HIGH SCHOOL EDITION
Journal of Student Research

Volume 9 Issue 2 (2020)
AP Research

A Case Study on the Factors of Biometric Counterterrorism Policies as a Result of September 11, 2001

Sharon Liu[1] and Robert Hodgson[1]

[1]McDowell High School, Erie PA, USA

ABSTRACT

Biometrics has emerged as a rapidly moving technology that has been continuously evolving and improving. It has even been incorporated as a form of counterterrorism, preventing incidents of terrorism as well as providing safety measures. While various researchers have analyzed the effectiveness of biometric counterterrorism measures, the factors behind the reasonings of those decision-making process of implementation have been untouched. This paper looks to analyze the factors through a case study on the events of September 11, 2001, using a qualitative thematic analysis to identify the factors. It is important to note that rather than analyzing secondhand sources, this study will analyze firsthand sources throughout the study. Through this study, it can be concluded that there are five main factors behind implementation of biometric counterterrorism policies: ensuring safety if a terrorist incident were to happen, increasing security to prevent the incident from occurring, public sentiment, potential to become in the future, and current effectivity.

Introduction

Terrorism has been utilized as a potent political weapon throughout the international community. Between 1969 and 2009, there were 38,345 terrorist incidents across the world, yielding an average of four fatalities per terrorist attack. In response to these terrorist incidents, different counterterrorism strategies have emerged that utilize new technology. Biometrics is an authentication tool for systems to recognize an individual based on physiological or behavioral characteristics and has become a prominent form of anti-terrorist technology. Since its first appearance in the field of automated fingerprint matching published in 1963, authentication tools have made significant technological progress. In 2006, Singapore adopted biometric features in the country's passports to make forgery and illegal immigration more difficult in the hopes of deterring further terrorists. Moreover, the U.S. National Institute of Standards and Technology reported that from 2010 to 2018, facial recognition technology became about twenty times more effective at finding a matching photograph in a database. Based on a 5% error in algorithms in 2010 falling to a .2% error in 2018, biometrics have improved significantly but still have room to further develop. While many scholars have analyzed the effectiveness of biometric counterterrorism measures, none have looked at the factors behind the decision-making process regarding the implemented measures. This paper aims to explain and analyze why various biometric counterterrorism measures are utilized.

Literature Review

Terrorism

Terrorism is the use of violence through intimidation or fear directed at the general public, designed to extend beyond the immediate victims, which are those that are present onsite. Terrorism can vary across a wide spectrum, but there are three consistent aspects considered fundamental to an act being considered terroristic:

1. The goal of the act is to create and incentivize political change.
2. The perpetrators are distinguished by their non-state character, and while they may receive support from states, such as funding or weapons, they remain rogue actors with their own agendas.
3. The deliberate use of surprise attacks that do not abide by international norms or the accepted standard use of force.

Biometrics

In biometrics, information systems gain controlled access to physical assets by recognizing the individual based on physiological (also referred to as biological) or behavioral characteristics. Physical biometrics refers to recognition of some part of a person's anatomy, such as fingerprints, facial features, or retina. On the other hand, behavioral biometrics refers to the analysis of a person's behavior, including voice recognition, eye movement patterns, or analysis of a subject's walking gait. While physical biometrics are more accurate, due to their consistent stability as a result of many years of research and refinement, this type of information is also extremely invasive and cannot be recovered if the biometric database is ever compromised. Alternatively, behavioral biometrics are not as intrusive to the user; however, behavior biometrics is not as accurate as physical biometrics due to its variability and inconsistency.

In the biometric recognition framework, there are two stages of operation: the enrollment stage and the recognition stage. In the enrollment stage, the biometric system acquires the biometric trait of an individual, extracts the feature, and stores it in a database, often referred to as a template. During the recognition stage, the system undergoes the same process, except it compares its results to the template already in the database from the enrollment stage. Two outcomes may result depending on the type of biometric system.If the system uses biometric authentication, which is the process of comparing the data of the person's characteristics to the data stored, the database would contain only a single person's characteristic, which would be compared to authenticate the person. In other words, it answers the question "Are you who you say you are?" On the contrary, identification seeks to determine the identity of the individual. The goal is to capture an item of biometric data from the individual and compare the data to the database containing multiple people in order to answer the question, "Who are you?"

