International Journal of Cybersecurity Intelligence & Cybercrime

Volume 6 | Issue 1 Article 3

3-31-2023

# Threat Construction and Framing of Cyberterrorism in the U.S. News Media

Bastug et al. (2023). *International Journal of Cybersecurity Intelligence and Cybercrime, 6*(1), 29-44.

# Threat Construction and Framing of Cyberterrorism in the U.S. News Media

Mehmet F. Bastug*, Ph.D., University of Scranton, U.S.A.
Ismail Onat, Ph.D., University of Scranton, U.S.A.
Ahmet Guler, Ph.D., Pennsylvania State University, U.S.A.

*Keywords: Cyberterrorism, Fear of cyberterrorism, Media framing, Cultivation theory*

**Abstract:**
This research aims to explore the influence of news media on the fear of cyberterrorism and how cyberterrorism is framed in the media. Using a mixed-method approach as a research strategy, this paper reports on two studies that explore the influence of news reading on the fear of cyberterrorism. The first study analyzed survey responses from 1,190 participants and found that increased exposure to reading news media was associated with increased fear of cyberterrorism. The second study, built on the first, sought to investigate how cyberterrorism is framed and constructed as a threat by the US local and national newspapers. The framing and portrayal of cyberterrorism in US newspapers are discussed.

## Introduction

Data breach incidents, cyberattacks against critical infrastructure, ransomware hacks, and cybercrime victimization have been on the rise in recent years. Malicious hackers continuously develop more sophisticated hacking tools and methods to bypass cybersecurity measures and become more competent in infiltrating computer systems. Modern cyberattacks are more destructive and are carried out by hacker groups with substantive resources and capabilities. Foreign governments allegedly sponsor some hacker groups, as in the cases of Colonial Pipeline and SolarWinds hacks, whereas some other groups allegedly have ties with terrorist organizations (Bastug, 2021a, 2021b).

There are many definitions of terrorism, and therefore cyberterrorism, in the literature. It is the convergence of cyberspace and terrorism (Denning, 2000), but it is not clear what constitutes cyberterrorism. In simple terms, cyberterrorism is "an act or acts of terrorism carried out through the use of a computer" (Em-bar-Seddon, 2002, p. 1035). Some scholars define it in narrow terms and argue that it should result in physical violence. Maura Conway (2002, p. 436), for instance, defined the concept as "premeditated, politically motivated attacks by subnational groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against noncombatant targets." Some other definitions adopted a broader approach and included the terrorist use of the Internet in cyberterrorism: "the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change" (Brickey, 2012, p. 6). Terrorist use of the Internet is a form of "enabling" cyberterrorism. Modern terrorist groups display a growing interest in cyberspace. They use it to spread propaganda, recruit militants, and communicate

*Corresponding author
Mehmet F. Bastug*, Ph.D., Department of Sociology, Criminal Justice & Criminology, The University of Scranton, 800 Linden Street, Scranton, PA, 18510, U.S.A.
Email: mehmet.bastug@scranton.edu

with each other (Bastug et al., 2020; Lee et al., 2021). They also use it to launch cyber-attacks against their targets (Bastug, 2021a).

In parallel with these issues, the fear of cyberterrorism is rising, as suggested by public polls. Cyberterrorism has become one of the top ten fears among Americans (Chapman University Survey of American Fears, 2019). Although becoming a more fearsome phenomenon, what fuels this specific fear is understudied in the literature. Cyberterrorism is an exotic crime, and individuals rarely, if any at all, become victims of cyberterrorism. Even though terrorist organizations have shown some efforts toward initiating significant cyberattacks, they vastly prefer to carry out "traditional" terrorist attacks against their targets (Piazza & Guler, 2019). There have been only a few recorded incidents of cyberterrorism in the Global Terrorism Database (START [National Consortium for the Study of Terrorism and Responses to Terrorism], 2022). Some researchers developed their own datasets using various resources and identified more cases of cyberterrorism (see Lee et al., 2021), yet the number is still very small. Despite its infrequent occurrence, the fear of cyberterrorism is somewhat prevalent. Media is often blamed for instilling the fear of cyberterrorism because of its framing of the phenomenon (see Debrix, 2001; Weimann, 2005). Since cyberterrorist attacks usually target organizations or businesses, and individuals rarely experience such attacks, the media could be the primary source of creating awareness, information, and hype about cyberterrorism.

Previous research on fear of crime, as well as fear of terrorism, investigated the role of media in creating fear and anxiety in society (see Comer & Kendall, 2007; Kula & bastug, 2021; Nellis & Savage, 2012; Onat, 2016; Onat et al., 2021; Onat et al., 2022; Williamson et al., 2019). As explained in the next section, just a few studies have examined the relationship between media exposure and fear of cyberterrorism. Along those lines, the current research first explored how reading local and national newspapers influences the fear of cyberterrorism using a national survey of American adults. To further explain the result of the quantitative analysis and investigate the media coverage of cyberterrorism, the study also employed a qualitative analysis of news articles from US newspapers. Overall, the study contributes to the literature by providing a comprehensive picture of how the US print media frames cyberterrorism and the link between exposure to media and fear of cyberterrorism.

## Literature Review

Studies on cyberterrorism go back to the late 90s (see Littleton, 1995; Nelson et al., 1999; Ogren & Langevin, 1999). The concept drew growing scholarly attention in the early 2000s and proceeded to increase after that. Early studies mainly focused on defining the then-emerging phenomenon (see Gordon & Ford, 2002; Veerasamy, 2009) and assessing the threat (see Embar-Seddon, 2002; Thomas, 2003; Weimann, 2004). A review of the early literature reveals that while some scholars saw cyberspace as a force multiplier for terrorist activities and predicted the possibility of a digital menace (Benson, 2014; Denning, 2013; Rudner, 2016), other scholars had a skeptical approach to cyberterrorism and argued that the threat was exaggerated particularly by the media (see Debrix, 2001; Weimann, 2004, 2005).

