International Social Science Review

Volume 94 | Issue 1 Article 4

A Question of Triumph: Effectively Measuring the Success of Intelligence against Terrorism

Whitney W. Gibbs

A Question of Triumph: Effectively Measuring the Success of Intelligence against Terrorism

Cover Page Footnote
Whitney Gibbs is a postgraduate student at the University of Leicester. She wrote this paper while completing her Master of Arts degree in Intelligence and Security Studies at the University of Leicester.

A Question of Triumph: Effectively Measuring the Success of Intelligence against Terrorism

On July 7, 2005, British intelligence failed to anticipate a series of terror attacks upon London's transportation services, resulting in more than 700 injured and the deaths of fifty-two British citizens in what would become known as the "worst single terrorist atrocity on British soil."[1] Starting towards the end of the twenty-first century, governments were forced to address the rise of terrorism and terrorist-inspired acts that struck every corner of the globe.

As governments' time, funds, and resources are bolstered in order to combat these threats and the deadly risks, attacks continue to happen as almost a daily occurrence. For this reason, civilians frequently question if intelligence gathering vis-à-vis terrorism is successful and, if it does yield success, how can that success be effectively measured? This article discusses possible successes of intelligence against terrorism such as prevention, minimization of impact, and prior forecast of future attacks in order to demonstrate how success can, in fact, be measured in regard to specific objectives of intelligence against terrorism, rather than simply the intelligence process against terrorism as a whole.

The Code of Federal Regulations defines terrorism as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."[2] Though terrorism affects every corner of the globe, this article will focus of terror attacks within the United States, Great Britain, and France. The article will use both examples of significant terror incidents and publicly available statistics from intelligence organizations in order to prove explore this topic.

Counterterrorism Intelligence

Intelligence in counterterrorism efforts has been the center of much debate and criticism. Daniel Byman, a professor of Security Studies at Georgetown University, contends that the lack of understanding of the capabilities of intelligence in counterterrorism and the emphasis placed on

intelligence to prevent all cases of terror against a nation have led to the neglect of intelligence use within the counterterrorism system.[3] Byman further suggests that intelligence is, in fact, crucial to counterterrorism. It is simply not recognized because the understanding of intelligence success and failure is greatly reliant on intelligence organizations' ability to prevent all future terror acts, while paying little attention to the utility of intelligence to the day-to-day efforts of counterterrorism agencies—which in itself may help to prevent attacks that are never carried out.[4] Michael German, Rosa Brooks, and the Editorial Board of the *New York Times* disagree with Byman's view. They suggest that intelligence is only significant in quelling offensive attacks against a nation, or in cases of national security issues when they arise, rather than as a way to address ongoing prevention of terrorism growth; therefore, it is unable to prevent the growth of terrorism.[5] It does not yield success because terrorism will continue to threaten a nation or nations. Byman, German, Brooks, and the *New York Times* Editorial Board all present relevant points. If intelligence is helping prevent daily threats of terrorism, it is then proving its utility within the counterterrorism community. However, if the goal of counterterrorism is to definitively prevent the growth and promote the dismantling of terrorist groups, does intelligence fail, as it has not proven to do so?

To answer this, one must look to the definition of counterterrorism. The United States Joint Chiefs of Staff define counterterrorism as "activities and operations that are taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."[6] Although terrorism has a long history dating back to the French Revolution, counterterrorism as a designated practice was not adopted extensively by intelligence communities around the world until after World War II. The first use of counterterrorism intelligence against a terror group was in 1883, when British Home Secretary Sir William Harcourt established the Special Irish Branch as part of the Criminal Investigation Department of London's Metropolitan Police force with the goal of combatting Irish republican

terrorism by means of infiltration and disruption.[7] It is activities or operations that help to stop terror groups from committing acts against society; this then would prevent the group from instilling fear in order to achieve their specific goal. Without the achievement of these goals, there is little prospect for growth of the group. This does not by any means suggest that counterterrorism's goal is not to dismantle a group completely; but, rather, that this is the end goal and by succeeding in thwarting terror acts, this goal has the potential to be achieved. In working to render a terror group incapable of using violence against a population, there must be an explicit understand of the group's structure, capabilities, and future plans. Intelligence provides this means of understanding through the use of the intelligence cycle.