Varying inferences exist within the field regarding the factors affecting counterterrorism policies; for example, Stanley Feldman conducted a study on public perception and its effect on counterterrorism policies. Through surveys, he was able to conclude the political effects of perceived threat and anxiety, leading to support for government counterterrorism policies. Likewise, Winston Koh, professor of Economics at the Singapore Management University, analyzed economic factors related to counterterrorism policies; he found that without sufficient economic resources, implementation of policies would not be able to occur. In the field of political science, it is a general consensus that various factors, such as those stated above, may be contributing factors towards policymaking. However, both researchers lack biometric security measures in their studies. Of course, this lack of measures may be partly due to the fact that biometrics is a relatively new form of technology. Although researcher Nikolas Kairinos focused on biometric policies and how they are implemented, he fails to examine the counterterrorism aspect in his studies. While his research primarily focuses on biometric policies, it fails to incorporate the usage of biometric policies specifically designed to address terrorism. Additionally, he lacks a replicable method and sufficient data to prove his theories, which many other researchers criticize.

While studies in biometric counterterrorism have been abundant, there is a gap within the literature: no study has adequately analyzed the factors behind the decisions of those states implementing biometric policies. For example, in 2004, the United Kingdom enforced the use of 10,000 identity cards using biometric features. Many researchers have analyzed the effects, including benefits and repercussions, of this policy. However, analysis of the reasoning behind implementation of these policies is lacking. No research has found the overarching theme in efforts behind biometric counterterrorism policies. While examining the effects of actions is important, observing the reasoning of the actions taken in the first place is just as, if not more, important. For example, in the case of a terrorist attack, one does not simply look toward its aftermath; rather, attention should be focused on examining the root cause, as it would be crucial to preventing the same result. In this paper, the incentives, beyond its proven effectiveness, in implementing biometrics as a counterterrorism policy will be examined. Thus, this paper seeks to analyze the different factors that result in biometric counterterrorism policies using a case study of the events of 9/11 along with the United States' response.

Method

Expectations

My method was designed to address the question, "Through a case study of the terroristic events of September 11, 2001, what are the factors behind implementation of biometric counterterrorism policies in the United States?" While there may be a variety of case-specific explanations for counterterrorism policies, I expect the main factors contributing to biometric counterterrorism policy to be the amount of research and development (R&D) on biometrics and public support. Feldman's studies highlight the importance of public support, and not only does the sentiment of the public influence the type of counterterrorism policy pursued, but it also pushes the government to take action. Other studies have showed that heightened public anxiety tends to result in domestic surveillance counterterrorism policies, whereas perceived threat results in heightened support for domestic and international government actions to combat the threat of terrorism, including overseas military action. However, I also expect the economy to have a significant impact on biometric policies. Economic capital influences the amount of money that can be dedicated to R&D in biometrics; as Koh identified, R&D is crucial to the growth of biometrics and, therefore, would influence the implementation of biometrics in counterterrorism policies.

Case Study

To assess the factors behind biometric counterterrorism policies, a case study was utilized, which included a careful examination of organizations, events, and phenomenon. This research focuses on a case study of the United States after the events of September 11, 2001 (also known as 9/11). Almost 3,000 people were killed as the Islamic extremist group Al-Qaeda hijacked four planes, crashing them into the World Trade Center in New York City, the Pentagon in Washington, D.C., and a field in Shanksville, Pennsylvania. The specific case was chosen due to 9/11 being classified as a major terrorist incident that occurred within the age of biotechnological development that triggered major U.S. initiatives to combat terrorism. Additionally, the event has been utilized as a case study constantly as a way to structure and focus analysis by other researchers within the political science field. A case study method allows for thorough analysis and investigation of the factors involved in biometric counterterrorism policy. The goal through the usage of this type of method is to highlight how different factors contribute to biometric counterterrorism policy making. Narrowing the research to a case study is the most effective way to analyze the data as there are many cases of the implementation of biometrics as an anti-terrorism policy. Additionally, a case study method allows for information to be collected and examined through a thematic analysis, as policymaking choices vary based on the event.

Numerous U.S. law enforcements and biometric security systems have been implemented since the events of 9/11; however, it is important to keep in mind that the goal of this paper is to identify the reasoning behind the implementation of these policies. Perhaps the most widely known is the US-VISIT, developed by the Department of Homeland Security to track the arrival and departure of foreigners through automated biometric control systems. The US-VISIT program has visitors' index finger scanned and a digital photo taken, which is saved to a biometric database.