In conjunction with the debates around the definition and threat assessment, researchers began exploring the ideas encompassing the fear of cyberterrorism. In an early study, Debrix (2001) investigated cyberterrorism as a media-induced fear and argued that the media coverage of the cyberterrorism concept does tend to generate public anxiety and panic. Similarly, Weimann (2005, p. 132) criticized the media framing

of cyberterrorism: "The mass media frequently fail to distinguish between hacking and cyberterrorism and exaggerate the threat of the latter by reasoning from false analogies."

According to Onat et al. (2022), the fear of cyberterrorism is a particular type of terrorism fear that has gained growing interest, especially following the 9/11 terrorist attacks. In fact, some scholars predicted an increase in cyberterrorism attacks after 9/11 and discussed the possibility of catastrophic cyberterrorist attacks perpetrated by global terrorist groups (Denning, 2013). Considering terrorism as a specific form of crime, early studies on terrorism fear drew on the overarching fear of crime literature that suggested a relationship between the consumption of mass media coverage and the fear of crime. Crime news essentially takes place in the massive media that can distort the facts, and people may be fearful of crime as a result of this exaggeration. More specifically, the cultivation theory (Gerbner, 1969; Gerbner et al., 1986) posited that exposure to media could influence the audiences' perceptions of social realities. The media has various components that provide people with instant information, and communication literature encompasses two types of media footage (Cho et al., 2003). Media delivers messages through print or audiovisual footage. While a newspaper is an example of print footage, television news uses audiovisual footage. Television news can employ close-ups, slow motions, video graphics, and sound. All these effects provide a feeling of presence to a viewer. In this vein, Gerbner (1998) suggested that the mass media is a socializing agent and has a cultivating power on attitudes and judgments in the social world. Relative to the amount of time spent on media coverage, the reality in people's eyes may become what the media presents.

According to the cultivation theory, the media depicts the world very differently from the actual conditions. In order to obtain more public interest, the media exaggerates the realities. Especially the coverage that involves frequent violence presents a dangerous world. Thus, reporting crimes in a distorted manner affects the audiences' perceptions of the incidents in the real world. In other words, exposure to the exaggerated media coverage of crimes may generate fear and concerns about being victimized (Gerbner et al. 1994).

The effect of exposure to the media as regards the fear of terrorism has long been scrutinized in literature (see Debrael et al., 2019; Nellis & Savage, 2012; Skøt, Nielsen & Leppin, 2020; Onat et al., 2021; Williamson et al., 2019). Accordingly, it appears terrorist organizations want their attacks to be publicized through the media to convey their political messages to wider audiences (Nacos, 1996, 2003; Schmid & Graff, 1982). Terrorist attacks, indeed, draw media attention. This creates a controversial relationship between terrorism and the media (Onat et al., 2021). The media coverage of terrorist attacks also contributes to anxiety and fear in society (Comer & Kendall, 2007), which is a desirable outcome for various terrorist groups.

The fear-inducing effect of media has been reported through empirical research. Nellis and Savage (2012) found that those who watch more television news on terrorism are more likely to have higher levels of fear. Similar research also reported such a relationship between fear of terrorism and exposure to various types of media (see Nellis, 2009; Onat, 2016; Dillon et al., 2019; Wilcox et al., 2009; Oksanen et al., 2020; Williamson et al., 2019). Similarly, exaggerated depictions of cyberterrorism can distort reality and generate fear.

The role of media in creating the fear of cyberterrorism has been investigated in studies that explored the framing of cyberterrorism by various media outlets. Jarvis et al. (2015) analyzed news articles about cy-

berterrorism published in seven countries between 2008 and 2013 and examined how cyberterrorism is constructed as a security threat by the news media. Their analysis revealed that most of the stories showed concern over cyberterrorism. The authors further explored the media coverage of this topic in a 2016 study and identified the referents of cyberterrorism news media discourse (Jarvis et al., 2017). They found that the nation-state is the most common referent threatened by cyberterrorism in the context of media coverage, followed by critical infrastructure and the private sector.

## Research Design

This research aimed to investigate the influence of reading news on the fear of cyberterrorism by administering two studies. For this purpose, the research utilized a sequential explanatory mixed-methods design, employing both quantitative and qualitative analysis. Using a nationally representative sample of American adults, Study 1 examines the relationships between the fear of cyberterrorism and exposure to media. The first study answers the following research question: How does exposure to newspapers influence the fear of cyberterrorism?

To elaborate on the quantitative results, Study 2 analyzes newspaper articles on cyberterrorism published in the last five years in the U.S. The following research question guides the study: How do US newspapers frame cyberterrorism?

### *Study 1: Data and Method*

For the purpose of Study 1, the authors used secondary data drawn from the 2018 wave of the Chapman University Survey on Americans Fears (CSAF). The survey involves responses from 1,190 participants, and the data were collected in 2018. To provide a nationally representative sample, the survey was balanced by phone usage and key demographics (age, gender, education, race/ethnicity, and census region) to match the 2017 Census Bureau's Current Population Survey (Rapoport & Berta, 2018).

The dependent variable in this analysis was the fear of cyberterrorism, measured with one survey question based on a 4-item Likert scale ranging from 1 (not afraid) to 4 (very afraid). Respondents were asked how afraid they were of cyberterrorism, and higher scores on the fear scale indicated higher levels of fear of cyberterrorism.