The Intelligence Cycle

The intelligence cycle, a five-stage process consisting of planning and direction, collection, processing, analysis, and dissemination through which raw data is analyzed and developed into completed intelligence, has played an integral role within the intelligence community since its formation during the First World War. Most of the same components of the intelligence cycle are utilized, while adaption and addition of other components are necessary in order to combat the inherent challenges, such as pinpointing terror targets and collecting intelligence, which surround intelligence within counterterrorism. The most evident difference is in the means of collection, specifically the origins of the intelligence. When using a standard intelligence cycle model, intelligence is collected on known targets by means of informants, electronic communications, written communications, or surveillance. As terror groups are not linked to a specific government and, very commonly have been known to work as 'lone wolf' participants inspired by, but not necessarily in contact with, a central group, it is often difficult to collect information from an informant who has access to the group's plans and work. Furthermore, if an individual is working alone, plans for an attack are generally not shared with anyone else or written down. Without this, there is little chance of collection. This makes any

available human intelligence (HUMINT), the process in which intelligence is collected from human sources, and signals intelligence (SIGINT), in which intelligence is derived from communications, electronics, and foreign instrumentation signals, much more vital to the success of counterterrorism intelligence collection than it would be in standard intelligence collection, where sources tend to be vast and often contribute to too much unwanted information.[8] The intelligence cycle must also add steps in order to identify the specific intended target. This is much more difficult as targets are not always known players, but anyone that may have an intention of committing an act of terror in the future. This, then, fundamentally affects public policy as intelligence organizations must forge and utilize connections between themselves and known criminals in order to gain information vital to counterterrorism experts; often turning a blind eye to criminal activity in the hopes of stopping a much more potentially dangerous individual or group of individuals.[9] This is also risky for the informants passing information to intelligence agencies. As known criminals, their criminal records are not automatically erased by cooperation with intelligence agencies. In the United States, there are guidelines to protect FBI informants, which were set forth in 2006, requiring intelligence agents to consider the criminal history and motivation of the informant before registering them through the agency field manager.[10] The agents cannot promise the informants that they will not face charges for their past crimes, as this would put the intelligence community would be at odds with law enforcements; rather, they can only promise to testify to the assistance the informant gave to their operation.[11] However, if this can be achieved the use of informants is fruitful, and the information gathered could be the difference between success and failure of counterterrorism efforts.

Allocation of Resources

If the intelligence cycle and the use of its findings are as crucial to counterterrorism as they appear, the allocation of resources to counterterrorism intelligence must be of significant importance to the intelligence agencies. It is estimated that in the United Kingdom, 57 percent of MI5's intelligence

resources in 2004 were specifically allocated to be utilized for counterterrorism programs.[12] In comparison, the second largest amount of allocated resources within MI5's intelligence programs in 2001 and 2002 was for counterespionage at—a much less significant—14.4 percent.[13] These funds come from what is known as the Single Intelligence Account, which provides funding to MI5 as well as the Secret Intelligence Service and GCHQ from a predetermined amount of funds allocated by Ministers, based on the Spending Review.[14] Currently, MI5 reports on their public website that it has allocated 81 percent of its resources to counterterrorism, both international counterterrorism and that relating to Northern Ireland-related terrorism, and 19 percent to counterespionage; increasing and decreasing resources when necessary.[15] Since 2001, the allocation of resources to counterterrorism intelligence agencies have been raised and lowered numerous times; notably in 2006 when the resources allocated to the counterterrorism were at 86 percent. This is not unique to British intelligence organizations. Though the United States Government does not publicly list the percentage of its resources allocated to counterterrorism programs, in 2003 the United States National Strategy for Combating Terrorism stated that, "At every opportunity we will continue to enhance international counterterrorism cooperation through the further expansion and sharing of intelligence and law enforcement information."[16]

The USA PATRIOT Act

Allocation does not only refer to the division of funds; allocation is also the way in which intelligence is collected, disseminated, and presented. After the September 11, 2001, terror attacks, the American government sought to better identify threats, both international and domestic, that were essentially hiding in plain sight amongst the average citizen. Just one month after the attacks, the United States Congress passed the USA PATRIOT Act, a now highly controversial congressional bill, which allowed for the robust foreign and domestic arbitrary surveillance of suspected terror threats.[17] The USA PATRIOT Act has a specific goal that policymakers struggled to achieve prior to its

inception; the PATRIOT Act attempted to fill the gaps in counterterrorism efforts by means of intelligence, not only internationally, but domestically as well, in order to identify the 'silent' or 'underground' terror participants. This is regulated by policymakers, as Maureen Baginski stated, "Intelligence collection is only done in accordance with the intelligence priorities set by the President, and is guided at every step by procedures mandated by the Attorney General."[18] This highlights an allocation of focus on surveillance, which policymakers have deemed particularly valuable to the success of intelligence against terrorism. This is not to say that the allocation of focus has not at times been misused. In May 2004, Steve Kurtz, an associate art and biotechnology professor at the University of Buffalo, was arrested by the Department of Homeland Security and the Federal Bureau of Investigation's Joint Terrorism Task Force for his use of biological equipment and benign bacterial cultures in his work.[19] Though the New York State Commissioner of Public Health had determined that no harm could come from the materials used by Kurtz and all his equipment was lawful and commonly obtained for scientific education, Kurtz spent four years fighting charges under Section 175 of the US Biological Weapons Anti-Terrorism Act, which was broadened by the USA PATRIOT Act."[20] His defense contended that the seizure and charges were an abuse of the Act aimed at silencing the artist and scientist; a defense which Kurtz eventually won.[21]

