 2021, a Sunday. Another similarity to the Colonial Pipeline case is that the workers found the ransom communication and then reported it up the chain (Bunge 2021). The company quickened their defensive measures by halting systems at risk by contacting the FBI and security experts immediately. The team at JBS was able to ensure that encrypted data had not been breached within the same day (Crowe 2021). At 7pm on 1 June 2021, JBS paid 301 bitcoins or the equivalent of $11 million to the hackers to mitigate the threat, as workers feared that other systems may be at risk. The day before, 31 May, was spent isolating and reopening shipping systems to transport JBS products. Mr Nogueria announced to the public that they were confident that operations would resume as normal the next day.

It was early June when the FBI identified REvil as the culprit (Durbin 2021). Regarding the ransom payment, Mr Nogueira told the *Wall Street Journal* that 'It was very painful to pay the criminals, but we did the right thing for our customers' (Bunge 2021). As of the beginning of 2022, the ransom amount has still not been recovered by the authorities.

JBS was able to minimise halts to production through back-up data and identifying functions that can be executed offline, which saved the meat industry from an even bigger supply-chain disruption. Regardless, there were still financial effects for the

farmers, distributors and consumers. Farmers in the US rushed to contact alternative manufacturers, but ultimately were operating at a loss, restaurants felt a price hike as high as 25 per cent for certain types of meat, and customers experienced a temporary increase of cost (Crowe 2021). Disruptions in the operations of a production giant such as JBS hits farmers particularly hard when there is a lack of demand for animals (Rosenbaum 2021). Additionally, workers lost shifts as production was halted to protect food safety, which could not be guaranteed without functioning technology responsible for the quality management systems at JBS (Fontanazza 2021).

The case of the 2022 wiperware attacks against Ukraine

On 24 February, Russia launched a military operation by land, sea and air against Ukraine which was labelled by some news outlets as 'the biggest attack by one state against another in Europe since World War II' (Al-Jazeera 2022). While this drastic move by the Kremlin caught leaders and analysts by surprise, the tension between Russia and Ukraine had only been rising over the previous decade, particularly with the annexation of Crimea in 2014. This act was also accompanied by cyberattacks against Ukraine, which intensified even more in the beginning of 2022 (European Parliamentary Research Service 2022). January 2022 was the beginning of a cluster of wiperware attacks – a type of pseudo-ransomware, which is a cyberattack disguised as ransomware, but instead of actually giving the victim a chance to recover the files after paying the ransom, it actually seeks to destroy data in the adversary's computer system. Despite some definitional differences, as noted previously, we still consider wiperware a form of ransomware, due to both sharing many common characteristics and the fact that in the eyes of the victim, it is possible to retrieve the locked information if a ransom is paid. Therefore, it could be argued that wiperware is a notably more dangerous form of ransomware, as the victim can suffer even more damages if the ransom is paid – first, the amount of money paid for the ransom (if paid), and second the loss of the data.

These attacks were used against Ukrainian information systems, and Microsoft (2022) suggests that Russia had been preparing for increased cyberattacks, in particular launching a cluster of wiperware, since March 2021. The first wiperware – WhisperGate – was deployed against the Ukrainian government systems on 13 January 2022. This attack was followed by HermeticWiper, IssacWiper and CaddyWiper.

WhisperGate was identified by Microsoft on the day of the attack, which was noted in conjunction with attacks on government websites in the days prior to the event. A bitcoin ransom note was left requiring $10,000 with a transfer of accounts to follow the next day (Avertium 2022). The ransom message stated: 'Ukrainian! All your personal data was uploaded to the public network. All data on the computer is destroyed, it is impossible to restore it. All information about you has become public, be afraid and expect the worst. This is for your past, present and future' (Krebs and Kwon 2022). There was evidence of additional meddling on government sites on the morning of the 14th. More wiperware was launched against Ukraine in the following months.

Two weeks after the WhisperGate ransomware was identified, on 23 February 2022, HermeticWiper was reported by ESET Digital Security. The company Hermetica Digital Ltd was linked to the attack via a signed certificate. The company dated back to April 2021. The message left read thus: 'Thank you for your vote! All your files, documents,

photos, videos, databases etc. have been successfully encrypted … Do not try to decrypt then by yourself – it's impossible! It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instructions. To prove that we have a decryption send us any encrypted file … and we'll send you it back being decrypted. This is our guarantee' (Andres Guerrero-Saade and van Amerongen 2022). Resembling WhisperGate, HermeticWiper was also identified as a 'decoy-ransomware', which does not provide a data recovery mechanism, but just destroys the data.