***Independent variables.*** The quantitative analyses included ten independent variables. The main independent variable was reading news, measured by asking respondents how often they read a national newspaper such as USA Today, The Wall Street Journal, or The New York Times in print or digital. Participants responded to the question on a six-item scale ranging from 1 (never) to 6 (every day). The other independent variables captured the participants' political views, religiosity, vulnerabilities, and socioeconomic status. Political view was measured with one of three possible answers: liberal (coded 1), moderate (coded 2), and conservative (coded 3). Religiosity was measured by asking respondents how religious they consider them selves to be as one of the following: not at all religious (coded 1), not too religious (coded 2), somewhat religious (coded 3), or very religious (coded 4). Vulnerabilities were controlled by gender, age, marital status, race, and socioeconomic status. Gender was coded as a binary variable with two options: female (coded 1) and male (coded 0). Gender was coded as a binary variable with two options: female (coded 1) and male (coded 0).

Marital status was coded as a dummy variable with two options: married (coded 1) and not married, divorced, widowed, etc. (coded 0). Race was coded as a binary variable with two options: Whites (coded 1) and others (coded 2). Age was measured on an ordinal scale in four categories: "18 to 29" (was coded 1), "30 to 49" (was coded 2), "50 to 64" (was coded 3), and "65 and older" (was coded 4).

Three measures captured socioeconomic status. Education was measured by using one of eight possible answers ranging from "less than high school" (coded 1) to "postgraduate or professional degree" (coded 8). Employment was coded as a binary variable with two options: full-time employed (coded 1) and others (coded 0). Homeownership was also coded as a binary measure, with homeowners coded as "1" and others as "0".

### *Findings*

Fifty-eight percent of the sample were females, and 42% were males. Fifty-three percent of the participants were married, 72% identified themselves as White, 48% said they were employed full-time, and 71% were homeowners. The average score describing the fear of cyberterrorism was 2.63 (see Table 1).

Table 1. *Descriptive Statistics*

| **Variable** | N | Mean | Std. Dev | Min | **Max** |
|---|---|---|---|---|---|
| Dependent variables | | | | | |
| Fear of cyberterrorism | 1,188 | 2.63 | 0.91 | 1 | 4 |
| Media exposure | | | | | |
| Reading newspapers | 1,188 | 2.79 | 1.72 | 1 | 6 |
| Politics & religion | | | | | |
| Political view | 1,190 | 1.98 | 0.86 | 1 | 3 |
| Religiosity | 1,190 | 2.53 | 1.04 | 1 | 4 |
| Demographics | | | | | |
| Gender (female=1) | 1,190 | 0.58 | 0.49 | 0 | 1 |
| Age | 1,190 | 2.54 | 0.99 | 1 | 4 |
| Marital status (married=1) | 1,190 | 0.53 | 0.5 | 0 | 1 |
| Race (white=1) | 1,188 | 0.72 | 0.49 | 0 | 1 |
| Socioeconomic status | | | | | |
| Education | 1,190 | 5.27 | 1.8 | 1 | 8 |
| Employment (full-time emp=1) | 1,190 | 0.48 | 0.5 | 0 | 1 |
| Home ownership (homeowner=1) | 1,190 | 0.71 | 0.45 | 0 | 1 |

The results of the bivariate analyses showed that two out of the ten independent variables were significantly correlated with the fear of cyberterrorism. On average, participants with higher exposure to reading newspapers reported higher levels of fear of cyberterrorism. The age variable was positively associated with the fear of cyberterrorism. Older respondents stated they experienced higher levels of fear of cyberterrorism. Table 2 shows the results from the bivariate analyses.

Table 2. *Bivariate Analyses*

| Variable | Fear of Cyberterrorism |
|---|---|
| Media exposure | |
| Reading newspapers | **0.13**** |
| Politics & religion | |
| Political view | 0.001 |
| Religiosity | 0.02 |
| Demographics | |
| Gender (female=1) | 0.04 |
| Age | **0.11**** |
| Marital status (married=1) | -0.05 |
| Race (white=1) | 0.01 |
| Socioeconomic status | |
| Education | 0.02 |
| Employment (full-time=1) | -0.05 |
| Home ownership (homeowner=1) | 0.004 |

** p<0.01, * p<0.05

As the level of measurement for the dependent variable was ordinal, we estimated a weighted ordinal-logistic-regression model for fear of cyberterrorism. The regression assumes that the relationship between the lowest category of the dependent variable is the same as the next lowest category and all upper categories, also known as the parallel lines assumption (Williams, 2016). Therefore, the effects are assumed to be constant across all categories of the outcome variable. Our ordinal post-hoc tests (Brant, 1990) indicated that the model violated the parallel lines assumption (PLA). Hence, we continued with the generalized ordered logit model that relaxes the assumptions and allows covariates to be constrained or unconstrained in accordance with the PLA (Williams, 2016).

In Table 3, we reported the constrained factors relative to all categories. The dependent variable was coded as "1" (not afraid), "2" (slightly afraid), "3" (afraid), and "4" (very afraid). The coefficient values for the unconstrained independent variables require a comparison across all dependent variable categories because the coefficients vary at least for one category of the dependent variable. The coefficients for the constrained covariates do not necessitate a comparison across categories of a dependent variable in this type of model.

The results indicate that one independent variable not constrained by the PLA was education. The education variable was negatively associated with the cyberterrorism fear variable. However, the relationship was only statistically significant for the 'afraid' category of the dependent variable compared to the reference category, indicating that individuals with lower levels of education were more likely to be fearful of cyberterrorism.

