This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2020-6100C

Malicious Threat Anticipation using an Adaptive Complex Systems Approach

Sue A. Caskey, Adam D. Williams, Thushara Gunda

Sandia National Laboratories[1], Albuquerque, NM, USA, [scaske; adwilli; tdunda]@sandia.gov

Abstract:

Anticipating the emerging—and evolving—behaviors of threat actors, those with malicious intent toward US critical infrastructure, is a complex problem. Current threat analysis frameworks fail to adequately tackle this problem, and as such we have been taken by surprise by threat actors with evolving motives, capabilities, and tactics resulting in their ability to exploit gaps within our security posture. Consider, for example, the common understanding of "threat" in the US on September 10, 2001 versus that on September 12, 2001. Similarly, recent problems within the European Union can partially be described as resulting from the emerging nexus of terrorists and criminal organizations.

In response, this paper will look at the feasibility of framing threat actors as a complex and adaptive system of systems in order to leverage a new suite of analytical tools and insights for better understanding their observed evolution. To investigate the feasibility of building such a framework, this paper will introduce core concepts for a complex and adaptive system of systems thinking approach and apply them to the threat actor space. More precisely, such an approach focuses on identifying and describing interactions between different threat actors and their motives, capabilities, and technical means. Such a complex system framing can better support anticipatory thinking regarding emerging and evolutionary behaviors in threat actors. The resulting insights and implications can have beneficial impacts on designing security solutions for the US nuclear infrastructure.

INTRODUCTION

The nexus between terrorist organizations, criminal, and radicalized individuals (TOCRI) is a growing concern. There have been several studies and articles that highlight how diverse threat groups (TGs) will work together to achieve a common objective, often overlooking political and social differences. Social relationships exist between terrorist groups, between terrorist groups and criminal groups, and between terrorist or criminal groups and radicalized individuals. A 2005 study used social network analysis to consider the social relationships between terrorist groups within South Asia (Basu, 2005). This paper presented a look at how even groups with ethnonationalist differences will work jointly. Recent reports from organizations working to reduce organized crime have identified that there is a willingness for criminal organizations to work with terrorists and have, in some cases, merged into a joint organization (Global Initiative Against Transnational Organized Crime, 2020). Terrorist organizations have a history of working within the world of organized crime, blurring the definition between criminal and terrorist (Hutchinson, 2007).

Observation suggests that long-term TOCRI objectives tend to fall in one of four categories: 1. changing the politics of an existing state, 2. creating their own state (e.g., a caliphate), 3. to cause apocalyptical like conditions, or 4. for financial gain. Independent TGs operate as a complex system

[1] **SAND2020- xxxx.** Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525

with unique motives, capabilities, and technical means. Multiple TGs working toward a common larger objective mirror the concepts used to define a system of systems (SoS). This paper posits the TOCRI nexus as a complex and adaptive SoS, which enables use of structured and analytical techniques to recognize adaptive and emerging behaviors – specifically, looking at the potential of this nexus to acquire and produce a weapon of mass destruction (WMD).

TOCRI AS A SYSTEM OF SYSTEMS

Rather than a SoS (e.g. national air traffic control), the TOCRI nexus could be argued as a complex system (e.g. a commercial airline) or a series of simply independent systems (e.g. a single plane). Thus, to support the argument of the TOCRI nexus representing a SoS, alignment between TOCRI and six principles of SoS where evaluated (Keating, 2011):

1. Operational independence of each TG;
2. Managerial independence of each TG;
3. Evolutional development of each TG;
4. Emergent behavior within each TG;
5. Geographical distributions between the TGs; and,
6. Interoperability of the TGs.

All three types of TGs (i.e., terrorist organizations, criminals, and radicalized individuals; TOCRI) have their own identity and objectives, indicating operational independence. A different group may work toward a common objective within the SoS, but what binds them into this SoS may not be the same. That is, a criminal organization may support this system for financial motives while a terrorist organization may support the system for political motives. Each of these TGs also have managerial independence in their execution of the objectives. Specifically, they have their own leadership, independent funding, and mechanisms for funding. Consider groups like Al Qaeda in comparison to the D-Company – there is a clear distinction in operational structure and management. Even within two groups with similar motives (e.g., Al Qaeda and the Islamic State of Iraq and Syria (ISIS)), there is a notable difference in the operations between the threat groups.