A third kind of wiperware – IssacWiper – was identified one day after HermeticWiper on 24 February 2022. It had a timestamp dating back to the previous October. A revised version of IssacWiper was deployed on 25 February 2022, which may indicate that the ransomware was not working according to design (ESET Research 2022a). CaddyWiper followed IssacWiper on 14 March 2022. Each malware appears to have had different authors, with CaddyWiper being the least destructive (Malware Bytes Labs 2022). Similarly to the other attacks, there is evidence that CaddyWiper had infiltrated Ukrainian systems before the time of the deployment (ESET Research 2022b). Ukraine's Vice Prime Minister Mykhailo Fedorov responded with an IT Army recruiting international support against Russian cyberattacks (Zakrzewski 2022).

Applying the model to the cases

Colonial Pipeline

Before discussing how our adapted model applies to the Colonial Pipeline case, it needs to be noted that all ransomware cases may include some element of fear/panic, as the act itself represents a threat to a certain individual or a group, in case the conditions set by the perpetrator are not met. That said, in the case of Colonial Pipeline, the intent (fear/panic) element had an even broader meaning, as the employees who first saw the ransom demands were not the only ones who experienced these emotions, but also the numerous consumers whose daily lives were disrupted because of the petrol shortages. Evidence of this are the many consumers who rushed to petrol stations to fill their tanks, as this ultimately exacerbated deficiencies. While the motivation of the perpetrator cannot be clearly determined, as in many other cyberattack cases, the scale of the damages, along with the nature of the target itself, can signal that the motivation behind the acts was potentially not just financial.

The third element of our model – the requirement of death/harm or coercion – is fulfilled by the Colonial Pipeline case. Direct harm was caused to the company, whose operations were shut down, as well as to the employees whose personal data was stolen. The indirect effects of the attack that *must-have-been-anticipated* by the hackers spread even further to include consumers. This disruption to the consumer is also the main reason why the Colonial Pipeline attack qualifies as an act of cyberterrorism – coercion through affecting the supply of an essential resource for a substantial number of people in order to apply pressure on the victim to pay the ransom. The coercion to pay the ransom did not only include the expected significant consequences for the consumers but also the fear that the news of the ransomware case may weaken the company itself and force it to respond to serious questions by various stakeholders, including the US government. The hackers knew or should have known that by affecting the operations of such

an influential company there would have to be massive and negative consequences for many people unaffiliated with Colonial Pipeline, which also reveals some information about the potential intent of the attackers. At the same time, it is logical to assume that the hackers had an idea of the larger effects their actions would have on US consumers, based on the amount of the required ransom.

The next component of our model – the unlawful possession, handling, use and/or destruction of physical and/or digital property – is also represented by the Colonial Pipeline case. To begin with, there was an unlawful possession of the company's data, including the personal information of its employees. Next, the hackers handled the data in a manner that deprived the company from having access to it. The security infrastructure of the company was damaged. The first and the third element of the confidentiality-integrity-availability (CIA) triad were particularly compromised through the ransomware attack. While these consequences occurred in cyberspace, they had expressions in physical space as well when the petrol supply for various states was disrupted.

When the last component of our model – scale – is considered in the case of Colonial Pipeline, it could be considered satisfied as well. The scale of the attack has both material and psychological dimensions. While estimates of the second case's impact would be difficult, those of the first case can, to some extent, be measured quantitatively. As mentioned previously, the company is responsible for 45 per cent of the refined oil products supply of the US East Coast and the disruptions had a very significant impact, particularly in the ongoing COVID-19 pandemic. Moreover, the compromised personal information of nearly 6,000 employees of Colonial Pipeline, as a result of the data breach, is a serious issue that needs to be taken into consideration when discussing the scale of the event. The impact of the product disruption can also be measured in direct damages – $4.4 million paid in ransom, and the indirect damages that can potentially come from various lawsuits against the company for not providing sufficient cybersecurity for the pipeline and thus failing to supply nearly 11,000 US East Coast petrol stations (Ryskamp 2021).

JBS

There are various differences but also similarities between the case of Colonial Pipeline and the case of JBS. In terms of intent (inducing fear/panic), the aforementioned conclusion that all ransomware cases incorporate some level of fear/panic is also valid. However, JBS, contrary to Colonial Pipeline, had more protective layers (e.g. back-up data and an overall better emergency response), despite earlier reports of poor cybersecurity. The level of fear/panic was not as considerable as in the Colonial Pipeline case, but it was still relatively high, especially in light of the fact that had the company failed to respond so quickly to the attack, the consequences could have been much more substantial. Moreover, it should be noted that the operations of the company were spread across more than one continent, which makes the potential for damages (and fear of such) much higher. Regarding the motivation behind the attacks, in the case of JBS, similarly to that of Colonial Pipeline, the scale of the attack and the nature of the target can signal aims beyond pure financial gains.