Three of the constrained independent variables were significantly associated with cyberterrorism fear. Specifically, participants who (1) read the news more often, (2) identified themselves as more religious, and (3) were older had significantly higher levels of fear of cyberterrorism.

Table 3. *Multivariate Analysis*

| Constrained variables (all categories) | Fear of Cyberterrorism |
|---|---|
| Media exposure | (b (SE)) |
| Reading News | **0.22 (0.05)**** |
| Politics & religion | |
| Political view | n.s. |
| Religiosity | 0.16 (0.08) ** |
| Demographics | |
| Gender (female=1) | n.s. |
| Age | **0.29 (0.08)**** |
| Marital status (married=1) | n.s. |
| Race (white=1) | n.s. |
| Socioeconomic status | |
| Education | ---- |
| Employment (full-time=1) | n.s. |
| Home ownership (homeowner=1) | n.s. |
| Unconstrained variables: 'not afraid' category (1) | |
| Education | n.s. |
| Constant | -0.59 (0.49) |
| Unconstrained variables: 'slightly afraid' category (2) | |
| Education | n.s. |
| Constant | -1.37 (0.39)** |
| Unconstrained variables: 'afraid' category (3) | |
| Education | -0.11 (0.05)** |
| Constant | -2.46 (0.42)** |
| Wald $\chi 2$ (DF), significant | 66.29 (14) |
| | P< 0.01 |
| Pseudo $R^2$ | 0.04 (N=1,186) |

*P< 0.05; **P< 0.01, b=coefficient, SE= Standard Error, n.s.= not significant, "----" = significant at least for one category of dependent variable. Note: Reference category is 'very afraid' for all three models.

### *Study 2: Data and Methods*

To expand the quantitative findings from Study 1, the researchers collected qualitative data from US newspapers using the thematic content analysis method. The terms "cyberterrorism," "cyberterror," "cyberterrorist," "cyberterrorists" and their alternative spellings "cyber terrorism," "cyber terror," "cyber terrorist," and "cyber terrorists" were searched within the editorial and news sections of US newspapers that were published from 1 June 2016 to 1 June 2021. After automatically removing duplicate articles, the researchers examined the remaining 212 news and editorials.

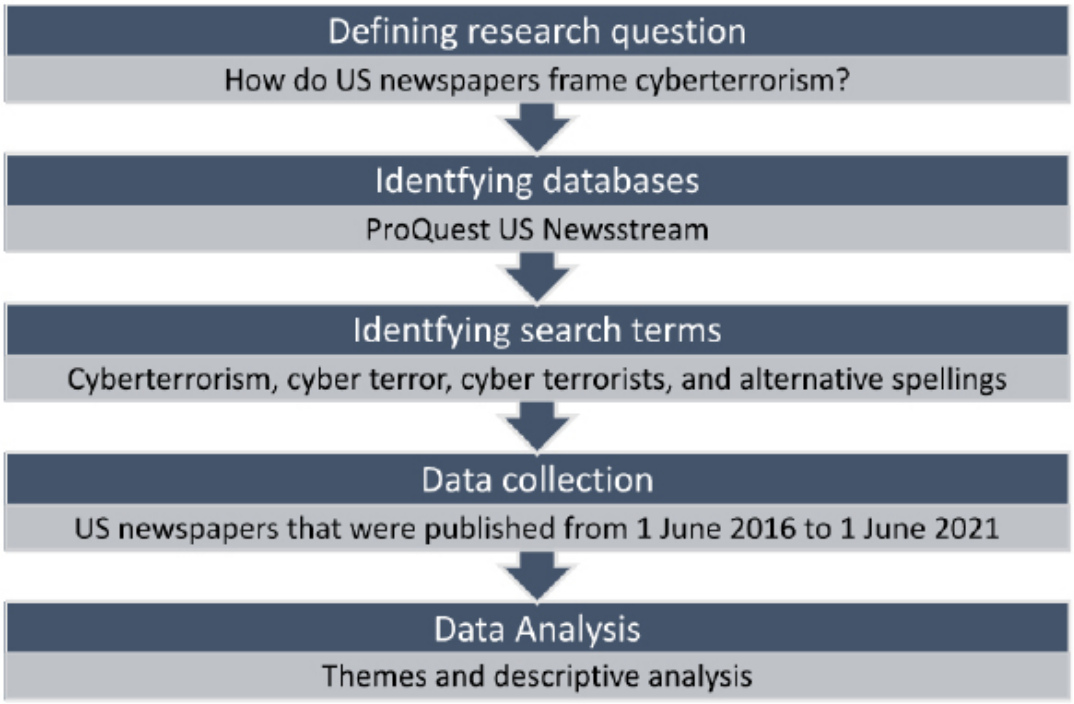


*Figure 1.* Study 2 Procedures

**Findings**

There were duplicate articles that were published in different newspapers. When the same article was published in more than one outlet, we kept the first source that appeared in the results and removed the succeeding sources. In some cases, although some articles include one of the search terms, cyberterrorism was not framed in any way and was not the subject of the article. Those articles mostly involved books or movie reviews. After removing such reports from the sample, the remaining 75 articles were coded, and nine themes were identified. The articles were published in 56 different newspapers. Table 4 shows the number of articles in our final sample from each newspaper in alphabetical order.

Table 5 presents the number of articles in each year during the period covered in the sample. The results reveal that most of the articles were published in 2016 although the sample includes only those published in the second half of that year. The number of articles decreased steadily in the following years until 2020 which unboxed significant cyberattacks such as the SolarWinds hack.

