2016 8th International Conference on Cyber Conflict
Cyber Power
N.Pissanidis, H.Rõigas, M.Veenendaal (Eds.)
2016 © NATO CCD COE Publications, Tallinn

The Cyber-Doom Effect: The Impact of Fear Appeals in the US Cyber Security Debate

Sean T. Lawson
Department of Communication
University of Utah
Salt Lake City, Utah, USA
sean.lawson@utah.edu

Haoran Yu
Department of Communication
University of Utah
Salt Lake City, Utah, USA

Sara K. Yeo
Department of Communication
University of Utah
Salt Lake City, Utah, USA
sara.yeo@utah.edu

Ethan Greene
Department of Communication
University of Utah
Salt Lake City, Utah, USA

Abstract: In the US cyber security debate, observers have noted there is a tendency for policymakers, military leaders, and media, among others, to use frightening ‘cyber-doom scenarios’ when making the case for action on cyber security (Dunn Cavelty, 2008, p. 2). Some have conjectured that these fictional cyber-doom scenarios, which exemplify ‘fear appeals’ in communication research, have the potential to undermine productive debate aimed at addressing genuine cyber security challenges (Valeriano and Ryan, 2015, pp. 7, 196). Yet, few have directly investigated the impacts of such rhetoric. Here, we assess the impact of cyber-doom scenarios by contextualising them within existing scholarship on the impact of fear appeals, a well-studied phenomenon in communication science. First, we review qualitative and quantitative research on fear appeals and their effects. Next, we report results of an empirical study that takes advantage of a nationally televised docudrama depicting a hypothetical cyber-doom scenario. Through content analysis of real-time responses to this docudrama on the social media platform Twitter, we assess the effects of this particular cyber-doom scenario on a large audience. Our findings suggest that the use of such extreme fear appeals in the absence of clearly communicated and efficacious information about how to respond to the threat is counterproductive, as they can lead to a sense of fatalism and demotivation to act. Thus, concerns that the use of cyber-doom scenarios could impair efforts to motivate appropriate policy responses to genuine cyber security threats are warranted.

Keywords: *cyber security, fear appeals, policy, discourse, communication*

1. INTRODUCTION

Concern about cyber security in the United States is growing, and there are ongoing public policy debates about how to respond to these challenges. How the United States chooses to respond will have profound impact on the future of the Internet, global civil rights, and international security. In this debate, observers have noted that there is a tendency for policymakers, expert commentators, and news media, among others, to use frightening 'cyber-doom scenarios' when making the case for action on cyber security (Dunn Cavelty, 2008, p. 2). These scenarios involve fictional tales of cyber attack resulting in mass destruction or even total economic and social collapse. Although they are not necessarily reflective of actual cyber threats facing the nation (Clapper, 2015), such scenarios are still common in US public policy discourse. Some have conjectured that these fictional cyber-doom scenarios, which are an example of 'fear appeals' in communication research, have the potential to undermine productive debate aimed at addressing genuine cyber security challenges (Valeriano & Maness, 2015, pp. 7, 196). Yet, few have directly investigated the impacts of such rhetoric.

Our paper assesses the impacts of cyber-doom scenarios by contextualising them within existing research findings on the impacts of fear appeals, a well-studied phenomenon in communication science. The goal of this paper is to provide an assessment of the degree to which cyber-doom scenarios could impair efforts to motivate appropriate policy responses to genuine cyber security threats. Assessments like those provided in 2015 by Director of National Intelligence (DNI) James R. Clapper indicate that the frightening rhetoric of cyber-doom scenarios is likely not an accurate reflection of real cyber threats. But can such rhetoric be dangerous in its own right?

In this essay, we first review qualitative and quantitative communication research on fear appeals and their effects. Then, we supplement our review by presenting preliminary results of an empirical study that takes advantage of a nationally televised docudrama depicting a hypothetical cyber-doom scenario. The fictional National Geographic Channel docudrama, *American Blackout*, aired in October 2013 and reached roughly 86 million American households (Seidman, 2015). Through content analysis of real-time responses to this docudrama on the social media platform Twitter, we assess the effects of this particular cyber-doom scenario on a large audience. Our findings suggest that the use of such extreme fear appeals in the absence of clearly communicated, obtainable, and efficacious information that viewers can use to help address the problem are counterproductive as they can lead to a sense of fatalism and de-motivation to act. Thus, concerns that the use of cyber-doom scenarios could impair efforts to motivate appropriate policy responses to genuine cyber security threats are warranted.

2. CYBER-DOOM SCENARIOS

For more than a decade, scholars have noted the use of cyber-doom scenarios by news media, expert commentators, and policymakers when talking about cyber security (Debrix, 2001; Weimann, 2005; 2008; Stohl, 2007; Conway, 2008; Dunn Cavelty, 2008, p. 2; Lawson, 2013a;