The attack on JBS did not result in death, but caused harm to a significant number of people – JBS employees, farmers and end-user customers. Anticipating the effects of a

potential halt of operations, JBS felt pressure and coercion to pay the ransom of approximately $11 million. Farmers also suffered financial damages, having to sell animals to JBS competitors at a loss. The decreased meat supply resulted in a 25 per cent price increase.

The third component in our model – the unlawful possession, handling, use and/or destruction of physical and/or digital property – is also present in the JBS case. There was an unlawful possession of data by the attackers and a handling of the data that prevented the company from accessing it and using it. The digital consequences of the attack mirrored those in physical space by preventing the company from executing their main operations – the production of meat, including the necessary adherence to food safety protocols, which is a task that has been largely automated and done by computers.

The scale of the impact of the ransomware attack against JBS was much smaller than the one against Colonial Pipeline, but it should be kept in mind that despite the prior concerns about the company's cybersecurity, JBS was more prepared to recover from its attack than Colonial Pipeline. Regardless, the disruptions were significant and more complex than the Colonial Pipeline attack, despite the operations being halted for only one day. The determination of whether or not an act of ransomware represents cyberterrorism should not be made based on the level of preparedness by the direct victim. Instead, the assessment should take into account the different groups of people affected by the attack and the size of the targeted unit – in this case a multinational company that was the second biggest supplier of meat and poultry in the US for 2021 (Statista 2021).

The wiperware attacks against Ukraine

Wiperware is by its nature coercive, as this specific form of ransomware often makes a demand that will ultimately have no effect upon the destruction of targeted data, as the data will be erased from the system regardless of whether the victim pays the ransom. However, the targeted entity has no knowledge of this, and views the attack as ransomware instead of wiperware. By targeting government systems and infrastructure, Russia initiated an operation intended to break down the will of the victim over time. Data destruction and disorganization serve as an attack on the country by creating long-term consequences, both material and non-material. Unlike the cases of JBS and Colonial Pipeline, the intent in this one was clear – to induce fear, terror and panic through politically-motivated actions, part of a bigger military, state-sponsored operation. The cluster of wiperware hit government websites, making services offered by them unavailable to citizens. Evidence shows also that at least one Ukrainian financial institution was also affected by the wiperware as well as a few government contractors. These actions represent the harmful, coercive tactic used against Ukrainians through the malware (Lyngaas 2022). As the request for ransom is only illusionary, as the attacker has no intent of recovering the data, the unlawful possession, handling, use and destruction of digital property of both the Ukrainian citizens and the government is evident. Combined with the physical threat of the large-scale attack ordered by Moscow, the premediated cyberattacks intended to cast additional doubt in Kyiv's ability to maintain order in the country by instilling fear and uncertainty in its citizens.

While it is difficult to estimate the scale of the impact the wiperware cluster launched by Russia had on Ukraine, cybersecurity analysts argue that Russia's goal might have been

to destroy critical infrastructure by multiple means (kinetic and cyber) and thus to 'cause chaos and increase mental stress on the enemy' (Revay 2022). In all cases, the series of wiperware attacks and their effects should be discussed in the political context of the relationship between the two countries, considering that the wiperware attacks occurred simultaneously with other cyber and kinetic coercive tactics. The details of this case satisfy all the conditions presented in our model and would therefore constitute an act of state-sponsored cyberterrorism, despite the lack of concrete numbers for the damages suffered by the government, the private sector and the number of affected citizens. In this case, the act should be labelled as state-sponsored cyberterrorism, as opposed to an act of war by Russia, due to the following reasons: 1) Russia never took responsibility for the attack by stating it was a state-sanctioned operation; and 2) the perpetrators, while connected to Russia, are not known to be official employees of the Russian government, and thus it cannot be claimed that this was an operation directly executed by the Kremlin, instead it was conducted by non-state actors.