The thematic content analysis method was applied using Corbin and Strauss's three interrelated coding strategies (2008): open coding, axial coding, and selective coding. This coding strategy was purposefully selected to do a rigorous qualitative data analysis for the collected news data. In the first step of the coding process, the researchers tried to identify emerging themes without restricting their analysis to facilitate the

Table 4. *Number of Articles from Each Newspaper*

| Newspaper | N | Newpaper | N | Newspaper | N |
|---|---|---|---|---|---|
| Albuquerque Journal | 1 | Los Angeles Times | 1 | The Desert Sun | 2 |
| American Banker | 2 | Madison Capital Times | 1 | The Greenville News | 1 |
| Asbury Park Press | 1 | Missoulian | 3 | The Jackson Sun | 1 |
| Boston Globe | 1 | Morning Call | 1 | The New York Observer | 2 |
| Charleston Gazette - Mail | 1 | New Haven Register | 1 | The News Leader | 1 |
| Chicago Tribune | 1 | New York Daily News | 1 | The Record | 1 |
| Cincinnati Enquirer | 1 | New York Times | 3 | The Salt Lake Tribune | 1 |
| Columbian | 1 | News - Star | 1 | The Santa Fe New Mexican | 2 |
| Concord Monitor | 1 | Newsday | 1 | The Taos News | 1 |
| Daily News | 1 | Philadelphia Inquirer | 1 | The Texas Tribune | 1 |
| Daily Press | 1 | Pittsburgh Tribune - Review | 1 | The Union Leader | 1 |
| Daily Times | 1 | Portland Press Herald | 2 | USA Today (Online) | 1 |
| Dayton Daily News | 1 | Ruidoso News | 1 | Valley News | 1 |
| Des Moines Register | 2 | Springfield News Leader | 1 | Wall Street Journal | 3 |
| El Paso Times | 1 | St. Louis Post - Dispatch | 1 | Wall Street Journal (Online) | 3 |
| Florida Times Union | 1 | Star Tribune | 1 | Washington Examiner | 6 |
| Florida Today | 1 | The American Israelite | 1 | Wausau Daily Herald | 1 |
| Great Falls Tribune | 1 | The Atlanta Journal | 1 | York Daily Record | 1 |
| Hartford Courant | 1 | The Christian Science Monitor | 1 | **TOTAL** | **75** |

open coding analysis of the data. After identifying and grouping similar items according to their features and dimensions observed in the dataset, the researchers revisited the data to identify subcategories and missing themes and subthemes more systematically. In the last and final step of our coding process, the researchers analyzed the codebook in an effort to extract the observed core themes and subthemes by conducting a selective coding strategy of data analysis. Using this systematic coding strategy, the researchers hoped to uncover the emerging themes framing cyberterrorism in various U.S. print media outlets.

Table 5. *Number of Articles from Each Year*

| Year | N |
|---|---|
| 2021 (first half) | 5 |
| 2020 | 11 |
| 2019 | 7 |
| 2018 | 12 |
| 2017 | 17 |
| 2016 | 23 |
| **TOTAL** | **75** |

The results of this thematic content analysis revealed nine themes. Table 6 shows the description of each theme. The first theme includes articles that frame cyberterrorism as a threat against the overall critical existing infrastructure components. Below is an example of a critical infrastructure frame that was published in USA Today on 30 May 2021:

> This isn't just an issue for policy wonks or wealthy financial institutions. This is a threat to the day-to-day lives of every American. Our drinking water supplies, electric power systems, petroleum and natural gas supplies, hospitals, vehicles, stop lights and road safety signs, air traffic control systems, railroads, and all the businesses selling us goods and services are vulnerable to attacks (Hogan & Blair, 2021).

The national preparedness theme highlights the importance of preparedness for cyberattacks at the national level. It frames cyberterrorism as one of the most serious threats to national security. The following report is extracted from The Washington Examiner:

> The most serious threat to the United States is not a physical terrorist attack, but a cyber-related one. In Washington, you can probably count on one hand the issues that both Republicans and Democrats can agree on -- this is certainly one of them. The inevitability of such a catastrophic event and the destruction that it could cause is a nightmarish scenario that without a doubt keeps our elected officials and military leaders awake at night (Vargas, 2017).

The cyber doom scenarios theme includes articles that frame cyberterrorism as an extremely fearful phenomenon by reporting some possible striking outcomes of cyberterrorist attacks. An article titled "The threat that might end the world as we know it" reports:

> "Distance is no defense," writes Greenberg. "Every barbarian is already at every gate. And the network of entanglements in that ether, which have unified and elevated the world for the past twenty-five years, can, over a few hours on a summer day, bring it to a crashing halt." (Hewitt, 2019).

The consequences theme places the emphasis on the likely consequences of cyberterrorist attacks. A Daily News article reporting possible outcomes of an attack against California's power supply is outlined below:

> Experts say energy grids are the new front in cyber-terrorism. Although the wildfires that periodically dominate the news are a serious threat to California's power supply, cyber-invaders are an around-the clock danger, trying to penetrate grid security every minute of every day. An all-hands-on-deck battle is being waged against them, and the network that serves nearly 40 million people's homes, industries and public-safety agencies depends on a successful defense (Cart, 2019).

The administrative theme is composed of articles that reports administrative related issues such as laws, policies, or strategies. An article discussed the Biden administration's investment plans in the realm of cybersecurity as follows:

> Critical infrastructure such as power plants and electrical grids are now targeted by adversaries who have demonstrated elsewhere their capacity to shut off the lights. Where private indu-

> stry has not invested in the cybersecurity to keep adversaries out, security experts say the government must inject investment for the sake of U.S. national interests. But with just 5% to 7% of the Biden plan reportedly going to traditional and future infrastructure, national security experts worry politics and patronage will surpass national security (Mahshie, 2021).