Valeriano & Maness, 2015). Perhaps the most influential recent use of a cyber-doom scenario by a policymaker occurred in 2012 when former US Secretary of Defense Leon Panetta warned about the possibility of what he termed 'cyber Pearl Harbor' in which coordinated cyber attacks wreak unprecedented destruction and chaos on the nation (Panetta, 2012). But Secretary Panetta was not the first or the last to contemplate such scenarios. In fact, the Pearl Harbor analogy dates back to 1991 when computer security expert and novelist Winn Schwartau warned about the threat of an 'electronic Pearl Harbor' (Schwartau, 1991). In the intervening years, analogies, metaphors, and scenarios positing cyber attacks with effects akin to military attacks, natural disasters, and nuclear weapons, have been common in the cyber security debate (Debrix, 2001; Conway, 2008; Clarke & Knake, 2010; Lawson, 2013a). In 1994, the influential futurist and theorist of the Information Age, Alvin Toffler, warned that terrorists could cyber attack the World Trade Centre and crash the US economy (Elias, 1994). In 1999, Fox News ran a documentary, *Dangers on the Internet Highway: Cyberterror*, warning of the possibility of catastrophic cyber attacks (Debrix, 2001; Conway, 2008). Eleven years later, CNN ran a televised war game called *Cyber.Shockwave*, which contemplated the implications of a massive cyber attack. That same year, Richard Clarke and Robert Knake began their book, *Cyber War*, with a tale of cyber attack crippling all US critical infrastructure and killing thousands in only a matter of minutes (Clarke & Knake, 2010). Others have speculated that cyber attacks could be as devastating as the 9/11 terrorist attacks (Martinez, 2012), the 2004 Indian Ocean tsunami (*The Atlantic*, 2010), Superstorm Sandy (Meyer, 2010), or the Fukushima nuclear disaster (Rothkopf, 2011). One former policymaker even warned that cyber attacks could pose a threat to all of global civilisation (Adhikari, 2009).

Cyber attacks against critical infrastructure are certainly not impossible, and we have seen examples of cyber attacks causing physical damage or destruction, the Stuxnet attack on Iranian nuclear facilities being perhaps the most prominent example thus far. Nonetheless, we have not seen attacks that come even close to causing the kinds of chaos and destruction contemplated in cyber-doom scenarios. Indeed, in the face of persistent warnings of cyber-doom, the US Director of National Intelligence told Congress twice in 2015 that such 'Cyber Armageddon' scenarios are not reflective of the real cyber threats facing the nation (Clapper, 2015). However, despite this clear rejection of cyber-doom scenarios by the nation's top intelligence official, warnings of a 'cyber Pearl Harbor' or 'cyber 9/11' persist among policymakers, commentators, and journalists. In February 2015, NSA Director, Admiral Michael Rogers, claimed that the hack of Sony Pictures the previous year constituted a 'cyber Pearl Harbor' of the kind Secretary Panetta had warned about in 2012 (Lyngaas, 2015). That same month, in a speech on cyber security, President Barack Obama urged listeners 'to imagine' cyber attacks that 'plunge cities into darkness' (Obama, 2015). In August 2015, Senator Susan Collins (R-ME) urged the passage of the Cybersecurity Information Sharing Act of 2015 'to reduce the likelihood of a cyber 9/11' (Collins, 2015). The legislation later passed (Pagliery, 2015). Finally, veteran journalist and television news personality Ted Koppel made headlines with his October 2015 book warning of the possibility of catastrophic cyber attacks on the power grid (Koppel, 2015). Indeed, since DNI Clapper's February 2015 statement to Congress, at least two dozen articles have appeared in major US newspapers warning of either 'cyber Pearl Harbor' or 'cyber 9/11'.[1] It is perhaps unsurprising, therefore, that cyber terrorism ranked second only to government

[1] Based on a search of LexisNexis Academic Universe database of 'US Newspapers' on 24 February 2016. Inclusion of broadcast transcripts, wire services, and online news sources not covered by LexisNexis would certainly turn up even more instances.

corruption in a survey of average Americans' fears in 2015, even beating traditional terrorism (Ledbetter, 2015).

Critics of the persistent use of cyber-doom scenarios point to several potential dangers of relying too heavily on such worst case thinking. Framing cyber threats in extreme terms invites a militarised response that may be ineffective and even counterproductive for dealing with the cyber threats that we do face (Lewis, 2010). In the first case, it is not at all clear that the military is the appropriate institution for dealing effectively with the kind of broad cyber threat to private intellectual property and personal information identified by DNI Clapper and his predecessors (Lawson, 2013b). More concerning, however, is the possibility that the types of policies and responses that worst case thinking promotes are actually counterproductive. Militarised cyber security policies by the US could undermine its own policy of promoting Internet freedom around the world. In an interconnected environment such as cyberspace, the kinds of offensive actions often contemplated or, in some cases already undertaken, can 'blow back' onto the party who initiated those actions, leading to unintended, negative consequences (Dunn Cavelty, 2008, p. 143; Lawson, 2015; Dunn Cavelty & Van Der Vlugt, 2015). In other cases, such framing might encourage defensive actions that are ineffective or even counterproductive (Ball et al., 2013; Gallagher & Greenwald, 2014; Schneier, 2014). There also exists the possibility that worst case, cyber-doom thinking could distract from and lead to a sense of complacency about the more mundane, but realistic, cyber threats that we do face (Debrix, 2001, p. 156; Lewis, 2010, p. 4; Lawson, 2012). Finally, some worry that worst-case, cyber-doom thinking and the militarised responses it promotes could end up as a self-fulfilling prophecy, leading to conflict escalation where non-physical cyber attacks escalate to physical warfare, or even to the kinds of preventive war scenarios witnessed in the 2003 US invasion of Iraq (Furedi, 2009; Thierer, 2013; Blunden & Cheung, 2014; Valeriano & Maness, 2015).

3. FEAR APPEALS

Cyber-doom scenarios are an example of the use of fear appeals to raise awareness of, and motivate a response to, cyber security problems. In general, scholarship indicates that while fear appeals can be effective and ethical forms of argument, they are prone to failure, to producing counterproductive effects, and to being used in ways that are detrimental to political deliberation in a democracy.