Since 2001, surveillance has become a way of life, and a source of such public backlash, outrage, and media coverage that their have been Congressional bipartisan calls for revision to the US counterterrorism surveillance programs.[22] The National Security Agency of the United States' counterterrorism programs (established by the USA PATRIOT Act) falls under particular scrutiny. In 2013 Edward Snowden, a computer professional and independent government contractor from Booz Allen Hamilton consulting firm, believed the United States government's surveillance actions were infringing upon the Fourth Amendment rights of its citizens.[23] Feeling compelled to speak out, Snowden presented the public with the classified USA PATRIOT Act surveillance programs carried out

by the National Security Agency. These became known as the Edward Snowden leaks. The leaks provided proof for civil liberties groups, which criticized the programs for endangering the privacy and Constitutional rights of US citizens as the programs were found to practice mass collection of phone, internet, and data records of not only suspected criminals, but also, law-abiding Americans and foreign government officials.[24] On June 11, 2013, The American Civil Liberties Union filed a lawsuit directly related to the information produced by Edward Snowden, in which the organization challenged the legality of the National Security Agency's collection of private citizens' phone records.[25] Though the court dismissed the case in December 2013, the American Civil Liberties Union successfully appealed that the Executive use of the Patriot Act went far beyond that of the framework permitted within the bill, to which the court of appeals agreed.[26] The Edward Snowden leaks also brought to question the success of intelligence programs against terrorism. The average citizen began to ask, if intelligence agencies have access to such a vast amount of information, why has terrorism not been eliminated? What challenges does the intelligence community face with such access and do these challenges prove that the success of intelligence against terrorism cannot be effectively measured? Furthermore, do the benefits of counterterrorism intelligence outweigh the risks of threatening liberties of citizens, to be constituted as a success for intelligence?

Counterterrorism Intelligence Challenges

Although the use of surveillance in counterterrorism intelligence has significantly expanded the scope of intelligence collection and has allowed for the greater potential of identifying and tracking terror groups and individuals, counterterrorism intelligence continues to face challenges that affect its success. Since intelligence agencies largely operate covertly, they are intrinsically prone to operating within a gray area of ethical concern. With the revelations of Edward Snowden's 2013 leak of classified documents on mass data collection by the United States government and its allies, intelligence programs had to recognize the ethical tightrope on which they were continuously walking.

The American Civil Liberties Union, Electronic Frontier Foundation, and Electronic Privacy Information Center, alongside several other civil liberties groups launched reviews of the expanded surveillance programs of the National Security Agency while weighing the potentially harmful effects of 'Big Brother' on the law-abiding citizens of the nation.[27] Though leading technology and social media giants such as Facebook, Apple, Twitter, and Google contend that they will only share user information when a legal warrant is served, it has been found that these companies comply with requests for information on average approximately 80 percent of the time.[28] There have also been far-reaching surveillance attempts by the government, such as in February 2017, when the US Department of Justice issued warrants naming three Facebook users it said were "anti-administration activists who have spoken out at organized events, and who are generally very critical of this administration's policies."[29] Though Facebook reached out to the individuals targeted in the warrant to notify them of the government surveillance request which would include information such as the individuals' credit card numbers and passwords, as well as access to approximately 6,000 users in contact with the targeted individuals, this contact by Facebook was not made until September 2017, after a gag order placed by the Department of Justice was dropped.[30] All court filings by the Department of Justice and the communications from Facebook between February and September are still sealed.[31]

Oversight Demands

Constant use of terms such as 'Big Brother,' 'threats to civil liberties,' and 'watchers,' increased the fear of surveillance programs amongst the general population. Further still, Delflem writes, the ACLU has claimed that the intelligence programs have directly contributed to "violating the rights of immigrants, especially those of Muslim and Arab descent. Yet, upon investigation, these claims have often been found to be unsubstantiated."[32] These claims often lead to scrutiny as to the effectiveness of the intelligence programs in question. Operating within a clouded boundary of protection and liberty, the intelligence agencies can still not guarantee the safety of the nation; therefore, the programs are