The evolutional development of each of these TGs is also different and dynamic. Many terrorist organizations that have direct motives for a WMD (such as Al Qaeda or ISIS) were born out of a civil war. Al Qaeda emerged during the Soviet-Afghan conflict as a sect of Muslims were working to oust the communist Afghan government (History , 2018). ISIS, created out of an Al Qaeda splinter group operating in Iraq after 2003, was refueled and reemerged in response to the civil war between the Sunnis and Shiites and the Syrian civil war (Hassan, 2018). In contrast, transnational criminal organizations spawn from local organized crime, which in turn grew to take advantage of the growing global markets and expand smuggling/trafficking routes across the globe (National Institute of Justice, 2011). Motivations of individuals who have self-radicalized are varied and include financial reasons, internal frustrations with 'the system,' or sympathizing with terrorist causes (Olson, 2019).

The emergent behavior of TGs is driven by their independent operations as well as the context. These emergent behaviors are influenced by opportunities as well as constraints, such as interdiction by authorities. As such, the TGs may move geographically or change in organizational structure very rapidly (e.g. the splintering of Al Qaeda creating ISIS). The geographical distribution of these groups varies, with some operating within the same regions (e.g., the EU or Asia) while others operate in vastly different continents (groups operating in Central America as compared to the Middle East).

In both the EU and in Asia, there have been returning ISIS foreign fighters radicalizing criminals within the same prisons. Groups in South Asia (both criminal and terrorist organizations have also been sharing of trafficking couriers and routes. Both the areas where these various TGs coexist and areas where there is a geographic distance create new opportunities for joint operations. This interoperability is based on social affinities, including the underpinning philosophical beliefs of the groups and ethnicity as well as often, family ties and spoken language. That is, a group that is Sunnis would likely not work with a group that is Shiites but might work well with criminals. Money and/or a joint alignment of each other's objectives are also drivers for interoperability. Specifically, two groups that are both working to create a caliphate will easily interoperate; similarly, a group leveraging funding to link to a financially motivated group may also work together.

While the various individual TGs are clearly independent systems, there have also been examples where they have worked jointly to become more effective. This has been witnessed in recent attacks in Africa (Paquette, 2020) as well as during the Syrian conflict. Criminals have been known to supply terrorists with goods, people (victims of kidnapping), and funding support (e.g. trafficking of arms and drugs for terrorists). Terrorists also often support criminal actions as they can impact the destabilization of countries (Angelina, 2011). These dynamics highlight that while each TG may be independent, they can certainly come together for common goals, indicative of a SoS.

STRUCTURED FRAMEWORK FOR TOCRI NEXUS

A structured framing approach can support better understanding of the SoS. To build a framework to help define emerging and adaptive behaviors that would reflect a TOCRI nexus formation or indication of the existence of a nexus, nine problem framing elements have been used (Adams, 2011). These nine elements support defining the SoS context, problem domain, stakeholders, and complexity.

The broad context of this system links back to the three types of TGs and their motivations. These motivations define their values and patterns of behavior and include their willingness to support a larger objective such working together. The areas in which they operate offer various opportunities (and constraints) as well as unique capabilities of each group that help inform the larger context of this problem.

The exemplar system for this study is a nexus of TGs working together to acquire the needed materials and skills to develop a WMD. The parts of the system include the TGs with the overall aim to have and likely use the WMD, TGs who may be able to acquire or support the trafficking of materials, and possible self-radicalized individuals with access or skills. Each of the TGs may have unique underlying motivations. The primary constraints to this system are time, money, and counter-threat actions (to include the security posture of locations of needed materials). Free movement and communication may also be limited due to interdiction concerns. The environment of this system includes areas of operation (areas where these groups can freely move and operate) and areas where they must remain clandestine to avoid interdiction. Within the areas of operation, the situation can change rapidly; that is, the area can become hostile for the system or be susceptible to additional political unrest creating new opportunities. Resources vary from group to group but include skills, equipment, and funding. These are dynamic and often not directly applicable to the overall objective of the development of a WMD. For example, skills to develop a suicide bomb are only minimally applicable to the development of an improvised nuclear device. The overall TOCRI nexus has complex governance; in many cases, groups may merge and full under a single leader while, in other cases, they maintain their operational independence. Where this nexus has been witnessed to date, and groups have maintained operational independence, they worked as separate units. A clear example is the D-Company smuggling explosive precursor chemicals to the Taliban (Kennedy, 2019).

TGs are soft systems (human-based) and, as such, are more dynamic and evolving than a simple technical system. Each independent TG has changing short-term objectives and often dynamic leadership. The environment causes turbulence that can completely disrupt the system. The nexus between systems is often ad hoc in nature and can change rapidly. The system under study is morphing and adapting and devolving daily. As such, a study of this system requires innovative approaches.