A fear appeal is a kind of argument that attempts to persuade or influence through the use of 'warning[s] that some bad or scary outcome will occur if the respondent does not carry out a recommended action' (Walton, 2000, p. 1). Fear appeals can take a number of forms. Cyber-doom scenarios, however, most closely resemble the form of fear appeal that works based on invoking uncertainty about a possible future. In this form, '[s]ome dangerous event that, it is said, might happen in the future, raises gloomy foreboding and fears related to the uncontrollability of what could possibly happen in an uncertain world. Fear appeal arguments [of this type] trade on uncertainty about a possible future sequence of events that might be set into motion once a step in a certain direction is taken' (Walton, 2000, pp. 14-15) or, we might add, *not taken*.

There is a long tradition of studying such arguments. Rhetoricians, logicians, and scholars of argumentation have been concerned with the effectiveness of such arguments, but also their logical structure, variations, and ethics. These scholars have traditionally argued that fear appeals are fallacious, unethical, or both because they rely on appeals to emotion or, in some cases, overt threats such as in a classic protection racket. However, more recent scholarship has questioned the notion that fear appeals are always fallacious or unethical (Walton, 2000; Pfau, 2007). For example, Pfau (2007) examines Aristotle's advice about how to effectively employ appeals to fear. Aristotle advised that to be effective one must convince the audience that the threat is painful and destructive, that it is near, that it is contingent (preventable or controllable), and buoy the courage of the audience to act. Pfau (2007, pp. 231-233) argues that, for Aristotle, fear appeals can be effective and ethical if they are employed to call attention to a real danger, serve to open deliberation, and encourage appropriate responses, as opposed to closing discussion and coercing a pre-determined response. He also notes that Aristotle warned against the use of 'overpowering fears', which could inspire 'flight or resignation and inaction' instead of appropriate responses (Pfau, 2007, p. 227).

Social scientists have posited models of fear appeals that bear a close resemblance to the one offered by Aristotle. In the model proposed by Rogers (1975), there are three components of fear appeals: (i) the severity of the threat; (ii) the probability of occurrence of the threat; and (iii) the efficacy of a response (see also Maddux & Rogers, 1983). More recently, models of fear appeal messages have been said to be composed of four components, two related to the threat and two related to the recommended response (Witte, 1994). The threat components convey the ideas that the threat is particularly harmful (severity) and that the listener is at risk of experiencing these harmful effects (susceptibility). The response components convey the ideas that the recommended response will be effective (response efficacy) and that the listener is capable of carrying out the response (self-efficacy; Witte, 1994, p. 114). The study of why fear appeals succeed or fail has been prominent in health communication, particularly among those concerned with how to promote healthy behaviours and discourage unhealthy behaviours. More recently, researchers in the field of information security have looked to health-related fear appeals research to guide their own work on promoting better security practices among computer users (Boss, et al., 2015).

In general, studies of the effectiveness of fear appeals in health communication and information security have largely confirmed Aristotle's advice; some use of fear is helpful, but too much is counterproductive. Success occurs when listeners engage in danger control behaviours, those that reduce the threat. Failure occurs when listeners engage in fear control behaviours, those that reduce their feelings of fear but do nothing to prevent, or sometimes even increase the risk of, the threat. Initially, researchers hypothesised that the greater the fear elicited in the fear appeal message, the greater the likelihood of message success. That, however, turned out not to be the case. Instead, researchers have found that fear only works up to a certain point. Too much fear can actually be counterproductive. Aristotle's 'contingency' and 'courage' seem to be key to message success. Listeners cannot only be scared into action. They must also believe that something effective can be done to address the threat and that they are capable of carrying out the necessary response. That is, threat components of the fear appeal message must be accompanied by, and in balance with, convincing response components for the message to succeed (Witte, 1994; Peters, et al., 2013). Researchers in information security have only recently begun to explore the role of fear appeals in promoting better security practices, but this early work tends to agree with the findings from health communication (Doohwang, et al., 2006; Herath & Rao, 2009; Pfleeger & Caputo, 2011; Siponen, et al., 2014; Boss, et al., 2015).

In addition to the effectiveness of fear appeal messages, scholars of rhetoric, logic, and argumentation have also explored the ethical and normative aspects of fear appeals. This work lends support to the concerns raised about possible negative effects of cyber-doom scenarios. Although recent scholarship rejects the traditional idea that fear appeals are always fallacies and are unethical, this work still maintains that fear appeals can be dangerous. For example, Walton (2000, p. 199) argues that these arguments can serve as ‘a potent obstacle to free democratic political deliberations and open critical discussions of political issues’. He describes various cases in which fear appeals are weak, unethical, or even fallacious forms of argument that are ‘destructive to the democratic process’. These cases include instances where speakers resort to fear appeals because of weak evidence or weak ties between their premises and conclusions. That is, they use fear or threat as a shortcut to prematurely close down deliberation and get their way (Walton, 2000, pp. 188-191). Similarly, fear appeals can be fallacious and unethical when they rely on deception. In these cases, the speaker knows that the fear or threat is not supported by, or that it is even contradicted by, the evidence (Walton, 2000, pp. 193-194). Finally, fear appeals can also be unethical and perhaps fallacious when they are used as a tool of misdirection or distraction in political deliberation, taking attention away from other, relevant issues or considerations and focusing attention instead on one, emotionally charged issue (Walton, 2000, p. 200).

4. AMERICAN BLACKOUT

The fictional *National Geographic Channel* docudrama, *American Blackout*, aired in October 2013 and reached roughly 86 million American households (Seidman, 2015). In addition to depicting a cyber-doom scenario in detail, this programme is exemplary of the blurring of distinctions between news and entertainment media that some have argued are central to the emergence of a culture and politics of fear in the last several decades (Altheide, 2002, 2006; Glassner, 1999). Thus, this programme and the responses that it elicited on social media are valuable for understanding how traditional and new media contribute to the articulation of cyber security-related fears and audience responses to the communication of those fears.