seen as failures and in need of the implementation of safeguards to protect its citizen from a program built upon the very same intent. When society begins to fear and question counterterrorism's intentions it leads to a greater use of public oversight of programs that often require secrecy to be effective. Within the United States and the United Kingdom, oversight committee investigations of intelligence organizations, including the yearly US Department of Justice reviews of violations, have been carried out by various sectors of the US Department of Justice and UK Intelligence and Security Committee.[33] Though these questions of individual liberties and effectiveness of invasive intelligence programs are warranted and should be highlighted and discussed by policymakers and the private citizens alike, they do come at the cost of effectiveness within the intelligence community. Exposure, due to oversight committees, could be the difference between success and failure of intelligence against terrorism. The greater the revelations of oversight committees, the greater the transparency within the program will be. This leads to more of the intelligence becoming public knowledge to both the nation's citizens and its adversaries. This was one of the main fears of MI5 during the 'Troubles'—a 30-year span of terror in the United Kingdom organized and carried out by the Provisional Irish Republican Army who were known for their use of counterintelligence practices when planning attacks. As a result, even internal intelligence within MI5 was on a need-to-know basis, meaning that one intelligence agent stationed within Belfast, Northern Ireland would not know who the other agents were stationed elsewhere in the country or city, in order to keep their identities from the terror group.[34]

Foreign Concern and Cooperation

In addition to oversight committees exposing intelligence programs to all—including the criminals which they were designed to combat—their exposure risks creating fractures between a nation and its foreign liaisons. This occurred with the Edward Snowden leaks fiasco, when it was made public that the United States government was utilizing its intelligence programs in order to gain information on allied nations and foreign government officials. A revelation of this 'breach of trust'

could be detrimental to the success of current and future intelligence programs which are reliant upon the cooperation and coordination of allied states.[35] As Professors Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R.B.J. Walker state, "Trust between the services—which was limited, but nevertheless existed in the name of the struggle against terrorism—largely disappeared when it became clear that spying on politicians, industrial espionage, data mining of the personal information of large populations in order to profile the evolution of consumer choices, and even political opinions about future elections, have been used by NSA analysts."[36] The exposed US government surveillance programs left allied nations feeling hurt and untrusting of their formidable foreign associate; the German Justice Minister Sabine Leutheusser-Schnarrenberger calling the behavior "reminiscent of the actions of enemies during the Cold War."[37] Moreover, the idea that the trust between nations can give way to the unintended consent for other governments to gather sensitive information without the explicit knowledge of said nation, could put the national security of the nation and its citizens at risk. As a result, many nations raised concerns about the civil rights limitations of intelligence agencies, which may vary from country to country. These concerns would then be taken to the respective Minister of Foreign Affairs or Secretary of State of each nation in order to iron out concerns or set boundaries if a nation has infringed upon the rights of another. This can be addressed by the Ambassador to the foreign nation of concern or by the senior official themselves, dependent on the magnitude of the violation or threat.

Exhausted Resources

Although intelligence organizations collect massive amounts of data in order to stop known terrorist groups, foreign and domestic, it is impossible for an intelligence organization to be 100 percent certain that they have collected all sources necessary to identify all threats. This issue stems from the inherent composition of terrorism as a whole and the informal militias terror groups recruit. As previously stated, intelligence agencies have difficulty identifying targets that have not yet

committed crimes or suspicious activities that may indicate intent of causing terror, and this holds true even as intelligence gathering extends to mass data collection such as that implemented under the PATRIOT Act.[38] While intelligence agencies could exhaust all resources they possess, there is no way to accurately guarantee that these efforts have produced all information necessary in order to stop terrorism unreservedly. This is due to the many ways terrorist groups can form, either as a large energized assembly, a small cell, or a lone wolf terror suspect whose movements are difficult to track. Furthermore, when successfully tracking the communications and movements of a known terror group or individual, intelligence agencies cannot be certain that the methods used by the suspects will not change in order to guard against detection.

Until there is a way to read the inner thoughts of 'lone wolf' terror suspects which would then inform intelligence personnel of intent prior to attack, the resources available to intelligence do not have the capability to yield results. Theodore "Ted" Kaczynski, more commonly known as the Unabomber, is the perfect example of such instances in which a 'lone wolf' terrorist was not caught prior to a terror attack due to virtually no evidence of prior intent. Educated at Harvard University and with no prior criminal record, Kaczynski merely appeared to be an individual who struggled with personal interaction and pursued a life of solitude.[39] The reality was much darker. Harboring anti-technology and anti-government ideologies, Kaczynski carried out sixteen attacks over the course of eighteen years, in which bombs were delivered by mail or by hand and which resulted in three killed and twenty-three injured before his eventual capture in 1996.[40] Cases such as these lead to challenges of intelligence within society and brings forth the very questions this article seeks to answer. If intelligence agencies cannot guarantee the end of terrorism with the current capabilities they have, some of which may in fact threaten civil rights of their own citizen, is intelligence succeeding against terrorism? Furthermore, can the resources allocated to the utilization of intelligence against terrorism continue to be justified if it is proven not to be successful against terrorism? How, and on what levels,

can intelligence be effectively measured in order to thoroughly understand, to the greatest extend, the successes of its practices? Is this possible or can success simply not be effectively measured?