Source Selection

There exists a substantial body of literature regarding biometric counterterrorism policies; however, it is important to differentiate the types of documents. Since the research is primarily based on the sources themselves, as interpretations are derived from the sources, it is imperative that the sources selected to be analyzed fit a specific framework and meet certain criteria. Primarily, the sources should be first-hand data rather than previously analyzed texts or papers. A multitude of first-hand sources are focused upon, including documents from government agencies, public opinion/polling numbers, testimonies, etc. Each source was selected due to its first-hand data, so that I may make my own individual analyses. For example, if researcher X analyzes a congressional testimony, rather than analyzing researcher X's findings, I will be analyzing the congressional testimony itself. Researcher X's writing would be considered a second-hand source, whereas the congressional testimony that researcher X has analyzed is the first hand source that will be targeted within this study. Another important aspect to be taken into consideration is the focus of analysis; rather than a generalization of entire documents, the focus should remain on biometric counterterrorism policies. These sources originated from the Electronic Privacy Information Center (EPIC), a research center in Washington D.C. EPIC is a nonprofit organization serving as a database of primary sources for technological information, specifically governmental policies. Sources were selected by using the search words, "biometric counterterrorism policies", "biometric", "counterterrorism", "policy", "9/11", "September 11", and "factors." The sources were then sorted to determine whether they would be suitable for the study, as they had to fit the criteria of being a first-hand source. As the sources were derived from the search words, they were considered relevant enough to the topic at hand. A total of 24 sources were selected to take into account the development of technology and improvement in biometrics.

Qualitative Thematic Analysis

Qualitative analysis centers on analysis on the text, and the connections between one another. Specifically, it can be defined as the "rational organization of such categories that condense the substantive meanings of the given text, with a view to testing pertinent assumptions and hypotheses." In accordance to what is commonly utilized in the field of political science, a thematic analysis was used to identify the various factors in biometric counterterrorism policies. Rather than just counting phrases and words in a text, which is commonly used in a content analysis, qualitative thematic analysis explores the underlying meaning within the data through grounded coding. Grounded coding is identifying the overarching themes from the documents themselves.

Thematic analysis determines overarching common themes in a sample of collected data. The method of a qualitative thematic analysis, which combines a qualitative analysis and a thematic analysis, allows analysis of common "themes", or factors, that can be applied to a determinant of biometric counterterrorism policies. I conducted my qualitative thematic analysis in three main steps: first, I selected my sources from a database, EPIC, while utilizing specific search words as referenced before. Next, I read the sources multiple times while annotating to familiarize myself with the content, identifying, or "coding", the similar components regarding biometric counterterrorism policies. Factors were identified by the main message being given to the audience, which indicated types of motives to lead toward the formation of biometric counterterrorism policies. The goal of this step was to determine specific factors which may lead to a biometric counterterrorism policy. After the identification of the similar factors were revealed, they were analyzed on how they could affect the formation of a policy- specifically biometric counterterrorism. These similar factors were categorized into groups, labeled as general themes, which would be recorded and compared to other themes.

For example, if source A contained reference to public support, source A would be classified under the public category. If source B suggested the use of biometric counterterrorism policy as a means to pacify the public and give the public a sense of safety, it would be taken into the public and safety category. Afterwards, when sorting into general themes, sources A and B would be a part of the public sentiment theme, but source B would also be included into the safety theme. Tallying the final results, based on the number of times biometric counterterrorism policies corresponded with a specific reasoning, a conclusion could be reached.

Data and Analysis

Findings

The following table highlights the five main themes identified regarding biometric policy formulation and implementation. These five themes are: (1) Security, (2) Safety, (3) Public Sentiment, (4) Potential in Future Endeavors, and (5) Current Amount of Investments. The table below defines the five factors to establish a clear distinction. The last column quantifies the number of sources the theme appears in. For the purpose of a clear analysis and line of reasoning, these factors will not be discussed in isolation or individually, rather, they will be analyzed in the larger context of 9/11 and the effects of those events.