We collected the responses to the show on the social media platform, *Twitter*. Tweets with the hashtag #AmericanBlackout were collected on the first night that the show aired and for about 12 hours afterwards using a free tool called *Twitter* Archiving Google Spreadsheet (TAGS) v.5. This tool uses the *Twitter* API to collect into a spreadsheet tweets meeting a certain search criteria.[2] Though the program reached 86 million U.S. homes, gauging viewer responses to the program using more traditional methods would require knowing which of the 86 million homes, and who in them, actually viewed the program so that a survey could be conducted. However, using Twitter responses that included the hashtag #AmericanBlackout had the advantage of providing a more direct route to a group of people who presumably watched the program or

[2] For more information about his tool, see https://tags.hawksey.info/ (accessed December 29, 2015).

were aware of it. This collection method resulted in 16,501 tweets. We content analysed a random sub-sample (10 percent) of the collected tweets for preliminary analysis. Of the 1,650 tweets in the sub-sample, one tweet was not in English and was thus excluded from analysis. In accordance with models of fear appeals, we content analysed the tweets for susceptibility, severity, and efficacy of responses. Because we were interested in the type of responses to cyber-doom scenarios, we examined the tweets for preventative and reactive responses, that is, tweets mentioning responses to prevent or react to a cyber-doom scenario like the one depicted in the show. It is important to note that these data represent viewers' responses to the docudrama and are thus people's *perceptions* of the threat and recommended responses. In addition to perceptions of threat, efficacy, and types of recommended responses, we also coded any expressions of fatalistic reactions or avoidance in each tweet, such as tweets where individuals expressed the idea that nothing could be done or a desire to avoid thinking about such a scenario. Finally, as tweets can be original (created and posted by the user) or re-posted content, we felt it important to quantify how many tweets were re-tweets or modified tweets, which are re-posts that are altered in minor ways. Descriptions of the variables coded in this study and examples of tweets can be found in Table 1. Two independent coders each read and coded the full sample of 1,649 tweets. Disagreements between coders were reconciled through discussion. Of the 1,649 tweets coded in our preliminary analysis, 1,157 (70.2 percent) were re-tweets or modified tweets. Although the majority of tweets were not original, users are likely to re-post content as a way to engage with other users tweeting about the show and further share content they believe worthy of dissemination.

TABLE 1: DESCRIPTION OF CODED VARIABLES AND EXAMPLES FROM TWEETS CONTAINING #AMERICANBLACKOUT

Variable	Definition	Examples
Susceptibility	Expression that he/she is likely to be in such a scenario	When will the real #americanblackout happen?
Severity	Expression that the threat of cyber-doom is harmful and/or large	Im freaking out right now im worried about my kids :(#americanblackout
Presence of response	Tweet expresses that individual perceived some response to threat	#americanblackout is petrifying. I will now become a doomsday prepper.
Efficacy of response	Tweet expresses whether the perceived response will work	#americanblackout M.R.E I had five cases and gave them away wish I hadn't now. M.R.E are the way to go they last long for years
Self-efficacy	Belief about whether user is capable of carrying out responses and/or cope with the threat	#americanblackout after this show I am surely becoming a doomsday prepper / survivalist when the s*** hits the fan what are you going to do?
Preventative government response	Expression of government response that is preventative	#americanblackout is so freaking scary omg i would die ▯ like no. the government better ensure that NEVER happens or im movin to canada
Preventative personal response	Expression of personal response that is preventative	

Variable	Definition	Examples
Preventative other response	Expression of preventative response not associated with personal or government actions	Lets all cross our fingers and pray this never happens, lol I'll be looking like a cave women.. if I survive. :o #americanblackout
Reactive government response	Expression of government response that is reactive	FEMA repeats orders for millions of body bags
Reactive personal response	Expression of personal response that is reactive	I need to go buy a few gallons of water tomorrow. It might get real, soon. #AmericanBlackout
Reactive other response	Expression of reactive response not associated with personal or government actions	Learn how to get prepared rationally, by real people. Not Scared. #preppertalk chat Daily-6PM Eastern. #AmericanBlackout
Fatalistic reaction or avoidance	Expression of inability or unwillingness to act or respond to threat	Honestly, I don't think I would survive. #americanblackout
Re-tweets	Tweets that contain 'RT,' 'MT,' or quotations marks around content	RT @Aj_Dreww: This #americanblackout is freaking me out...

As a fear appeal, *American Blackout* begins with two epigraphs that establish the supposed severity, susceptibility, and credibility of the threat depicted in the programme. The first, a quote from Dr. Richard Andres of the US National War College, asserts, '[a] massive and well-coordinated cyber attack on the electric grid could devastate the economy and cause a large-scale loss of life'. The second explains, '[t]he following program draws upon previous events and expert opinions to imagine what might happen if a catastrophic cyber attack disabled the American power grid'. The implication is that such an attack is a possible scenario that would severely affect the entire nation.

Much of the remainder of the show repeatedly reinforces these themes of severity and susceptibility as we see cell phone videos taken by average people documenting their attempts to survive what turns into a ten day blackout. These personal cell phone videos are interspersed with news footage, which helps to provide the big picture view of the cyber attack's effects. In this scenario, no one is untouched by these effects, which in just three days includes violence, looting, rioting, and loss of life. Early in the programme, one citizen tells his camera that the United States has become 'a Third World country'. Later, another talks about society no longer existing, and even the President admits that government cannot 'keep society afloat.' The implication is clear: Electricity and society are one and the same; without the former, the latter quickly ceases.