Policy implications

Despite an increasing volume of scholarly studies dedicated to the topic of ransomware and cyberterrorism, there is still a notable lack of firm scholarly agreement on the defining elements of cyberterrorist acts. This inhibits the ability to provide a complete assessment of whether a ransomware case is also a cyberterrorism case, particularly at a time when the UN is negotiating a cybercrime treaty, and cyberterrorism should be an important topic within the overall focus of the treaty. Even if scholars can agree on a definition, it may not work for practitioners and policymakers, as the existence of some of the elements in the definition may be difficult to prove in practice. This is an area where our study tries to bridge the gap by implementing a more practical approach to intent and motivation by focusing on the scale, method and damages of the attack. On a national level, following the components proposed in this and earlier works, each government should assess the evidence for the intent and motivation of the perpetrator, what the minimum damages/victims/impact of the cyberattack would be, so that it can be considered an act of cyberterrorism. In the case of Colonial Pipeline, if the ransomware attack had been investigated as a case of cyberterrorism on federal level, a much more coordinated response by the US government might have prevented some of the negative consequences and relieved anxiety among the consumers in various US states. This is especially necessary as ransomware affects companies that have global operations, and harmonised international norms pertaining to ransomware and cyberterrorism will notably enhance a joint response to such events by governments, such as in the JBS case study. In the case of the wiperware attacks against Ukraine, it becomes even more evident that a more specific definition for cyberterrorism is necessary so that state-sponsored acts of cyberterrorism are categorised as such and a proper response is crafted.

The price for not better defining cyberterrorism at a national level will be to continue having political, as opposed to evidence-driven, determinations on whether a case constitutes cyberterrorism. Dealing with issues on a case-by-case basis opens room for unfair treatment, the potential for diplomatic conflicts, and even interstate economic and military measures. The benefit of defining cyberterrorism and whether ransomware can be categorised as such presents various opportunities for states to also create a

consistent approach to prosecuting these crimes, to notice common patterns among them, to create and use the correct capabilities to prevent them, to mitigate their damages and to deter future attacks.

Some non-state actors, such as the European Union and NATO, should also attempt to follow more specific criteria for defining cyberterrorism, after these conversations take place within national governments first and some patterns and basis for negotiations emerge. Following this bottom-up approach may help the negotiations at the UN as well at a later point. On an international level, the price for not more clearly defining cyberterrorism can lead to a lack of a coordinated response to ransomware attacks, which are only expected to increase. A survey of more than 3,500 CIOs, CTOs and CISOs (VMware 2021) showed that compared to the first months of 2020, there was a 900 per cent rise in the number of ransomware attacks in 2021 (Winder 2021). This study also shows that adopting a clear definition, based on the recommended pillars, can also present an opportunity for a coordinated response in cyberterrorism cases, particularly in which the damages spread across borders. Lastly, a common definition for cyberterrorism can also resolve some of the issues which exist between insurance companies offering cyber insurance to their clients in cases in which there is a legal dispute about what risks are covered and what are not, as exemplified in the Mondelez vs Zurich case (Tatar et al. 2021). When it comes to international humanitarian law and its application to cyberspace in the case of significant cyberattacks, the definitional (Gisel et al. 2020; Lin 2012) and the jurisdictional issues arising as hindrances (Pipyros et al. 2016) can also be eliminated to a large extent if a definition of cyberterrorism is to be accepted. In the words of Shavit Matias, the first Deputy Attorney General of Israel for International Law, 'cyberterrorism, cyberwarfare and cybercrime can hit national security as well as other interests of a state from places where, without international cooperation, a state has little or no control, nor will it have, without international cooperation, sufficient ability to defend or protect itself' (p. 131).

All of these considerations should be noted during the UN negotiations for a cybercrime treaty so that the issue of ransomware and cyberterrorism is addressed. When discussing this topic both at the UN level and the scholarly one, three other implications should be emphasised as well. First, defining cyberterrorism too broadly hides the risks of including not only many small cases of ransomware attacks, but also other cybercrimes which are not so significant in scale. Second, defining cyberterrorism too narrowly also hides risks, as the definition may exclude certain acts which would otherwise constitute acts of cyberterrorism. Thus, it is crucial that a careful balance is maintained. Our model strives to satisfy the requirements for some more concrete aspects in the definition, but at the same time allows for an evaluation of the cases in their entirety.

Limitations

The findings from this study need to be considered within the context of various limitations. First, the topic of terrorism, and specifically cyberterrorism, presents a high number of unresolved issues in the scholarship, thus finding agreed-upon elements of the definition was a challenging task that resulted in basing our model on a fragile fact-based consensus. Second, another very important issue pertains to the role of intent and motivation in models of terrorism and cyberterrorism. With this idea in

mind, we proposed some additional elements related to the context of the cyberattack, which may contribute to a slightly more enhanced understanding of intent and motivation in cases in which there is a notable lack of information regarding these components. Lastly, while we do not have the ambition to conclusively resolve any definitional debates, with this study we attempt to at least make a step towards a hopefully more unifying academic perspective on cyberterrorism, applicable to real-life cases. Our goal was to continue the effort to connect scholarly concepts to their possible application in practice, despite challenges presented by the unique components of each case.