The state-linked cyberterrorism theme involves articles that reports cyberthreats from China, Iran, Russia, and North Korea. This frame includes threats from nation state actors and state-sponsored hacking groups. An article that was published in Springfield News Leader highlighted the cyberthreats that Iran poses as follows:

> Beyond the asymmetric threats Iran poses through its terrorist network, Tehran also presents one of the most aggressive and innovative threats in the cyber realm. Iran will not seek to confront America directly and will look to take advantage of the asymmetric benefits that a cyberattack offers, so this threat will prove significant. The most likely targets will be closely associated with the U.S. government and possibly the U.S. financial sector, which Iran has previously attacked (Brian & Peter, 2020).

The cyberthreats from terrorist groups theme contains articles which discuss cyberattacks launched by terrorist organizations. All these articles reported the cyber activities of ISIS. There has been no article in our sample reporting a cyberattack from another terrorist organization. Below is an example of this frame:

> Indeed, in August, the “Islamic State Hacking Division” sent out a message on Twitter warning the “Crusaders” that it would “strike at your necks in your own lands.” The tweet came with a 30-page attachment listing the personal data of those 1,300 service members and government workers (Barakat, 2016).

The growing threat theme emphasizes the growing threat of cyberterrorism. The articles in this frame discuss the increasing severity of cyber terrorist attacks. The following article covers the ever-increasing danger of cyberattacks:

> The internet and its endless nodes of connectivity, both wired and wireless, simply boggles the mind. The dark side of this phenomena that we call progress is that each point of connection along this digital global highway represents a potential hacking opportunity for those wishing to do harm. Global cyber-security and the construction and management of firewalls is estimated to be a $125 Billion industry and growing at double digit rates. However, it seems that unscrupulous hackers continue to outsmart the good guys (Johnson, 2019).

Finally, the criticism theme involves a contrarian approach, that is, arguing that cyberterrorism is an exaggerated threat that should not be a top priority in the government’s agenda. An article emphasized the fact that there have been no casualties as a result of any cyberterrorist attack:

> Cyber-terrorists have never killed an American citizen, no failed state threatens America and more Americans are killed by lightning strikes than sadistic radicals. “And we are under attack every single day. The threats are relentless." No, they're not (Cohen, 2017).

Table 6. *Themes – Description*

| Themes | Description |
|---|---|
| Critical infrastructure | The article frames cyberterrorism as a threat against critical infrastructure |
| National Preparedness | The article highlights the importance of national preparedness for cyberterrorist attacks |
| Cyber doom scenarios | Cyberterrorism is framed as an extremely devastating phenomenon |
| Consequences | The article emphasizes the consequences of cyberterrorist attacks |
| Administrative (policies, orders, laws etc.) | The article discusses administrative issues and processes |
| State-linked cyberthreats | State-linked groups are discussed |
| Cyberthreats from terrorist groups | Terrorist groups are discussed |
| Growing threat | Cyberterrorism is framed as a growing threat |
| Criticism (exaggerated, etc.) | Criticizing the exaggerated threat of cyberterrorism |

Table 7 demonstrates the number of articles that correspond with each frame. We should note that an article may be coded with multiple themes. Our analysis reveals that growing threat is the most common theme, followed by administrative and state-linked groups themes. More than one-third of the articles in our sample framed cyberterrorism as an emerging threat that should be taken seriously. Another prominent theme, the administrative frame, is supported by 23 articles focusing on administrative issues regarding the threat of cyberterrorism. Those articles mostly discuss policy recommendations, budgetary issues, and cybersecurity strategies. Thirteen articles placed their emphasis on cyber threats against critical infrastructure. Eleven articles reported the likely consequences of cyberterrorist attacks. Some articles discussed how such attacks could damage the economy, while others viewed them as a threat to the social and political order. The national preparedness frame was identified in ten articles. The remaining three frames were rare. Interestingly, our analysis found only four articles that mentioned terrorist groups as the actors behind the attacks. Cyberterrorism, as we realized during the analysis, was generally not framed in a way that refers to cyberattacks perpetrated solely by terrorist groups. The type of attack, not the perpetrator, has been the main determinant when defining cyberterrorism. Contrary to general expectations, cyber doom scenarios were very rare in our sample. Only three articles exaggerated the threat of cyberterrorism to the extent that it could lead to an extremely catastrophic incident. Finally, we identified only one article that criticized how cyberterrorism is considered among the public and politicians.

Table 7. *Themes - Analysis*

| Themes | N | Themes | N |
|---|---|---|---|
| Growing threat | 29 | National Preparedness | 10 |
| Administrative (policies, orders, laws etc.) | 23 | Cyberthreats from terrorist groups | 4 |
| State linked groups | 22 | Cyber doom scenarios | 3 |
| Critical infrastructure | 13 | Criticism (exaggerated, etc.) | 1 |
| Consequences | 11 | | |

## Discussion

Cyberterrorism is becoming a more frightening phenomenon among Americans. It is even more fearful than traditional terrorism within this survey sample. The recent cyberattacks and their coverage in the media

seem to be a driving factor, as our analysis demonstrated. Our quantitative analysis of a nationally representative survey of American adults revealed that reading news is a significant predictor of fear of cyberterrorism. To further investigate the relationship between fear and exposure to media, we collected a sample of cyberterrorism-related media articles and explored how cyberterrorism is framed in the American print media.

Our qualitative analysis showed that most of the time, cyberterrorism is framed as a growing problem that is threatening American society. This is not unexpected as cyber threats continuously evolve, and cyberattacks victimize more businesses and individuals. The Administrative frame is also a prevailing theme, as results demonstrate. The Biden administration vowed to prioritize cybersecurity soon after the devastating Colonial Pipeline hacking incident. As a result, there have been many discussions around new regulations in national cybersecurity.