Despite the show's attempt to portray such a scenario as frighteningly harmful and likely, our analysis of *Twitter* responses shows that only 35.8 percent of tweets contained expressions of perceived susceptibility to cyber attack and only 26.3 percent of tweets contained expressions of perceived severity of the threat of cyber attack. However, a smaller proportion contained expressions of both severity and susceptibility (21 percent), while 48.8 percent of tweets did not contain mentions of either dimension.

Though *American Blackout* quickly, clearly, and repeatedly establishes the threat components of its fear appeal message, the programme does not clearly articulate a recommended response for preventing the threat of cyber attack or for mitigating the effects should such an attack occur. In the show, any recommended responses that are even implied are focused on government, individual, family, or small group responses in the aftermath of the attack. There are no depictions of responses at a level between the government and the individual or small group. This is exemplified in the tweets about the show, only 20.1 percent of which contained mentions of recommended responses to a cyber attack.

Where government is concerned, the programme depicts centralised and militarised responses, such as military and riot police using force to quell riots and looting, as well as declaring a state of emergency in which the federal government takes centralised control of all food and water supplies. However, the majority of tweets did not mention government responses. Only 5.0 and 0.2 percent of tweets mentioned preventative (e.g., power grid drills) and reactive (e.g., declaring a state of emergency) government responses, respectively. In the programme, individuals, families, and small groups mitigating the effects of the attack for themselves are largely portrayed as helpless to prevent or effectively react to such a cyber-doom scenario. This is borne out in the content analysis where none of the 1,649 tweets coded contained expressions of preventative actions that individuals or small groups could take. In fact, almost all (99.1 percent) of the tweets contained no expression of self-efficacy at all.

In the show, there is one exception with regards to individuals' ability to mitigate the threat; a family of so-called 'preppers.' These are people who prepare for doomsday by planning to 'bug out' to a safe location stocked with food, water, and weapons. In the programme, the prepper family does just that, withdrawing from society to an undisclosed location in the mountains, refusing to help their neighbours, dressing in military garb, and drawing weapons on a neighbour who asks for some food and water. Throughout the show, an advertisement for the *National Geographic Channel* show, *Doomsday Preppers* appears often in the upper right corner of the screen, another tacit endorsement of 'prepping' as the only possible response to a cyber-doom scenario. Roughly 7.5 percent of tweets contained reactive responses to *American Blackout*, typically expressing intentions to become preppers ('I'm about to become a doomsday prepper after watching #americanblackout this is mad scary').

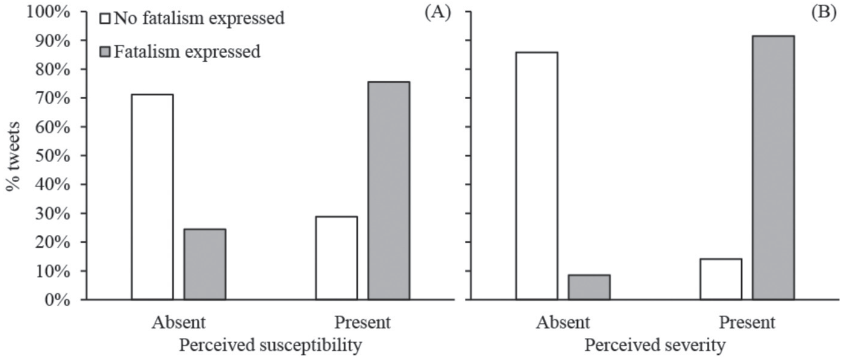
Even though the docudrama seems to tacitly endorse militarised and centralised government responses and 'prepping' on the part of individuals and families, neither of these responses is depicted as particularly effective. In the first instance, a week into the crisis the President must admit that government efforts are not sufficient and asks for assistance from the United Nations. In the second, even the prepper family barely survives. When the show comes to an end, they are in an armed standoff with a group trying to steal their supplies and are only saved when the power comes back on, which is represented by the sudden sound of a ringing iPhone. Just as suddenly, the standoff ends as society/electricity is restored. Equally as abruptly, the show comes to a close. As suddenly as lack of electricity destroyed society and led to disaster from which there was no escape or response, society was just as quickly restored and all was right with the world once again.

As a fear appeal, we can say that this cyber-doom scenario has strong and clear threat components that articulate a clear vision of the severity and susceptibility of a massive cyber attack. Moreover, this fear appeal is much less clear when it comes to offering recommended responses, which are arguably entirely absent. Likewise, the message does little to address either response or personal efficacy, largely depicting any implied responses as ineffective or, in the case of 'prepping', requiring years of work and a great amount of resource to achieve results that are uncertain at best in terms of their effectiveness.

It is perhaps unsurprising, therefore, that viewers were more likely to tweet about the threat components of the show than about the response components. Nonetheless, the volume of viewer mentions of severity or susceptibility was still quite low, which may be read as an indicator that they did not perceive the scenario depicted in the show to be believable. This is important because, as discussed below, perceptions of the believability of the threat components influence perceptions of the response components of the message. Certainly, a small number of viewers explicitly rejected the threat components outright. Similarly, when response components of the show were mentioned at all, they tended to mention government action to prevent the threat, or individual responses focused on reacting to the threat by 'prepping'. Viewers did not perceive that there was anything effective that they could do to prevent such a scenario.