Measuring the Success of Intelligence in Regards to Terrorism

In order to determine whether or not the success of intelligence against terrorism can be effectively measured, one must first look at counterterrorism intelligence on several levels to include terrorism as a whole—terrorism in regard to intended known attacks, intended unknown attacks, 'lone wolf' terrorists, and the impact of the attacks that have taken place since the implementation of a robust counterterrorism intelligence program. Each focused section or level will indeed yield vastly different results and, thus, will be able to come together in order to decisively conclude if there is overwhelming evidence of measured success of intelligence against terrorism. First, however, one must start where many of the critics of counterterrorism intelligence have; looking at counterterrorism intelligence's success against terrorism as a whole.

The Continued Threat of Terrorism

In the post-9/11 era, terrorism has not been completely thwarted by the efforts of counterterrorism intelligence personnel and agencies around the world. Since September 11, 2001, there have been thirty-four significant terror-related attacks, ranging in size, impact, and weapon of choice, within the United States alone.[41] On November 28, 2016, an attack on several students at Ohio State University was carried out, believed to be in the name of Anwar al-Awlaki, an outspoken member of the al Qaeda terrorist group.[42] This came just days after the United States announced an expansion of their fight against the al Qaeda forces, to include the Shabab militant group located in Somalia.[43] In 2014, the Islamic State emerged as the newest threat of global terror and declared its caliphate. Since, there have been more than 140 terror attacks in twenty-nine nations, not including those recorded in Iraq and Syria, directly linked to the Islamic State and its global followers.[44] Today, although efforts have been taken to reclaim key cities such as Mosul in Iraq, that have been strongholds by the Islamic

State for the past two years, the terror group continues to control a significant portion of northern and western Iraq and central and eastern Syria.[45]

In regard to the blaring evidence that terrorist organizations do continue to operate, causing a continued need for the use of counterterrorism efforts, the success of counterterrorism intelligence cannot be effectively measured in that, success does not seem to be apparent. By this measure, the implementation of the USA PATRIOT Act, as well as joint transnational intelligence programs have not yielded successful results as intelligence agencies have not stopped the attacks from happening. As a whole, the success of intelligence against terrorism cannot be measured. Measurement is possible, however, if one focuses on an element of intelligence programs such as identifying potential terror attacks.

Foreseen Attacks

Intelligence gathering has been reassigned to counterterrorism departments of the federal government rather than law enforcement officials with the authority to arrest and detain known criminals. This moved the focus of intelligence agencies to collecting vital information about terror groups and activities that "allowed for long-term surveillance of terrorist suspects (as intelligence services are not concerned with the immediate requirement of criminal prosecutions), which has helped with the disruption of both operational and/or logistical cells."[46] While focusing their efforts on obtaining as much information as possible on the central terror group or cell—rather than simply the individual—and with the ultimate goal of preventing terrorism on a mass scale, their efforts have thwarted potential terror plots around the world. Jessica Zuckerman, Steven Bucci, and James Jay Carafano of the Heritage Foundation found that between 2001 to 2012, "At least fifty publicly known, Islamist-inspired terrorist plots against the homeland had been thwarted."[47] In the same report published by the Heritage Foundation, it is shown that out of the sixty terror plots within the United States from September 11, 2001 until the time of publication, only four had been successful.[48] In Great

Britain, Prime Minister David Cameron confirmed that seven terror plots had been obstructed in 2015 by British intelligence services.[49] Furthermore, across the globe, more than forty-five terror plots were derailed in 2016, including a terror plot targeting several landmarks in Paris set for December 1.[50]

The facts presented are significant. Although terror attacks occurred in more than twenty nations since 2001, the number of attacks that have been thwarted due to intelligence agencies' efforts is immense. Taking the statistics presented by the Heritage Foundation, between 2001 and 2012, terror groups had a 6.67 percent success rate when planning and implementing terror attacks on US soil.[51] In 2015, there was only one completed terror attack in Great Britain, making the success rate of terror groups within the country 12.5 percent.[52] By these numbers alone it would be difficult to disregard the success of intelligence against terrorism. Although there have been numerous attacks that continue to feed the global culture of fear, these numbers show that the impact of the terror groups could have been much more significant without the intelligence gathered and disseminated proactively.