Conclusion

In an increasingly complex world, more and more fields of study require the combined efforts of experts, particularly when policymakers have the complicated task to negotiate a comprehensive cybercrime treaty at the UN level. The issue of ransomware and cyberterrorism is no exception to this and only an interdisciplinary mindset can resolve the problem. Professionals from disciplines such as political science, international relations, criminal justice, criminology, law, psychology, economics and business should engage in a joint endeavour to provide a framework for the analysis of a phenomenon which is becoming over time more frequent and no less threatening to businesses, governments and people. To contribute to understanding and alleviating this issue, we drew on scholarship from various fields in an effort to suggest a pragmatic approach to an abstractly defined topic. We proposed an adapted model for the assessment of ransomware cases, as potential cyberterrorism acts. We then used the model and applied it to three recent ransomware cases with significant consequences. During the discussion of the extent to which they fit the criteria in our model, the need to have a more concrete measurement for the required threshold of each element became apparent. In light of this finding and the seriousness and difficulty of the issue itself, the authors of this paper hope that more attention will be paid by scholars, policymakers and practitioners to these questions during the UN negotiations for a cybercrime treaty and even beyond this.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Dr. Lora Pitman holds a PhD in International Studies from Old Dominion University, a Master's in Humanities from the same institution, and a Master of Laws degree from Sofia University, Bulgaria. As a subject matter expert, Dr. Pitman worked on different projects on disinformation, sponsored by NATO and by the U.S. Department of State. She was also a contributor to international events organized by the Tactics Institute for Security & Counter Terrorism (UK), the Legal Innovation Lab Wales (UK), NATO-ACT and NATO Innovation Hub. She has published multiple peer-reviewed articles and book chapters with a focus on international security and cybersecurity. Her publications appear in the International Journal of Cyber Criminology, the International Journal of Intelligence & Cybercrime, the International Journal of Criminal Justice Sciences, the Journal of White-Collar and Corporate Crime, the Journal of Criminal Justice Studies, the Journal of Simulation Engineering, the

Encyclopedia of Global Security Studies, and in various NATO Science for Peace Series volumes. She is also a co-editor of the NATO-issued book *Advances in Defence Analysis, Concept Development and Experimentation: Innovation for the Future*.

Wendy J. Crosier graduated with honors from the University of Maine's Political Science Program with a minor in Ecology and Environmental Science. Her interest in renewable energy, policy and national security has led to an internship in Governor Mills' office and a research fellowship through the University of Maine. The Department of Energy has selected Crosier for the Clean Energy Innovators Fellowship - – administered by the Oak Ridge Institute, amongst 18 other participants nationally.

ORCID

Lora Pitman http://orcid.org/0000-0002-5547-0371

References

Ahmad, R., Z. Yunos, S. Sahib, and M. Yusoff. 2012. "Perception on Cyber Terrorism: A Focus Group Discussion Approach." *Journal of Information Security* 3 (03): 231–237. https://doi.org/10.4236/jis.2012.33029.

Ainsley, J., and K. Collier. 2021. "Colonial Pipeline Paid Ransomware Hackers $5 Million, U.S. Official Says." *NBC News*, May 13. https://www.nbcnews.com/tech/security/colonial-pipeline-paid-ransomware-hackers-5-million-u-s-official-n1267286

Al-Jazeera. 2022. "Russian Forces Launch Full-Scale Invasion of Ukraine." February 24. https://www.aljazeera.com/news/2022/2/24/putin-orders-military-operations-in-eastern-ukraine-as-un-meets

Andres Guerrero-Saade, J., and M. van Amerongen. 2022. "AcidRain | A Modem Wiper Rains Down on Europe." SentinelOne. Sentinel LABS. March 31. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Avertium. 2022. "How WhisperGate Affects the U.S. and Ukraine." February 1. https://www.avertium.com/resources/threat-reports/how-whispergate-affects-the-u.s.-and-ukraine

Backhaus, S., M. L. Gross, I. Waismel-Manor, H. Cohen, and D. Canetti. 2020. "A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure." *Cyberpsychology, Behavior, and Social Networking* 23 (9): 595–603. https://doi.org/10.1089/cyber.2019.0692.

Beaman, C., A. Barkworth, T. D. Akande, S. Hakak, and M. K. Khan. 2021. "Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions." *Computers and Security* 111: 102490. https://doi.org/10.1016/j.cose.2021.102490

Braue, D. 2021. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031." *Cybercrime Magazine*, June 3. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Bunge, J. 2021. "JBS Paid $11 Million to Resolve Ransomware Attack." *The Wall Street Journal*, 9 June.