As fear appeals are a persuasive messaging technique, the outcomes are typically message acceptance or rejection. Using the Extended Parallel Process Model (EPPM) of information processing, Witte (1994) posits that message acceptance is motivated by a need for protection against the threat, while rejection is driven by defensive motivation. Defensive motivation occurs 'when perceived threat is high and perceived efficacy is low, and produces message rejection responses such as defensive avoidance or reactance' (Witte, 1994, p. 116). Our content analysis found the majority of tweets (83.6 percent) contained no expressions of defensive motivation. The remaining 16.4 percent contained fatalistic or avoidance reactions characterised by an inability to deal with the threat. Examples include '#AmericanBlackout If this really happens I can't deal' and 'Uhmm I am ok with not watching #AmericanBlackout. Don't really want to imagine all the terrible things that would happen.' We used chi-square tests to examine the relationships between perceived susceptibility and expressions of fatalism, as well as perceived severity and expressions of fatalism. We found these relationships to be significant (perceived susceptibility-fatalism: $\chi^2 = 211.54$, df = 1, $p \leq .00$; perceived severity-fatalism: $\chi^2 = 675.17$, df = 1, $p \leq .00$). Among tweets that had no evidence of defensive avoidance (83.2 percent of all tweets), 71.2 percent contained no expression of susceptibility to the threat. Conversely, among tweets that expressed fatalism (16.8 percent of all tweets), 75.6 percent contained some expression of defensive motivation in the form of fatalism or avoidance of the scenario. A similar pattern is observed in the relationship between perceived severity and fatalism (Figure 1). In other words, our data suggest that perceived severity and susceptibility are positively related to expressions of defensive motivation.

FIGURE 1: CROSS-TABULATIONS OF PROPORTIONS OF EXPRESSIONS OF PERCEIVED SUSCEPTIBILITY (A) AND SEVERITY (B) WITH THOSE OF DEFENSIVE MOTIVATION. IDENTICAL COLORED BARS IN EACH PANEL TOTAL 100 PERCENT



Given the evidence, it is clear that the frightening rhetoric of cyber-doom scenarios, such as the one depicted in *American Blackout*, can be counterproductive to addressing real cyber attack threats, particularly if such messaging leads people to discount or downplay the potential threat.

5. CONCLUSION

The findings presented here lend support to concerns that the use of cyber-doom scenarios could have a negative impact on our ability to raise awareness of, and appropriately respond to, actual cyber security challenges. Existing scholarship in communication on the use of fear appeals has consistently demonstrated that such arguments can be counterproductive, unethical, or both, when they rely too much on raising fear of a threat, while simultaneously failing to offer the audience effective responses, or at least promote deliberation about possible responses. These findings are borne out in our preliminary assessment of instantaneous viewer responses on social media to the cyber-doom scenario depicted in *American Blackout*. Viewers were more likely to respond to the threat components of the message than to the response components, which makes sense given the strength of the threat depicted in *American Blackout* and weakness of the efficacy component. Nonetheless, the volume of responses to the threat component was still low, a potential indicator that most viewers did not find the scenario believable. Viewer responses that did mention the threat components were more likely to also express a sense of fatalism about the threat. Likewise, few responses indicated that viewers believed that there was something efficacious that either they or the government could do to prevent or respond to the scenario depicted in *American Blackout*.

Despite our preliminary analysis, it is difficult to determine whether *American Blackout* was successful as a fear appeal message. Judging the success of the message depends on knowing its intended effects. However, beyond the obvious business goals of any media organisation (viewership and advertising revenue), the goals of this program remain uncertain. However, the most common goals for fear appeals messages in general are the promotion of particular preventive or reactive responses to, or the raising of awareness about, a threat. In the first case, if the goal of this particular fear appeal was to promote a particular preventive or reactive response, it seems to have failed. The vast majority of viewer responses did not express a perceived recommended response. In the second case, if the goal of the program was merely to raise awareness, to call attention to the problem rather than promote any specific response, there are still at least two possible problems. First, scenarios like the one in the program could raise awareness of the wrong problem; second, if audiences find a frightening, over-the-top depiction of cyber threats to be unbelievable, they may be more likely to discount or downplay all messages about cyber threats, even ones that are more realistic. There is another possible intended effect, however; the possible intent of using such scenarios is to scare audiences into passively acquiescing to government actions to combat cyber threats. If this was the intent behind *American Blackout*, then the fatalism exhibited by those who responded to the threat component of the message may indicate that this fear appeal was successful after all. If this were the case, then this message would meet the definition of one that is fallacious, unethical and thus deleterious to deliberation and decision-making in a democracy.

As we have noted throughout, this work represents a preliminary assessment of an extreme cyber-doom scenario and audience responses to it. More work is needed to analyse a larger sample of responses, as well as supplementary media produced as part of the *American Blackout* programme. These might include accompanying website and articles, expert interviews, infographics, and *National Geographic Channel* social media messaging, and responses to the programme in other venues such as blogs or news stories. Similarly, more work is needed to assess whether these findings hold when cyber-doom scenarios are depicted in different media and by different sources, such as government officials. Finally, not all cyber-doom rhetoric involves explicit depictions of worst-case scenarios like the one in *American Blackout* or Secretary Panetta's 2012 'cyber Pearl Harbor' speech. Indeed, cyber-doom rhetoric often involves the more subtle use of analogies and metaphors that imply the possibility of cyber attacks approximating the effects of military attacks or natural disasters but do not provide explicit depictions of those effects. More work is needed that seeks to measure empirically the effects of this more subtle form of cyber-doom rhetoric.

At minimum, however, the findings of this study lend support to concerns about the possible negative effects of cyber-doom rhetoric and should thus encourage policy makers, commentators, industry experts, journalists, and other cyber security advocates to be more cautious in their messaging strategies. Indeed, our study provides insights into recent findings from the Chapman University Survey of American Fears 2015, which found that fear of 'cyber-terrorism' ranked second only to government corruption in a list of top ten fears that average Americans said make them 'afraid' or 'very afraid' (Ledbetter, 2015). We noted above that one danger of cyber-doom rhetoric is that it can raise awareness of the wrong problems. The Chapman Survey may provide evidence that this is indeed occurring on a wider scale. For example, the survey showed that 'cyber-terrorism' (an as-yet hypothetical concern) ranked higher than other concerns directly related to actual cyber threats. These included tracking of personal information by corporations and government, identity theft, 'running out of money', and credit card fraud, all of which are related to the actual, low-level cyber threats over time to personal, corporate, and government data that DNI Clapper and so many others have consistently identified as representing the true cyber threat. Indeed, cyber-terrorism outranked traditional terrorism even at a time when ISIS was on the march in the Middle East and North Africa.