Table 1

Themes	Definition	Number of Sources
Security	Measures taken to ensure being free from danger or threat; specifically designed to prevent a terrorism incident from occurring	17
Safety	Being protected from or unlikely to cause danger, risk, or injury. If a terrorism incident were to occur, the measures taken to keep citizens safe	15
Public Sentiment	The overall population's attitude based on their thoughts and feelings	8
Potential in Future Endeavors	The extent in which technology can improve towards if continuous support is provided	10
Effectivity	Successful in producing a desired or intended result in the present according to scientific data	13

Discussion

One of the main issues identified after the events of 9/11 was the lack of airline security; hence, congressional members focused on a means to tighten security and increase public safety. Dianne Feinstein, a senator from California who strongly advocated for biometrics to be implemented as a means of counterterrorism, describes biometrics in airports as being "used to screen employees and control access to sensitive areas… preventing terrorists from getting a job as an airline or airport employee or posing as one in order to get access to implement a hijacking." Almost immediately after 9/11, airports such as the San Francisco International, Chicago O'Hare, and Charlotte Douglas implemented biometric usages for two main reasons: (1) to detect previous criminals and terrorists, and (2) to ensure passengers remain safe while in the air. In the context of 9/11, where terrorists took control of planes and were therefore able to crash into the twin towers, implementing biometric security measures on sensitive areas such as the pilot's cockpit ensured only the staff and the pilot may enter. Strom Thurmond, a senator from South Carolina, adds that "biometrics can be used to compare to a biometric database of criminals or terrorists… so a terrorist whose picture or fingerprint is in a law enforcement database can be stopped before boarding a plane or entering a country." Many others reference back to the usage of biometrics in airports as a means to ensure public safety and tighten security within the country, specifically closing loopholes that enabled the 9/11 attack.

The Integrated Automated Fingerprint Identification System (IAFIS) is a computerized system maintained by the Federal Bureau of Investigation (FBI) since 1999, and has been continuously referenced as an example of the standard for future biometric counterterrorism programs. Michael D. Kirkpatrick, assistant director of the Criminal Justice Information Services Division of the FBI, highlights the IAFIS's ability to retrieve, search, and store fingerprints while generating responses within two hours for a match. Kirkpatrick further demonstrates the effectiveness of biometrics in regard to the 9/11 incident; in relief support, the IAFIS was able to identify victims through fingerprints. He states: "The IAFIS is a high-volume system with a capacity for growth. In 2001, fingerprint receipts totaled 15,451,543, which equates to 1.3 million receipts per month… in addition, each day on average we add 7,853 new searchable entries to the database." Through the success of IAFIS, an example is set for the potential of future biometric systems based only on the technology available during that time (2001). Not only did biometric systems prove effective through the use of quantitative data, but they also signified the ability to improve in the future. It indicated the potential that biometrics could become, just from the improvement that was made within two years and the significant advancement that is made daily. It is important to note that rather than referring to the actual effects, many are actually referring to what the policies could potentially lead to; however, it does not signify what its actual effects are. Monte Belger, the acting deputy administrator of the Federal Aviation Administration (FAA), says "Our fundamental goal is 100 percent screening of all passengers, baggage, airport and airline personnel, and we believe that these systems [biometrics] have a role in the future." Belger depicts a future in which every person can be identified through biometrics, painting a potential future if biometric counterterrorism policies were to be implemented. It highlights the theme of potential in future endeavors, which is added on by Kirpatrick's statement of the IAFIS's effectiviness; Kirpatrick's statement in itself contributes to the theme of effectiveness due to its success, proven by numerical and scientific data.

Beyond airline safety and security, however, many policymakers noted the importance of border security. Orrin G. Hatch, a U.S. Senator from Utah, explains "to protect our nation from terrorists, we need to tighten our border security… by embracing new pioneering technologies [biometrics]." Senator Mike DeWine of Ohio incorporates the theme of security in his support for passing biometric counterterrorism policies in regard to border security as he describes a process of livescan fingerprint devices for those who wish to apply for a visa from their home countries. The data would be transmitted to the FBI for a criminal record check and saved to a database, so "prior to them coming to their country is, in fact, the person who shows up at our borders." DeWine illustrates a prospective future in which those within the border will remain secure through the protection of biometrics, which would ensure the identity of those coming into the country. Martin Huddart, the general manager of a recognition systems company, refers to the theme of effectiveness as he cites the Ben Gurion Airport in Tel Aviv, Israel, as a model in regard to biometric border systems. He describes the airport as "one of the world's most security-conscious airports. Twenty-one kiosks process 50,000 passengers per month today… the line to get through immigration can go from 60 minutes down to 20 seconds by verifying the identity of travelers where both hand geometry and face recognition is being used." Huddart urges his audience to model the Ben Gurion Airport, suggesting that the same effect may result if implemented. Through the usage of providing an example that has implemented biometric counterterrorism policies with success, it encourages the idea that the same can occur within the United States. Just as the Ben Gurion Airport has proven to be productive in border security systems, it reflects the effectiveness of biometric counterterrorism policies if they were to be implemented in airports within the United States.