Center for Strategic and International Studies. 2022. "Significant Cyber Incidents." https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Collier, K. 2021. "Meat Supplier JBS Paid Ransomware Hackers $11 Million." *CNBS*, June 9. https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html

Connolly, L. Y., and D. S. Wall. 2019. "The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures." *Computers and Security* 87: 101568. https://doi.org/10.1016/j.cose.2019.101568.

Crowe, D. 2021. "Ransomware Attack Roiled Meat Giant JBS, Then Spilled Over to Farmers and Restaurants." *Small Medium Business News Network*, June 11. https://smbnn.com/news/ransomware-attack-roiled-meat-giant-jbs-then-spilled-over-to-farmers-and-restaurants/

Desouza, K. C., and T. Hensgen. 2003. "Semiotic Emergent Framework to Address the Reality of Cyberterrorism." *Technological Forecasting and Social Change* 70 (4): 385–396. https://doi.org/10.1016/S0040-1625(03)00003-9.

Dogrul, M., A. Aslan, and E. Celik. 2011. "Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism." In *2011 3rd international conference on cyber conflict*, pp. 1–15. IEEE. June.https://ccdcoe.org/uploads/2018/10/DevelopingAnInternationalCooperation-Dogrul-Aslan-Celik.pdf

Durbin, D. A. 2021. "Meat Company JBS Confirms it Paid $11M Ransom in Cyberattack." *AP NEWS*, June 9. https://apnews.com/article/europe-hacking-technology-business-353f8dea34bbbba15207ff350e7a2f0f

Egloff, F. J. 2021. "Intentions and Cyberterrorism." In *The Oxford Handbook of Cyber Security*, edited by P. Cornish, 187–200. Oxford: Oxford University Press.

Ellis, M. J. 2021. "Time for a National Cyber Incident Disclosure Requirement." The Heritage Foundation. https://www.heritage.org/technology/report/time-national-cyber-incident-disclosure-requirement

Embar-Seddon, A. 2002. "Cyberterrorism: Are we under Siege?" *American Behavioral Scientist* 45 (6): 1033–1043.

Enders, W., and T. Sandler. 2011. *The Political Economy of Terrorism*. New York, NY: Cambridge University Press.

ESET Research. 2022a. "IsaacWiper and HermeticWizard: New Wiper and Worm Targeting Ukraine." March 1. WeLiveSecurity. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

ESET Research. 2022b. "CaddyWiper: New Wiper Malware Discovered in Ukraine." WeLiveSecurity. March 14. https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

European Parliamentary Research Service. 2022. *Cyberattacks Timeline*. Epthinktank. June 21. https://epthinktank.eu/2022/06/21/russias-war-on-ukraine-timeline-of-cyber-attacks/cyberattaks-timeline/

Evan, T., E. Leverett, S. J. Ruffle, A. W. Coburn, J. Bourdeau, R. Gunaratna, and D. Ralph. 2017. *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge, UK: Cambridge Centre for Risk Studies.

Fontanazza, M. 2021. "As Cyber Threats Evolve, Can Food Companies Keep Up?" June 16. https://foodsafetytech.com/tag/software/

Fung, B. 2021. "Colonial Pipeline Says Ransomware Attack Also led to Personal Information Being Stolen." *CNN*, August 16. https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html

Furnell, S. M., and M. J. Warren. 1999. "Computer Hacking and Cyber Terrorism: The Real Threats in the new Millennium?" *Computers and Security* 18 (1): 28–34. https://doi.org/10.1016/S0167-4048(99)80006-6.

Gallagher, R., and S. Alyza. 2021. "JBS Rebuffed Call to Boost Cyber Spending, Ex-Employees Say." *Bloomberg.Com*, June 8. https://www.bloomberg.com/news/articles/2021-06-08/jbs-rebuffed-call-to-boost-cyber-spending-ex-employees-say

Gisel, L., T. Rodenhäuser, and K. Dörmann. 2020. "Twenty Years on: International Humanitarian law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts." *International Review of the Red Cross* 102 (913): 287–334. https://doi.org/10.1017/S1816383120000387

IBM. 2023. "What is Ransomware?" https://www.ibm.com/topics/ransomware.

