Free literature review about united states vulnerability to cyberterrorism

Society, Terrorism

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

A Political Approach

Introduction

The purpose of this literature review is to provide an analysis of the United States' potential vulnerability to cyber terrorism attacks on its critical infrastructure system. Some experts suggest that the United States is not as vulnerable to cyber attacks and acts of cyber terrorism as many critics believe. American's direct and indirect involvement in growing uncertainties in the Middle East have sparked new debates and concerns regarding the threats new types of cyber terrorism now pose to the nation's data and information security (Abdulrahman, 139). Most importantly, this literature review has been conducted on the basis of answering the following research question: Do the current United States policies regarding conflict in the

Middle East make the U. S. more susceptible to threats of cyber terrorism? Each literary source referenced in this paper provides insight into the concept of cyber terrorism and how potential threats affect the United States. This includes the discussion of how cyberterrorism is defined, various characteristics and aspects of the approach, the organizational contexts that prove most successful for transformational leaders, and how gender differences might hinder effectiveness within organizations.

Methodology

This literature review has been composed by research derived from eight credited, scholarly sources. The majority of the sources are peer-reviewed articles, and two sources are derived from particular chapters within textbooks. In regards to locating the peer-reviewed articles, key words such as cyber terrorism, infrastructure attack, information attack, political theory, U. S.-Muslim relations were utilized through the online library database as other legitimate academic search engines. Due to the growing popularity of published literary works composed about threats of cyber terrorism in America, Academic Search Premiere by EBSCOhost Publishing returned a plethora of adequate research articles for each of the key words and phrases entered into the on-line database. Therefore, rather than discussing each literary source individually, the most common themes found among the research will be discussed in segments.

Cyberterrorism

There are also four categories of attacks that encompass acts of cyberterrorism that can potentially be utilized by terrorists: infrastructure

attacks, information attacks, technological facilitation, and promotion. Infrastructure attacks, information attacks, technological facilitation and promotion (Taylor et al., 132). Each of these categories holds their own degree of importance and relativity in aiding to explain the psychological and political basis for modern-day cyberterrorism. We will be discussing these categories in more detail as they pertain to each section throughout this piece.

Currently, terrorist organizations and other radical groups have ultimately failed to successfully perform a cyber attack on the United States (Ariely, 176). Regardless, the concept has received widespread attention in the past decade, and has ultimately found that the threats and likelihood of these types of attacks are very real and greatly deserve the attention they have acquired. Studying terrorists and terrorist groups has aided in understanding terroristic (group and individual) behavior, motives behind this behavior, resources and knowledge available to execute cyber attacks, potential targets, and has also led to the development of counter-terrorism strategies (Abdulrahman, 142).

It is accepted that acts of cyberterrorism are primarily used to obtain political objectives, and are also ideologically motivated. The motivations behind these attacks, when known, provide insight into the motivations of individual terrorists and terrorist groups as well; they are both politically and psychologically driven to engage in this behavior. While political agendas often change, ideologies rarely do not, and it is difficult to determine whether a psychopathological approach or a political approach is best suited in explaining terroristic behavior. Yet, does the shift from conventional

means of terrorism to digital means of cyberterrorism exemplify a shift in the political and/or ideological agendas of terrorists as well? The answer remains unclear (Abdulrahman, 144).

Cyber terrorism and Political Theory

As previously mentioned, it appears that terrorism is better defined by understanding the implications of ideologies and political goals held by terrorist groups and terroristic individuals. Aside from the definitive aspects that characterize terrorism, as previously mentioned, there is also a shared consensus among experts and researchers that terrorism is fundamentally political as well (Ariely, 179). Terrorists and terrorist organizations desire global media and political attention, maliciously choose a target audience, attempt to disrupt normal routines of society and destroy viable economies, and provoke the enemy interest to overreact to terrorist activity (Eriksson & Giacomello, 207).

Anti-American Sentiment in the Radical Muslim World

The influence of the terrorist group on the individual allows for internalization of the group’s ideologies, and repetitive dehumanization of the enemy allows for the individual to become desensitized morally. Terrorists are driven by their ideologies, as their belief system is what controls their thinking and their actions (Eriksson & Giacomello, 206). Governments, groups, and individuals that do not confirm to fundamental Islam are often obscured to be enemies.

Terrorist groups such as al Qaeda, Hezzbollah, and Muslim Brotherhood have largely disagreed with American foreign policy and presence in the Middle

East since occupation began decades ago. Recent Israel and U. S. relations, for example, have strengthened anti-American sentiment within the radical Muslim world. Evidence suggests that all of these groups are highly capable of executing cyber attacks, regardless of the fact that none have yet to execute a successful cyberattack against the United States. Yet these terrorist organizations, and others, perceive developed and highly technological-dependent Western countries and their use of complex communication systems, energy, and computer networks to be threats to fundamental Islam itself (Al-Kawi, 420).

Terrorist organizations are all too familiar with developed nations and their reliance on critical infrastructure. This, coupled with growing hostilities towards the United States, makes the threat of cyber attacks all the more real and probable. As technology advances and computer and Internet use becomes increasingly globalized, as do the risks of potential cyber attacks. The Internet has aided in the promotion of cyberterrorism and the advancement in online communications enabling for technological facilitation of attacks. Anonymity allows an unnerving layer of protection for terrorists and terrorist organizations when conducting their online affairs.