A second possible danger of fear appeals in general, and cyber-doom rhetoric in particular, identified in the literature and in our study, was a tendency towards fatalism and demotivation when threats are overemphasised relative to effective responses. It is potentially significant to note, therefore, that although cyber-doom rhetoric has been prominent in US public policy discourse about cyber security, and 'cyber-terrorism' was ranked second among American's top fears in 2015, we have seen very little government action on cyber security even as experts continue to downplay the threat of cyber-doom. For example, in February 2016, former Director of the National Security Agency and the Central Intelligence Agency, General Michael Hayden, echoed DNI Clapper's 2015 assessment of the cyber threat when he told the *Wall Street Journal* that fear of 'cyber Pearl Harbor, digital 9/11, catastrophic attack' are misplaced, and that the only piece of cyber security legislation passed thus far – the Cybersecurity Information Sharing Act of 2015 – is essentially too little, too late, and leaves businesses and individuals largely responsible for their own cyber defence (Bussey, 2016). The combination of what we know from the existing fear appeals literature, the findings of our study, and the results of the Chapman survey indicate that the persistence of cyber-doom rhetoric may help to explain this lack of substantive progress in addressing the most widespread cyber threats that Americans actually face.

This suggests lessons for policymakers, experts, news media, and others responsible for crafting and communicating responses to cyber threats. These actors should think much more consciously and carefully about the intended effects of messages meant to communicate the cyber threat to their peers and the wider public.

In turn, such messages should be more carefully crafted and targeted. There has been a tendency in cyber-doom rhetoric to conflate very different threats into one monolithic and more frightening cyber threat in an attempt to raise awareness and motivate a response (Lawson, 2013b). However, there is not just one threat, but many, each of which may need to be addressed by different actors, including businesses and even average computer users (Singer, 2016). As Peter Singer recently noted, basic 'cyber hygiene' 'would stop 90 percent of cyber attacks, and help to keep all of us safe' (Singer, 2016). Indeed, he is not the first to have suggested that a public health approach to cyber security is necessary (Charney, 2010).

As Gen. Hayden notes, in the absence of sufficient government action on cyber security, organisations and individuals must do more to defend themselves. As Singer and others note, this may actually be the best approach. In either case, communicating specific cyber threats in a way that encourages organisations and individuals to take action, not merely to wait for government, will be crucial to promoting improved cybersecurity. Doing that will require policymakers, experts, and news media to tone down the cyber-doom rhetoric and instead communicate clear and specific messages about specific, realistic threats and, most importantly, what audiences of such messages can do themselves to help address those threats. From Aristotle to recent social science, we know that more fear is not better when trying to motivate audiences to action. This applies to cyber security as much as to wearing one's seat belt or quitting smoking. In short, those responsible for effectively communicating cyber threats would do well to heed a version of Michael Pollan's dictum for healthy eating attuned to communicating threats: 'Use fear. Not too much. Focus on effective and obtainable responses'.[3]

REFERENCES

Adhikari, R. (2009, 2 December). Civilization's high stakes cyber-struggle: Q&A with Gen. Wesley Clark (ret.). *TechNewsWorld*. Retrieved from http://www.technewsworld.com/story/Civilizations-High-Stakes-Cyber-Struggle-QA-With-Gen-Wesley-Clark-ret-68787.html?wlc=1259861126&wlc=1259938168&wlc=1290975140.

Altheide, D. L. (2002). *Creating fear: news and the construction of crisis*. New York: Aldine de Gruyter.

Altheide, D. L. (2006). *Terrorism and the politics of fear.* Lanham, MD: AltaMira Press.

Ball, J., Borger, Julian, & Greenwald, G. (2013, 06 September). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security .

Blunden, W., & Cheung, V. (2014). *Behold a pale farce: cyberwar, threat inflation, & the malware-industrial complex*. Waterville, OR: Trine Day.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015, forthcoming). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*.

Bussey, J. (2016, 9 February). Gen. Michael Hayden gives an update on the cyberwar. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/gen-michael-hayden-gives-an-update-on-the-cyberwar-1455076153.

Charney, S. (2010). *Collective defense: Applying public health models to the Internet*. Redmond, WA: Microsoft Corp.

Clapper, James R. (2015, September 10). "Statement for the Record: Worldwide Cyber Threats." House Permanent Select Committee on Intelligence. Retrieved September 10, 2015 from http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

Collins, S. (2015, 06 August). Senator Collins continues to sound the alarm on the urgent need to bolster cybersecurity. *Press Release, Office of Senator Susan Collins*. Retrieved from http://www.collins.senate.gov/public/index.cfm/2015/8/senator-collins-continues-to-sound-the-alarm-on-the-urgent-need-to-bolster-cybersecurity.

Conway, M. (2008). Media, fear and the hyperreal: the construction of cyberterrorism as the ultimate threat to critical infrastructures. In M. Dunn Cavelty & K. S. Kristensen (Eds.), *Securing the 'Homeland': Critical Infrastructure, Risk and (In)Security* (pp. 109-129). London: Routledge. Retrieved from http://doras.dcu.ie/2142/1/2008-5.pdf.