Jasper, S. 2021. "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack." The Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/

Johnson, J. 2021. "Internet Users in the World 2021." Statista. September 10. https://www.statista.com/statistics/617136/digital-population-worldwide/

Krebs, K., and J. Kwon. 2022. "Cyberattack Hits Ukraine Government Websites." *CNN*, January 14. https://www.cnn.com/2022/01/14/europe/ukraine-cyber-attack-government-intl/index.html

Lee, H., and K. S. Choi. 2021. "Interrelationship Between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework." *Victims and Offenders* 16 (3): 363–384. https://doi.org/10.1080/15564886.2020.1835764.

Legal Information Institute. 2020. "Intent." In *LII / Legal Information Institute*. Cornell Law School. https://www.law.cornell.edu/wex/intent

Lin, H. 2012. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94 (886): 515–531. https://doi.org/10.1017/S1816383112000811

Lyngaas, S. 2022. "Key Ukrainian Government Websites hit by Series of Cyberattacks." *CNN*, February.24. https://www.cnn.com/2022/02/23/europe/ukraine-government-commercial-organizations-data-wiping-hack/index.html

Macdonald, S., L. Jarvis, and S. M. Lavis. 2019. "Cyberterrorism Today? Findings from a Follow-on Survey of Researchers." *Studies in Conflict and Terrorism*. https://www.tandfonline.com/doi/full/10.10801057610X.2019.1696444

Malware Bytes Labs. 2022 "Double Header: IsaacWiper and CaddyWiper." Malwarebytes. Accessed October 20, 2022. https://www.malwarebytes.com/blog/threat-intelligence/2022/03/double-header-isaacwiper-and-caddywiper

Mateski, M., C. Trevino, C. Veitch, J. Michalski, J. Harris, S. Maruoka, and J. Frye. 2012. *Cyber Threat Metrics* (No. SAND2012-2427, 1039394; pp. SAND2012-2427, 1039394). Sandia National Laboratories. https://doi.org/10.2172/1039394

Microsoft. 2022. "An Overview of Russia's Cyberattack Activity in Ukraine", 21. Microsoft's Digital Security Unit. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

National Consortium for the Study of Terrorism and Responses to Terrorism (START). 2021. "GTD | Global Terrorism Database." https://www.start.umd.edu/gtd/

Nawaz, A. 2021. "'Panic Buying' is Driving the Fuel Shortage After Colonial Pipeline Hack, Expert Says." PBS NewsHour, 11 May. https://www.pbs.org/newshour/show/panic-buying-is-driving-the-fuel-shortage-after-colonial-pipeline-hack-expert-says

Nershi, K., and S. Grossman. 2023. "Assessing the Political Motivations Behind Ransomware Attacks." [Unpublished Manuscript]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507111

Owen, Q., and L. Cathey. 2021. "Colonial Pipeline CEO Faces Grilling About Ransomware Attack." *ABC News*, June 8. https://abcnews.go.com/Politics/colonial-pipeline-ceo-faces-grilling-ransomware-attack/story?id=78149117

Perez, E., Z. Cohen, and A. Marquardt. 2021. "US Recovers Millions in Cryptocurrency Paid to Ransomware Hackers." *CNN*, June 8. https://www.cnn.com/2021/06/07/politics/colonial-pipeline-ransomware-recovered/index.html

Pipyros, K., L. Mitrou, D. Gritzalis, and T. Apostolopoulos. 2016. "Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International law Rules in Cyber Warfare." *Information and Computer Security* 24 (1): 38–52. https://doi.org/10.1108/ICS-12-2014-0081

Plotnek, J. J., and J. Slay. 2021. "Cyber Terrorism: A Homogenized Taxonomy and Definition." *Computers and Security* 102: 102145. https://doi.org/10.1016/j.cose.2020.102145.

Popken, B. 2021. "Some gas Stations run dry After Motorists Rush to Fill Their Tanks as Pipeline Shutdown Continues." *NBC News*, May11. https://www.nbcnews.com/business/consumer/some-gas-stations-run-dry-motorists-rush-fill-their-tanks-n1266993

Rapier, R. 2021. "Panic Buying Is Causing Fuel Shortages Along the Colonial Pipeline Route." *Forbes*, May 11. https://www.forbes.com/sites/rrapier/2021/05/11/panic-buying-is-causing-gas-shortages-along-the-colonial-pipeline-route/

Reeder, J. R., and T. Hall. 2021. "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack." *The Cyber Defense Review* 6 (3): 15–40. https://www.jstor.org/stable/48631153

Revay, G. 2022. "An Overview of the Increasing Wiper Malware Threat | FortiGuard Labs." *Fortinet Blog*, April 28. https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

Richards, A. 2014. "Conceptualizing Terrorism." *Studies in Conflict and Terrorism* 37 (3): 213–236. https://doi.org/10.1080/1057610X.2014.872023

Rogers, M. 2003. "The Psychology of Cyber-Terrorism." In *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and its Consequences*, edited by A. Silke, 77–92. Hoboken: John Wiley & Sons, Ltd.