Heightened Security Measures

The Central Intelligence Agency states, "The failure to determine an adversary's intention may simply be the result of missing information or, just as likely, it may be the result of missing hypotheses or mental models about an adversary's potential behavior."[53] As counterterrorism intelligence proves to have a significant impact on terror attacks, this often leads many to question whether or not intelligence is limited to just what is known and would not be successful in any capacity during an unforeseen attack. For this, one must look at the impact of successful terror attacks since 2001. Since then, nations around the globe have operated within a much more robust preventative security state in which security systems such as body scans, security cameras, and backgrounds checks have made it much more difficult for terror suspects to gain access to large capacity areas with weapons, undetected. Additionally, in the day-to-day implementation of intelligence against terrorism, nations such as the United States, the United Kingdom, Australia, Canada, and France have developed terror level

assessment systems which can indicate the projected terror threat of the nation at any given time.[54] These assessment systems, Chalk states, "Have played a highly instrumental role in national counterterrorist planning" as they are utilized by both the public and private sectors to "design viable and sustainable counterstrategies."[55]

These counterstrategy systems, as reactive as they may have been during their initial implementation, significantly aid in deterring terror threats on a daily basis. Many of these systems, whether it be heightened security forces, metal detector machines, or security cameras, stop plots in their tracks as would-be terrorists acting without sophisticated means, or without a number of accomplices, are deterred by the potential of being caught. One of the greatest criticisms of security programs, such as the Transportation Security Administration in the United States, is that the programs are not catching or identifying as many suspected terrorists as society assumed would be caught if the programs were successful; instead, they are adding an additional discomfort, such as increased wait times in lines and security measures that require the removal of clothing containing metal, to law abiding citizens without yielding significant results.[56] CNN Aviation Analyst and thirty-one-year veteran Boeing 777 captain Les Abend stated that even years after the implementation of the Transportation Security Administration (TSA) in 2001, airline crews are skeptical of the safety of the passengers aboard their flights; particularly after TSA failed an undercover test in 2015, planted to gauge their ability to detect explosives and weapons.[57] However, if the intensified security is deterring terror groups from attempting attacks, there would be little to catch, as they would not come into contact with the security officials. In order to measure the success of the programs, one must look at the gaps that were filled in the security programs that were not addressed before. Heightened airport security, metals detectors at amusement parks, and a greater security presence at public events such as marathons and parades, for example, not only create a much more robust and intimidating counterterrorism strategy, which has lead to less successful terror attacks in regard to amount of

affected victims, but also addresses the weaknesses in the previous security systems.

'Lone Wolf' Actors

Finally, in order to effectively measure the success of intelligence against terrorism, one must analyze the success of intelligence against 'lone wolf' terror attacks. 'Lone wolf' attacks are defined as 'inspired attacks' that are carried out by a single person or, perhaps, a small group of people in the name of a terror group or ideology, without specific orders from said group.[58] As they are characteristically not planned or executed by a group of individuals with the potential of leaving a paper trail detailing their intentions, 'lone wolf' actors are notoriously difficult to identify prior to the terror attacks they carry out.[59] Leenaars and Reed state that the only way to successfully identify these introverted and notoriously silent attackers is through a comparative analysis of "intention; socio-demographic information; psychological background and history; motivation behind the attack; target of the attack; *modus operandi*; objective of the attack; and aftermath."[60]

In order to identify and analyze many of these factors that then help intelligence and law enforcement impede lone wolf attacks, the information is generally gathered only when an attack has taken place. However, Striegher states that "they are adept at identifying indicative behaviours or actions that lead up to a terrorist event—post event."[61] This has been witnessed, Striegher continues, in Madrid when "investigators were able to piece together all of the evidence that led up to the 2004 Madrid bombing and what precursory actions Jamal Ahmidan undertook (post-blast), and were able to deconstruct Breivik's life once he had killed seventy-seven of his fellow countrymen."[62] This provides a greater understanding of the actions of 'lone wolf' terrorists and how best to identify them even as they work to remain anonymous.

This has been proven to work in the United States as well as Europe by means of information sharing between local and federal law enforcement and intelligence agencies. Following the November 2015 terror attacks in Paris, the French and Belgium governments followed leads obtained by footage

found of the terror suspects at the scenes of the attacks; conducted several anti-terror raids on homes in connection to the suspects and, by the December 24, 2015, had detained their ninth suspect in connection to the attacks.[63] This subsequently led to a number of suspects arrested in Brussels under suspicion of plotting a New Years' terror attack. Intelligence is recognized as the contributing factor of these arrests and, although intelligence gathering of 'lone wolf' terror suspects is one of the most challenging hurdles the intelligence community faces, has been successful when implemented. The success is not as largely recorded as that of the number of foiled known terror plots, as 'lone wolf' plots are much harder to detect than a plot conducted by a large cell or ordered by a central commanding force; however, success is in fact evident.