Public sentiment has been a common occurrence in statements. Congressmen describe the need to pacify feelings of fear and mistrust between the government and its citizens; more specifically, building a feeling of trust that the government can protect its people. Monte R. Belger, acting Deputy Administrator of the Federal Aviation Administration, asserts that "action reflects both the Department's and the FAA's [Federal Aviation Administration] unyielding commitment to civil aviation security and the restoration of public confidence in the nation's air transportation system." Belger notes that any action taken would be beneficial towards boosting the morale of the public, as it relays the importance the United States places the public. However, Belger's statement is not considered to be relevant to the theme of public sentiment, as it fails to focus primarily on biometric counterterrorism policies; rather, it focuses on actions as a whole rather than actions specifically targeted in the realm of biometric counterterrorism policies. Harris Poll, a market research and global consulting firm, on the other hand, conducted a telephone poll shortly after September 11 that showed 86% of the American public endorsed the usage of facial recognition to spot terrorists. This source would be deemed suitable for the theme of public sentiment, as it is relevant to biometric counterterrorism policies specifically, since facial recognition is a form of biometrics. Since the survey was conducted shortly after the events of September 11, it reflects the fear and uncertainty held by the public that can be mollified through solutions from the government, such as various forms of biometric counterterrorism policies, like facial recognition.

However, while many sources provide support for biometric policies, it is also important to address those that do not support biometric counterterrorism policies. One of the highlighted reasons is the invasion of privacy, specifically, the question of whether it is an encroachment of the first amendment rights to privacy. Although this proves to be a difficult obstacle, various spokespersons of tech companies have proposed solutions. An example is Joseph Atick, Chairman and CEO of Visionics Corporation. He explains that "the concern for privacy has to do with the misconception that the ID system is identifying every one of us… It is simply a criminal and terrorist alarm. If your face does not match one on the database, on the watchlist, there will be no alarm. There will be no record of you even going through the system." Rather than restricting rights of people, Atick assures that the system, if implemented, would only serve to compare data received with previously encoded data to identify if there is a match. Thus, only those that have a criminal record would a match take place.

Limitations

Before moving on to the conclusion of the research, it is important to identify potential limitations that may have impacted the data analysis. The two major limitations were sample size and subjectivity (i.e. human error). Taking into consideration the numerous first-hand sources regarding biometric counterterrorism policy making, 24 is a minuscule amount. Due to this limitation, it is possible I may have misconstrued my analysis, as an increase in the number of sources analyzed could produce a more accurate conclusion. However, due to time constraints, a larger sample size could not be taken. Additionally, some databases require monetary payment for access, which limits the range of databases to acquire sources. As an effect of time constraints, I was also unable to analyze multiple case studies, so the primary focus was on the case of 9/11. The second limitation is the most prevalent within this study; as I was the sole researcher in this study, the quantitative analysis would be inherently subjective, which could lead the analysis to be biased. Usually there would be more than one coder to avoid subjective results, as the proposed intercoder reliability agreeance rate is 90%. Siegfried Kracauer points out that "different analysts will arrive at similar conclusions with regard to many texts." Unfortunately, there was only one coder available. As a result, human error could have occured during the analysis. However, despite the lack of additional coders, it is important to recognize that a qualitative content analysis is the best way to analyze factors behind biometric counterterrorism policies; so despite the discrepancy due to the nature of content analysis, the results of this study allows new insights for further research.

Conclusion

In essence, the results of this study suggest that there are five contributing factors toward implementation of biometric counterterrorism policies: ensuring safety if a terrorist incident were to happen, increasing security to prevent the incident from occurring, public sentiment, potential to become in the future, and current effectivity. The initial hypothesis was incorrect; rather than increased R&D as the driving factor behind the implementation of biometric counterterrorism policies, it was mainly from the motive of providing safety and security, as those themes had the largest number of sources that included the theme. While public support was a contributing factor, it held the least number in sources. Thus, half of the hypothesis was proven true, but the other half (R&D), was proven to be false. Thus, there are multiple implications to these conclusions.