The most salient result of our analysis is regarding how media define and form a concept of cyberterrorism. Considering that only four articles discuss cyber threats that have emerged from terrorist groups, we can argue that the term cyberterrorism is being used to define cyberattacks in general, not only those carried out by terrorist groups but also by other adversaries. There are 22 articles identified in our sample that report cyberattacks or cyber threats that have emanated from state-linked groups. The analysis shows that the media does not always clearly distinguish cyberterrorism from other cyber threats, such as cyberwarfare.

Our analysis further revealed that the media's portrayal of cyberterrorism differs from that mainly defined in the cyberterrorism literature. Cyberterrorism is a form of terrorism; hence a cyber-attack should fulfill the characteristics of a traditional terrorist attack – such as being ideologically motivated and having far-reaching psychological repercussions beyond the immediate victims (Hoffman, 2018) – to be classified as a cyberterrorist attack. However, many cyber-attacks with criminal intentions and financial motivations are mistakenly associated with cyberterrorism in the media. This misconception of the term cyberterrorism results in its overuse in the media when reporting cybercrimes. Cyberattacks that are indeed not an act of terrorism and are wrongly portrayed as cyberterrorism could increase the fear of cyberterrorism among audiences.

As a policy recommendation from the findings of this research, it is necessary to distinguish the terms when discussing major cyberattacks in the media and use them appropriately to prevent any misrepresentation of cyber incidents. First, the editorial board of the US news media need to pay more attention to the use of the terms "cyberattack," "cyber threat," and "cyberterrorism" to inform the public correctly. Second, it is also beneficial to increase public awareness of cyber threats and their differences to prevent unnecessary fear of cyberterrorism among citizens.

This research used two different datasets: a survey and a collection of news on cyberterrorism. The survey participants were not exposed to the news media content in an experimental setting. Therefore, the study did not measure how a specific theme or news influences different levels of fear among the participants. Future research may benefit from conducting experiments to evaluate the emotional responses of individuals to cyberterrorism news.

**Acknowledgement**

The survey data were downloaded from the Association of Religion Data Archives, www.TheARDA.com

**References**

Barakat, M. (2016, June 16). Man pleads guilty to cyber terrorism in Virginia court. *Daily Press*.

Bastug, M. F. (2021a). *Cyber evolution of terrorist groups*. Orion Policy Institute. https://orionpolicy.org/orionforum/58/cyber-evolution-of-terrorist-groups

Bastug, M. F. (2021b). *Rethinking cybersecurity after colonial pipeline hack*. Orion Policy Institute. https://orionpolicy.org/orionforum/8/rethinking-cybersecurity-after-colonial-pipeline-hack

Bastug, M. F., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict & Terrorism, 43*(7), 616-637.

Benson, D. C. (2014). Why the internet is not increasing terrorism. *Security Studies, 23*(2), 293-328.

Brian, K., & Peter, J. (2020, January 12). Biggest threat from Iran: Cyber, terror attacks. *Springfield News Leader*.

Brickey, J. (2012). Defining cyberterrorism: capturing a broad range of activities in cyberspace. *Combating Terrorism Centre at West Point, 5*(8), 4-7.

Cart, J. (2019, Feb 19). Cyber-sabotage, wildfires, weather - a web of threats to the power supply could leave Californians in the dark. Daily News.

Chapman University (2018). The Chapman University Survey of American Fears, wave 5. Earl Babbie Research Center [producer].

Chapman University (2019). The Chapman University Survey of American Fears, wave 6. Earl Babbie Research Center [producer].

Cho, J., Boyle, M. P., Keum, H., Shevy, M. D., McLeod, D. M., Shah, D. V., & Pan, Z. (2003). Media, terrorism, and emotionality: Emotional differences in media content and public reactions to the September 11th terrorist attacks. *Journal of Broadcasting & Electronic Media, 47*(3), 309-327.

Cohen, M. A., (2017, Apr 25). Homeland Security's John Kelly is unhinged. *Boston Globe*.

Comer, J. S., & Kendall, P. C. (2007). Terrorism: The psychological impact on youth. *Clinical Psychology: Science & Practice, 24*(3), 179–212.

Conway, M. (2002). What is cyberterrorism?. *Current History, 101*(659), 436.

Corbin, J., & Strauss, A. (2008). Basics of qualitative research (3rd ed.): *Techniques and procedures for developing grounded theory*. SAGE Publications, Inc.

Debrael, M., d'Haenens, L., De Cock, R., & De Coninck, D. (2019). Media use, fear of terrorism, and attitudes towards immigrants and refugees: Young people and adults compared. *International Communication Gazette, 83*(2), 148-168.

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

Denning, D. E. (2000). Cyberterrorism: The logic bomb versus the truck bomb. *Global Dialogue, 2*(4), 29.

Denning, D. E. (2013). Terror's web: how the internet is transforming terrorism. In Y. Jewkes & M. Yar (E-ds.), *Handbook of internet crime* (pp. 212-231). Willan Publishing

Dillon, L., Hayes, B. E., Freilich, J. D., &Chermak, S. M. (2019). Gender differences in worry about a terrorist attack: A cross-national examination of individual-and national-level factors. *Women & Criminal Justice, 29*(4–5), 221–241.

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

Gerbner, G. (1969). Toward cultural indicators: The analysis of mass mediated message systems. *AV Communication Review, 17*, 137-148.

Gerbner, G. (1998). Cultivation analysis: An overview. *Mass communication and society, 1*(3-4), 175-194.