Measurement of Intelligence Success against Terrorism

After breaking down the success of intelligence against terrorism as a whole, to the many different levels of terrorism, one could conclude that the success of intelligence against terrorism cannot be effectively measured without regard to the various components of which it entails. However, when looking at the success counterterrorism intelligence has had on thwarting known terror attacks in the United States as well as Europe, the successful implementation of counterterrorism strategies such as a more robust security presence in highly populated facilities and target areas; and the growing success of understanding the identifiable characteristics of 'lone wolf' attackers prior to terror acts, the success of intelligence against terrorism can not only be effectively measured, but is also abundantly clear.

Moving forward, in order to fully understand the utility of intelligence within counterterrorism programs, one must not simply judge the success of intelligence solely on the continued appearance of terror groups across the globe. It is unreasonable to assume that intelligence can fully solve the threat of terrorism in just a few short years. Rather, the understanding of the capabilities of intelligence, as well as its limitations, and the ways in which intelligence has strengthened the nations fighting against

terrorism while weakening their adversaries, should be taken into account in order to determine the true success of intelligence.

Conclusion

In the post-9/11 era, counterterrorism intelligence has been the focus of criticism by individuals and policymakers alike as terrorism continues to threaten every corner of the globe. Many previous studies of counterterrorism intelligence tend to focus greatly on the failures of which are molded by the limited understanding of intelligence programs by the general public. With regard to the capabilities of, as well as, ethical and physical limitation to counterterrorism efforts, this article has sought to present a comprehensive analysis as to whether or not success can be measured with the current intelligence model. From the success of the United States and European intelligence agencies in thwarting known terror attacks with as much as percent success since 2001, to the strengthening of national security systems in order to make even an attempt of terror impossible, and the continued work of the intelligence community to best identify and stop 'lone wolf' attacks; intelligence against terrorism has proven its immense success. Moving forward, a greater understanding of intelligence practices and limitations by both the public and the policymakers which oversee the intelligence community, can help to propel the counterterrorism efforts of agencies around the world by means of greater allocation of resources to intelligence programs and a much more significant reliance on intelligence reports when policy and engagement decisions are made.

ENDNOTES

1. Lucy Rodgers, Salim Qurashi, and Steven Connor, “7 July London Bombings: What Happened that Day?” *BBC News*, July 3, 2015, http://www.bbc.com/news/uk-33253598.
2. 28 C.F.R. Section 0.85.
3. Daniel Byman, “The Intelligence War on Terrorism,” *Intelligence and National Security* 29(6) (2013): 837-838.
4. Ibid., 838.
5. Michael German, “4 Counterterrorism Strategies the US Must Abandon,” *US News*, October 26, 2016.; Rosa Brooks, “US Counterterrorism Strategy is the Definition of Insanity,” *Foreign Policy*, June 24, 2015.; Editorial Board, “Mass Surveillance Isn’t the Answer to Fighting Terrorism,” *New York Times*, November 17, 2015.
6. US Joint Chiefs of Staff, “Counterterrorism,” *Joint Publication* 3-26 (2014): I-5.
7. Clive Walker and Aniceto Masferrer Domingo, *Counter-terrorism, Human Rights and the Rule of Law: Crossing Legal Boundaries in Defence of the State* (Cheltenham, Glos: Edward Elgar), 294.
8. Byman, “The Intelligence War on Terrorism,” 840-841.
9. Ibid., 855-856.
10. United States, 2006, The Attorney General’s Guidelines Regarding the Use of FBI Confidential Human Resources, (Washington, D.C.: U.S. Dept. of Justice), https://s3.amazonaws.com/s3.documentcloud.org/documents/1314458/ag-guidelines-use-of-fbi-chs.pdf.
11. Ibid.
12. Peter Chalk, William Rosenau, and Martin Wachs, *Confronting "the Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies* (Santa Monica, CA: RAND, 2004), 10.
13. Ibid.
14. “*People and Organisation,*” Accessed on November 22, 2016, https://www.mi5.gov.uk/people-and-organisation.
15. Ibid.
16. “National Strategy for Combating Terrorism,” Accessed on November 30, 2016, https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.
17. United States, 2001, *The USA PATRIOT Act: Preserving life and liberty: Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism,* (Washington, D.C.: U.S. Dept. of Justice), https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf.
18. “*Testimony: Subcommittee on Crime, Terrorism, and Homeland Security House Committee on the Judiciary,*” Accessed on 22 November 2016, https://archives.fbi.gov/archives/news/testimony/importance-of-usa-patriot-act-to-fbi-information-sharing.
19. "What is This Case About?" Critical Art Ensemble Defense Fund, accessed March 1, 2018, http://critical-art.net/siteapps/WordPress-49402/htdocs/defense/overview.html#case.
20. Ibid.
21. Ibid.
22. New York Times, "Patriot Act Faces Revisions backed by Both Parties," April 30, 2015.