There are several implications of this study: it not only contributes to the works within the field of political science, but it also heavily affects future policies. These findings extend existing studies of biometric counterterrorism policies. Beyond policymaking, they suggest the importance of studying specific factors that may play an important role in future policies, and what drives the policies to be implemented. In a relationship where every result has a driving factor, it is imperative to not only analyze the effects, but also the causation. This is especially true in the field of political science, where policymaking plays a heavy role in political changes.

As addressed in the discussion section of this paper, many are worried of the effects of biometric systems being implemented and what it means for individual privacy. This study may assure people that the government has multiple valid reasons to implement biometric counterterrorism policies, with the plausible issue of infringement on privacy kept in mind as well.

Future research may incorporate biometric counterterrorism policies as a whole, rather than narrowing it down to a case study specific. This could eliminate the time-constraint limitation of this study. Additionally, as addressed before, a major limitation of this study is the lack of intercoder reliability, which may pertain towards a qualitative bias during analyses. Future research may have multiple coders to address this limitation. Furthermore, research on association between policymakers' views, such as the impact of their political party or views on the implementation of biometrics may also be a point of further research. Another form of research for the future may be the association between economic prosperity and implementation of biometrics, which would extend Koh's previous research by incorporating specifically biometric counterterrorism policies rather than just counterterrorism policies as a whole.

References

Bardach-Yalov, Elina. "Analyzing Russian propaganda: Application of Siegfried Kracauer's qualitative content analysis method." Journal of Information Warfare 11.2 (2012): 24-36.

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative research journal, 9(2), 27.

Carey, J. W., Morgan, M., & Oxtoby, M. J. (1996). Intercoder agreement in analysis of responses to open-ended interview questions: Examples from tuberculosis research. CAM Journal, 8(3), 1-5.

Crane, M. A., Levy-Carrick, N. C., Crowley, L., Barnhart, S., Dudas, M., Onuoha, U., ... & Ozbay, F. (2014). The response to September 11: a disaster case study. Annals of global health, 80(4), 320-331.

Garson, G. D. (2002). Case study research in public administration and public policy: Standards and strategies. Journal of Public Affairs Education, 8(3), 209-216.

Grbich, Carol. (2013). "Qualitative Data Analysis" (2nd ed.). The Flinders University of South Australia: SAGE Publications Ltd.

Guest, Greg; MacQueen, Kathleen; Namey, Emily (2012). Applied thematic analysis. Thousand Oaks, California: SAGE Publications. p. 11.

Hall, T. H., & Ross, A. A. (2015). Affective politics after 9/11. International Organization, 69(4), 847-879.

Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). Threat, anxiety, and support of antiterrorism policies. American journal of political science, 49(3), 593-608.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80-105.

Kairinos, N. (2019). The integration of biometrics and AI. Biometric Technology Today, 2019(5), 8-10.

Kalaiselvi, S., UniversityKaraikudi, A., India, T., Jothi, R. A., India, T., & Palanisamy, V. (2018). Biometric Security with Iris Recognition Techniques: A Review. International Journal of Pure and Applied Mathematics, 118(8), 567-572.

Koh, W. T. (2007). Terrorism and its impact on economic growth and technological innovation. Technological Forecasting and Social Change, 74(2), 129-138.

Lukyamuzi, L., McKenzie, S., Parks, C., & Smith, T. (2019). A Brief Look into Biometrics and One Use in Higher Education paragraphs 3-4

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. Psychological methods, 4(1), 84.

Morgan, D., & Krouse, W. (2005, February). Biometric identifiers and border security: 9/11 Commission recommendations and related issues. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Muhlhausen, David B., and Jena Baker McNeill. Terror trends: 40 years' data on international and domestic terrorism. Heritage Foundation, 2011.

Nacos, B. L., Bloch-Elkon, Y., & Shapiro, R. Y. (2007). Post-9/11 terrorism threats, news coverage, and public perceptions in the United States. International Journal of Conflict and Violence (IJCV), 1(2), 105-126.

Technikgestaltung, P. (2004). Biometric Identity Cards: Technical, Legal, and Policy Issues. In ISSE 2004—Securing Electronic Business Processes: Highlights Of The Information Security Solutions Europe 2004 Conference (p. 47). Springer Science & Business Media.

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. Nursing & health sciences, 15(3), 398-405.

Walls, E. (2017). Waves of Modern Terrorism: Examining the Past and Predicting the Future (Doctoral dissertation, Georgetown University).

Zucker, D. M. (2009). How to do case study research. School of nursing faculty publication series, 2.