Debrix, F. (2001). Cyberterror and media-induced fears: The production of emergency culture. *Strategies*, 14(1), 149-168.

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age*. New York, NY: Routledge.

[3] Pollan's dictum is 'Eat food. Not too much. Mostly plants.' (Pollan, 2008).

Dunn Cavelty, M., & Van Der Vlugt, R. A. (2015). A tale of two cities: Or how wrong metaphors lead to less security. *Georgetown Journal of International Affairs, Fall*, 21-29.

Elias, T. D. (1994, 2 January). Toffler: Computer attacks wave of future. *South Bend Tribune (Indiana)*, p. F10.

Furedi, F. (2009). Precautionary culture and the rise of possibilistic risk assessment. *Erasmus Law Review*, 2(2), 197-220.

Gallagher, R., & Greenwald, G. (2014, 12 March). How the NSA plans to infect 'millions' of computers with malware. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/.

Glassner, B. (1999). *The culture of fear: why Americans are afraid of the wrong things*. New York, NY: Basic Books.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Koppel, T. (2015). *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*. New York: Crown.

Lawson, S. (2012, 16 October). Of cyber doom, dots, and distractions. *Forbes.com*. Retrieved from http://www.forbes.com/sites/seanlawson/2012/10/16/of-cyber-doom-dots-and-distractions/.

Lawson, S. (2013a). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics, 10*(1), 86-103.

Lawson, S. (2013b). Motivating cybersecurity: Assessing the status of critical infrastructure as an object of cyber threats. In C. Laing, A. Badii, & P. Vickers (Eds.), *Securing critical infrastructures and critical control systems: Approaches for threat protection* (pp. 168-189). Hershey, PA: IGI Global.

Ledbetter, S. (2015, 13 October). America's top fears 2015. *Chapman University Blog*. Retrieved from https://blogs.chapman.edu/wilkinson/2015/10/13/americas-top-fears-2015/.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lewis, J. A. (2010). The Cyber War Has Not Begun. *Center for Strategic and International Studies*. Retrieved from http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf.

Lyngaas, S. (2015, 23 February). NSA's Rogers makes the case for cyber norms. *FCW*. Retrieved from https://fcw.com/articles/2015/02/23/nsa-rogers-cyber-norms.aspx.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi: 10.1016/0022-1031(83)90023-9.

Martinez, J. (2012, 31 October). Napolitano: Us financial institutions 'actively under attack' by hackers. *The Hill*. Retrieved from http://thehill.com/policy/technology/265167-napolitano-us-financial-institutions-qactively-under-attackq-by-hackers.

Meyer, D. (2010). Cyberwar could be worse than a tsunami. *ZDNet*. Retrieved from http://www.zdnet.com/news/cyberwar-could-be-worse-than-a-tsunami/462576.

Obama, B. (2015, 13 February). Remarks by the president at the cybersecurity and consumer protection summit. *Office of the Press Secretary, The White House*. Retrieved from https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

Pagliery, J. (2015, 27 October). Senate overwhelmingly passes historic cybersecurity bill. *CNN*. Retrieved from http://money.cnn.com/2015/10/27/technology/cisa-cybersecurity-information-sharing-act/.

Panetta L (2012) Defending the National From Cyber Attacks. Presentation to Business Executives for National Security, New York, NY. 11 October.

Peters, G.-J. Y., Ruiter, R. A. C., & Kok, G. (2013). Threatening communication: A critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review, 7*(sup1), S8-S31.

Pfau, M. (2007). Who's afraid of fear appeals? Contingency, courage, and deliberation in rhetorical theory and practice. *Philosophy and Rhetoric, 40*(2), 216-237.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611.

Pollan, M. (2008). *In defense of food: an eater's manifesto*. New York: Penguin Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. doi: 10.1080/00223980.1975.9915803.

Schneier, B. (2014, 14 August). Quantum technology sold by cyberweapons arms manufacturers. *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2014/08/quantum_technol.html.

Schwartau, W. (1991). *Terminal Compromise*. Seminole, FL: Inter.Pact Press.

Seidman, R. (2015, February 22). List of how many homes each cable network is in as of February 2015. *TV by the Numbers*. Retrieved October 1, 2015, from http://tvbythenumbers.zap2it.com/2015/02/22/list-of-how-many-homes-each-cable-network-is-in-as-of-february-2015/366230/.

Singer PW (2016, 11 February) Cybersecurity and Cyberwar: What Everyone Needs to Know. Presentation to College of Wooster. Retrieved from http://www.wooster.edu/news/releases/2016/february/recap-singer/index.php.

Siponen, M., Adam, M., M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change, 46*(4-5), 223-238.

The Atlantic. (2010, 30 September). Fmr. Intelligence director: New cyberattack may be worse than 9/11. *The Atlantic*. Retrieved from http://www.theatlantic.com/politics/archive/2010/09/fmr-intelligence-director-new-cyberattack-may-be-worse-than-9-11/63849/.

Thierer, A. (2013). Technopanics, threat inflation, and the danger of an information technology precautionary principle. *Minn. JL Sci. & Tech., 14*, 309. Retrieved from http://conservancy.umn.edu/bitstream/11299/144225/1/Technopanics-by-Adam-Thierer-MN-Journal-Law-Science-Tech-Issue-14-1.pdf.

Valeriano, B. and Ryan C Maness. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. London: Oxford University Press.

Walton, D. N. (2000). *Scare tactics: arguments that appeal to fear and threats*. Boston: Kluwer Academic Publishers.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism, 28*(2), 129-149. doi:10.1080/10576100590905110

Weimann, G. (2008). Cyber-terrorism: Are we barking at the wrong tree? *Harvard Asia Pacific Review, 9*(2), 41-46.