Gerbner, G., Gross, L., Morgan, M., & Signorielli, N. (1994). Growing up with television: The cultivation perspective. In J. Bryant & D. Zillmann (Eds.), *Media effects: Advances in theory and research* (pp. 17–41). Lawrence Erlbaum Associates, Inc.

Gerbner, G., Gross, L., Morgan, M., &Signorelli, N. (1986). Living with television: The dynamics of the cultivation process. In J. Bryant & D. Zillman (Eds.), *Perspectives on media effects* (pp. 17-48). Lawrence Erlbaum Associates, Inc.

Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security, 21*(7), 636-647.

Hewitt, C. (2019, Nov 17). The threat that might end the world as we know it. *Star Tribune*.

Hoffman, B. (2018). *Inside terrorism*. Columbia university press.

Hogan, L. & Blair, D. (2021, May 30). Washington has been asleep on cybersecurity. It's time to wake up. *USA Today*.

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing cyberterrorism as a security threat: A study of international news media coverage. *Perspectives on Terrorism, 9*(1), 60-75.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security, 2*(1), 64-87.

Johnson, W. (2019, Dec 13). Our desert homes increasingly exposed to global mischief. *The Desert Sun*.

Lee, C. S., Choi, K. S., Shandler, R., & Kayser, C. (2021). Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events. *Journal of Contemporary Criminal Justice, 37*(3), 333-355.

Littleton, M. J. (1995). *Information Age Terrorism: Toward Cyberterror* [Master's Thesis]. Naval Postgraduate School.

Mahshie, A. (2021, Apr 12). Joe Biden's infrastructure bill exposes America's weak defenses, experts say. *Washington Examiner*.

Nacos, B. L. (1996). *Terrorism and the media*. Columbia University Press.

Nacos, B. L. (2003). The terrorist calculus behind 9-11: A model for future terrorism. *Studies in Conflict and Terrorism, 26*(1), 1–16.

Nellis, A. M. (2009). Gender differences in fear of terrorism. *Journal of Contemporary Criminal Justice*, 25 (3), 322–340.

Nellis, A. M., & Savage, J. (2012). Does watching the news affect fear of terrorism? The importance of media exposure on terrorism fear. *Crime & Delinquency, 58(*5), 748–768.

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror: Prospects and implications.* White Paper. Naval Postgraduate School.

Ogren J. G., & Langevin, J. R. (1999). Responding to the threat of cyberterrorism through information assurance [Master's Thesis]. Naval Postgraduate School.

Oksanen, A., Kaakinen, M., Minkkinen, J., Räsänen, P., Enjolras, B., & Steen- Johnsen, K. (2020). Perceived societal fear and cyberhate after the November 2015 Paris terrorist attacks. *Terrorism and Political Violence, 32*(5), 1047–1066.

Onat, I. (2016). Media, neighborhood conditions, and terrorism risk: What triggers fear of terrorism? Rutgers, The State University of New Jersey.

Onat, I., Guler, A., Kula, S., & Bastug, M. F. (2021). Fear of Terrorism and Fear of Violent Crimes in the United States: A Comparative Analysis. *Crime & Delinquency*. Advance online publication.

Onat, I., Bastug, M. F., Guler, A., & Kula, S. (2022). Fears of cyberterrorism, terrorism, and terrorist attacks: an empirical comparison. *Behavioral Sciences of Terrorism and Political Aggression*. Advance online publication.

Piazza, J. A., & Guler, A. (2019). The online caliphate: Internet usage and ISIS support in the Arab world. *Terrorism and political violence, 33*(6), 1256-1275.

Rapoport, R., & Berta, K. (2018). Methodology report: American fears survey July 2018. SSRS. https://www.chapman.edu/wilkinson/research-centers/babbie-center/_files/fear-2018/fear-V-methodology-report-ssrs.pdf

Rudner, M. (2016). "Electronic Jihad": The Internet as al-Qaeda's catalyst for global terror. In *Violent Extremism Online* (pp. 8-24). Routledge.

Schmid, A. P., & Graff, J. (1982). *Violence as communication: Insurgent terrorism and the western news media*. Sage.

Skøt, L., Nielsen, J. B., &Leppin, A. (2021). Risk perception and support for security measures: Interactive effects of media exposure to terrorism and prior life stress? *Journal of Risk Research, 24*(2), 228–246.

START (National Consortium for the Study of Terrorism and Responses to Terrorism). (2022). Global Terrorism Database 1970 - 2020 [data file]. https://www.start.umd.edu/gtd

Thomas, T. L. (2003). Al Qaeda and the Internet: The Danger of "Cyberplanning". *Parameters, 33*(1), 112.

Vargas, M. (2017, May 16). How two different cyberattack threats could have a catastrophic effect on the US. *Washington Examiner*.

Veerasamy, N. (2009). A High-level Conceptual Framework of Cyber-terrorism. *Journal of Information Warfare, 8*(1), 43-55.

Weimann, G. (2004). Cyberterrorism: How real is the threat? United States Institute of Peace. Retrieved from https://www.usip.org/sites/default/files/sr119.pdf

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism, 28*(2), 129-149.

Wilcox Rountree, P., Ozer, M. M., Gunbeyi, M., &Gundogdu, T. (2009). Gender and fear of terrorism in Turkey. *Journal of Contemporary Criminal Justice, 25*(3), 341–357.

Williams, R. (2016). Understanding and interpreting generalized ordered logit models. *The Journal of Mathematical Sociology, 40*(1), 7-20.

Williamson, H., Fay, S., & Miles-Johnson, T. (2019). Fear of terrorism: Media exposure and subjective fear of attack. *Global Crime, 20*(1), 1–25.