United States Policy in the Middle East

Some experts question whether or not the United States is as highly vulnerable to cyber attacks as the majority believes. This skepticism is central to the idea that terrorist organizations and other radical groups have ultimately failed to successfully perform a cyber attack on the United States (Al-Kawi, 420). Yet, the United States undoubtedly faces growing hostilities

within the Middle East, and as digital terrorism continues to spread, many support the belief that America’s vulnerability increases as well (Jarvis, Macdonald & Novri, 74). This is further exemplified by U. S. involvement in the Israeli and Palestinian conflict that has been occurring over a period of time. The United States has repeatedly sided with Israel throughout the duration of the conflict, and more importantly, continues failing to recognize Palestine as a nation-state, which in two-thirds of the United Nations General Assembly currently does. Israel outwardly presses and exercises its desire to remain an ethically preferential state (Jewish rather than Muslim or Christian), and continues to illegally acquire Palestinian territories despite such actions being breeches of international law (Al-Kawi, 424).

Yet, U. S. support of Israel throughout the Israeli/Palestinian conflict has remained unwavering, and experts are quick to express that the animosity being displayed towards the United States by Palestinians and other Muslims certainly comes as no surprise. In fact, America’s commitment to Israel's security and livelihood has been a foundation of U. S. policy in the Middle East since Israel was founded in 1948, and obviously, these policies have never fared well among the Palestine nation. Israel and U. S. relations, overall, have strengthened anti-American sentiment within the radical Muslim world, including Muslim fundamental and radical groups such as al Qaeda, Hezzbollah, and Muslim Brotherhood (Al-Kawi, 421). As these groups strengthen through promotion, as does their technological facilitation and probabilities of successfully implementing an infrastructure or information attack. Evidence suggests that all of these groups are highly capable of executing cyber attacks, and perceives the United States and its use of

complex communication systems, energy, and computer networks to be threats to fundamental Islam itself (Jarvis et al., 74).

The Risk of Critical Infrastructure Attacks

Almost every essential aspect of American life is webbed into its critical infrastructure systems, and the United States has self-proclaimed itself as being the most infrastructure reliant of any nation on earth. This online infrastructure includes power, water, transportation, telecommunication and financial systems, and is accessible to the public online (Kallberg & Thuraisingham, 234). Therefore, the U. S. critical infrastructure is extremely vulnerable to attacks and technological facilitation. Skilled cyber criminals have the ability to perform information and infrastructure attacks, which could potentially hinder the security of all Americans. The protection of these systems is vital, yet America has become so technologically advanced in the last half-century that our society's reliance on computers and online networking has become an easy target for cyberterrorists (Larvis et al., 69). Many terrorists have recognized the clear advantage of scheming attacks on computer systems rather than waging traditional wars on America's homeland. However, cyber-attacks on its critical infrastructure could also result in the prevention of a military response to a conventional attack. Moreover, the loss of power, communication, water, financial systems, and transportation would definitely result in complete chaos; an entire country in distress. Digital crime and digital terrorism is not bound by physical borders, which is why the nation's critical infrastructure will never be completely safe from attacks (Kallberg & Thuraisingham, 233).

Conclusion

Little doubt remains that the U. S. has become increasingly vulnerable to cyber attacks, similar to other technologically advanced and developed nations in the Western world. America's political stance in the Middle East and on the Israeli/Palestinian conflict, coupled with its heavy reliance on critical infrastructure, continues to escalate the vulnerability that country faces. Still, some experts believe that terrorists do not yet have the capability to effectively execute a cyber attack on the United States. Recognizing and assessing our vulnerabilities to cyber attacks will be vital in maintaining the safety of American lives.

Works Cited

Al-Kawi, Ahmed. " Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army." Vol. 30, 3 420-428

Alqahtani, Abdulrahman. " Awareness of the Potential Threat of Cyberterrorism to the National

Security." Journal of Information Security 5. 4. (2014): 137-146. Web. 1 Dec 2014.

Ariely, Gil. Adaptive Responses to Cyberterrorism. New York: Springer New York, 2014. 175-

195.

Cavelty, Myriam. " From Cyber-Bombs to Political Fallout: Threat Representations with an

Impact in the Cyber-Security Discourse." International Studies Review 15. 1. (2013): 105-122. Web. 1 Dec 2014.

Eriksson, Johan & Giampiero Giacomello. “ International Relations, Cybersecurity, and Content
Analysis: A Constructivist Approach.” The Global Politics of Science and Technology 2. 1. (2014): 205-219. Web. 1 Dec 2014.

Jarvis, Lee, Stuart Macdonald & Lella Novri. “ The Cyberterrorism Threat: Findings from a
Survey of Researchers.” Studies in Conflict & Terrorism 37. 1. (2013): 68-90. Web. 1 Dec 2014.

Kallberg, Jan & Bhavani Thuraisingham. " From Cyber Terrorism to State Actors’ Covert Cyber
Operations." Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies (1 ed). Ed. Babak Akhgar; Simeon Yates. Oxford UK: Butterworth-Heinemann, 2013. Print & Online. 229-233.

Taylor, Richard, Edward Fritsch, John Liederbach & Thomas Holt. Digital Crime and Digital
Terrorism (2nd ed.). Upper Saddle River: Prentice Hall, 2014. Print.