Rosenbaum, E. 2021. "JBS Cyberattack: June 2. https://www.cnbc.com/2021/06/02/from-gas-to-burgers-hackers-hit-consumers-where-it-hurts.html
Ryskamp, D. A. 2021. "In the Wake of a Ransomware Attack, Colonial Pipeline Now Faces Lawsuits." July 22. Expert Institute. https://www.expertinstitute.com/resources/insights/in-the-wake-of-a-ransomware-attack-colonial-pipeline-now-faces-lawsuits/
Security Magazine. 2021. "US to Treat Ransomware Like Terrorism." June 7. https://www.securitymagazine.com/articles/95366-us-to-treat-ransomware-like-terrorism
Sheldon, R., and Hanna, K. T. 2022. "What is Cyberterrorism?" TechTarget. January. https://www.techtarget.com/searchsecurity/definition/cyberterrorism
Smith, D. C. 2021. "Cybersecurity in the Energy Sector: Are we Really Prepared?" *Journal of Energy and Natural Resources Law* 39 (3): 265–270. https://www.tandfonline.com/doi/full/10.1080026468 11.2021.1943935
Statista. 2021. "Meat and Poultry Industry: Leading U.S. Companies, 2021." https://www.statista.com/statistics/264898/major-us-meat-and-poultry-companies-based-on-sales/
Tatar, U., B. Nussbaum, Y. Gokce, and O. F. Keskin. 2021. "Digital Force Majeure: The Mondelez Case, Insurance, and the (un) Certainty of Attribution in Cyberattacks." *Business Horizons* 64 (6): 775–785. https://doi.org/10.1016/j.bushor.2021.07.013.
Terzi, M. 2019. "E-Government and Cyber Terrorism: Conceptual Framework, Theoretical Discussions and Possible Solutions." *TESAM Akademi Dergisi* 6 (1): 213–247. https://doi.org/10.30626/tesamakademi.528011.
Thackrah, R. 1987. "Terrorism: A Definitional Problem." In *Contemporary Research on Terrorism*, edited by P. Wilkinson, and A. M. Stewart, 24–41. Aberdeen: Aberdeen University Press.
Tilly, C. 2004. "Terror, Terrorism, Terrorists." *Sociological Theory* 22 (1): 5–13. https://doi.org/10.1111/j.1467-9558.2004.00200.x
Turton, W., and K. Mehrotra. 2021. "Hackers Breached Colonial Pipeline Using Compromised Password." *Bloomberg*, June 4. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
United Nations General Assembly. 2020. "Resolution adopted by the General Assembly on 27 December 2019: 74/247." Countering the Use of Information and Communications.
US Department of Justice. 2021. "Warrant to Seize Property Subject to Forfeiture; Case No. 3:21-mj-70945-LB." https://www.justice.gov/opa/press-release/file/1402051/download
Uthoff, C. S. 2022. *Cyber Intelligence: Actors, Policies, and Practices*. Boulder, CO: Lynne Rienner Publishers, Incorporated.
VMware. 2021. *Global Security Insights Report 2021: Intelligence from the Global Cybersecurity Landscape*. VMware.
Warner, M. 2022. "Wiperware (Pseudo Ransomware) Used in Ukraine Cyberattacks." *Security Magazine*, March 2. https://www.securitymagazine.com/articles/97176-wiperware-pseudo-ransomware-used-in-ukraine-cyberattacks
Wilkie, C. 2021. Colonial Pipeline Paid $5 Million Ransom one day After Cyberattack, CEO Tells Senate. *CNBC*, June 8. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html
Winder, D. 2021. "The Five Most Important Ransomware Attacks of 2021." *Raconteur*, September 21. https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021/
Yunos, Z., and S. Sulaman. 2017. "Understanding Cyber Terrorism from Motivational Perspectives." *Journal of Information Warfare* 16 (4): 1–13. https://www.jstor.org/stable/26504114
Yuryna Connolly, L., D. S. Wall, M. Lang, and B. Oddson. 2020. "An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability." *Journal of Cybersecurity* 6 (1): 1–18. https://doi.org/10.1093/cybsec/tyaa023.
Zakrzewski, C. 2022. "4,000 Letters and Four Hours of Sleep: Ukrainian Leader Wages Digital War." *Washington Post*, March 30. https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/