23. BBC News, "Edward Snowden: Leaks that exposed US spy program," January 17, 2014.
24. Mathieu Deflem and Shannon McDonough, "The Fear of Counterterrorism: Surveillance and Civil Liberties since 9/11," *Society* 52(1) (2015): 70.
25. ACLU, "ACLU v. Clapper – Challenge to NSA Mass Call-Tracking Program," last modified October 29, 2015, https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program?redirect=national-security/aclu-v-clapper-challenge-nsa-mass-phone-call-tracking.
26. Ibid. Deflem and McDonough, 71.
27. *Quartz*, "Here's how often Apple, Google, and others handed over data when the US government asked for it," February 19, 2016.
28. *CNN*, "DOJ Demands Facebook Information from 'Anti-Administration Activists,'" September 30, 2017.
29. Michael Kirk-Smith, and James Dingley, "Countering Terrorism in Northern Ireland: The Role of Intelligence," *Small Wars and Insurgencies* 20(3-4), 565.
30. *CNN*, "DOJ Demands Facebook Information from 'Anti-Administration Activists,'" September 30, 2017.
31. Ibid. Mathieu Deflem and Shannon McDonough, 73.
32. Peter Gill, "Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror,'" *Intelligence and National Security* 22(1) (2007): 16-27.
33. Zygmunt Bauman, et al, "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8(2) (2014): 126-127.
34. Ibid., 127.
35. *The Guardian*, "New NSA Leaks Show How US is Bugging its European Allies," June 30, 2013.
36. Anne Joseph O'Connell, "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World." *California Law Review* 94(6) (2006): 1663-1665.
37. "Unabomber," accessed on March 4, 2018, https://www.fbi.gov/history/famous-cases/unabomber.
38. Ibid.
39. Bobby Ilich, "The United States After 9/11: How Many Major Terrorist Attacks Have There Been In America Since 2001?" *International Business Times,* September 9, 2016.
40. *Fox News,* "Stop interfering with other countries': OSU attacker slammed US over treatment of Muslims on Facebook," November 29, 2016.
41. Charlie Savage, "Obama Expands War with al Qaeda to include Shabab in Somalia," *The New York Times,* November 27, 2016.
42. Tim Lister, et al., "ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043," *CNN*. September 1, 2016.
43. *BBC News,* "Islamic State and the Crisis in Iraq and Syria in Maps," November 2, 2016.
44. Peter Chalk, William Rosenau, and Martin Wachs, *Confronting "the Enemy Within,"* 43.
45. Jessica Zuckerman, Steven Bucci, and James Jay Carafano, (2013) "*60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism,*" http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism#_ftn2.
46. Ibid.
47. Michael Wilkinson, "Revealed: Britain Has Foiled Seven Terror Attacks in One Year," *The Telegraph,* November 16, 2015.
48. *France 24,* "Thwarted terror plot targeted Disneyland Paris, Champs-Elysées, police say," November 25, 2016.
49. Jessica Zuckerman, Steven Bucci, and James Jay Carafano, (2013) "*60 Terrorist Plots Since*

9/11: Continued Lessons in Domestic Counterterrorism," http://www.heritage.org/research/reports/2013/07/60-terrorist-plots-since-911-continued-lessons-in-domestic-counterterrorism#_ftn2.

50. *BBC News,* "Leytonstone Tube Station Stabbing a 'Terrorist Incident,'" December 6, 2015.
51. Between 2001 and 2012, there were 4 successful terror attacks out of the 60 known to have been plotted against the United States of America. *"Analytic Culture in the U.S. Intelligence Community: Chapter 1-Definitions,"* Accessed on October 13 2016, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm.
52. Chalk, Peter, William Rosenau, and Martin Wachs, Confronting "the Enemy Within", 46.
53. Ibid.
54. *New York Times*, "Screening Still a Pain at Airports, Fliers Say," November 21, 2011.
55. *CNN*, "Pilot: Is TSA Security a Complete Failure?" June 4, 2015.
56. Jan Leenaars and Alastair Reed, "Understanding Lone Wolves: Towards a Theoretical Framework for Comparative Analysis," The International Centre for Counter-Terrorism–The Hague (2016), 4.
57. Ibid., 3.
58. Ibid., 5.
59. J.L. Striegher, "Early Detection of the Lone Wolf: Advancement of Counter-Terrorism Investigations with an Absence or Abundance of Information and Intelligence," *Journal of Policing, Intelligence, and Counter Terrorism* 8(1) (2013): 43.
60. Ibid.
61. *BBC News,* "Paris Attacks: Belgium Police Arrest Ninth Suspect," December 24, 2015.