The system under study is based on an uncertain number of elements; that is, there may be two groups working to create this nexus, or there could be several dozen. Currently, the US Department of State lists more than 60 foreign terrorist organizations (US Department of State, 2020). Within that list, there are more than 20 ISIS-affiliated groups worldwide, each of which is operating under separate leadership and structure (Terrorism Research and Analysis Consortium, 2020), and Interpol lists dozens of transnational criminal organizations within every region of the world. The interactions and relationship between these groups is often ad hoc and dynamic. The number of different states within the system under study (the TG nexus) is also dynamic. Within this nexus, the independent systems are often driven by their personal objectives and may derail the overall objective based on opportunities. As an example, a group with access to materials that are of use for a WMD (and was working to acquire these to support the larger objective of the nexus) may change their mind and pursue a different target based on the potential profit of the new target. Thus, the nexus of TOCRI in characteristically complex.

The exemplar SoS problem can be defined by a representation focusing on the three types of TGs defined previously rather than by specific TG and the drivers and motivations they have to work together and those to work separately. Each of the TGs is characterized by motive, technical means, and capabilities. As noted above, each group has a motive that drives their independent behavior is regarding WMD acquisition, ranging from creation of new states (terrorist organizations) to financial gains (criminal organizations) or a combination of things (self-radicalized individuals). The technical means of each group are those resources that can be used to support the overall objective. If a terrorist organization had access to all needed resources independently, they would not have a need for a SoS to achieve the overall system goal. Since, to date, terrorist use of WMD materials has been limited to chemicals and biologicals on a small scale, the supposition of this study is that a SoS is needed to achieve WMD acquisition/production. Typically, criminal organizations have technical means and capabilities for the acquisition of almost any materials and trafficking this material to a 'safe' location. Self-radicalized individuals may have unique access to materials or skills to support the production of a WMD. A self-radicalized individual may also be someone who has been coerced or recruited to support the objective.

The following representation (Figure 1) visualizes the capabilities of the three TGs for the three domains (motive, technical means, and capabilities). While there are limitations in a TG’s individual ability, together they have all the resources to produce a WMD (Figure 1).

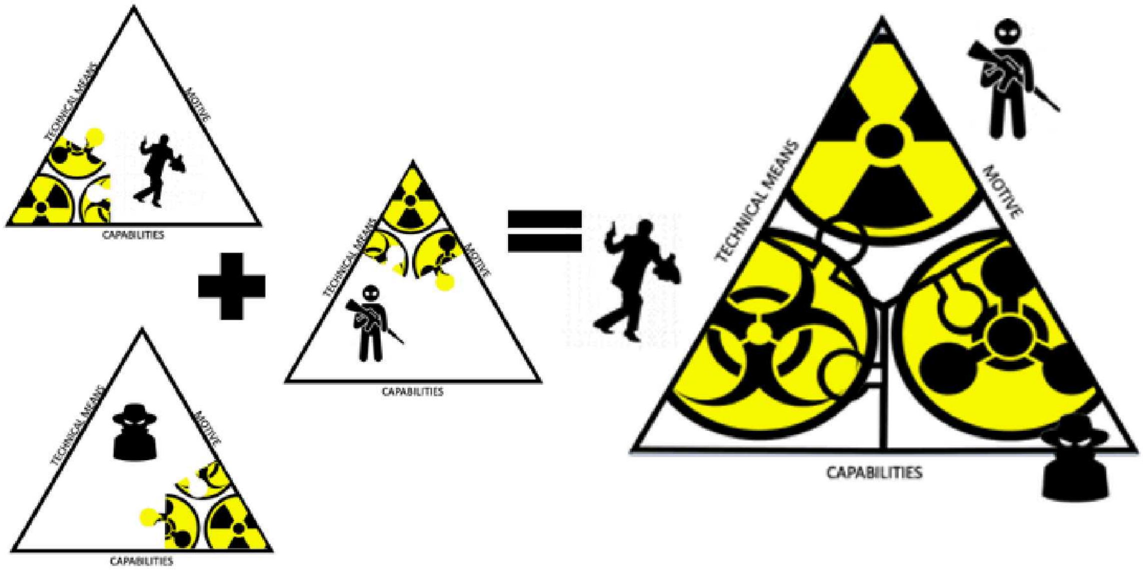


Figure 1 System of Systems Representation of the Three Domain Interactions towards a Common Goal. Criminals have some level of capabilities and technical means (upper left), insiders have a different set of capabilities and motives (lower left), while terrorist organizations have yet a different set of technical means and motive (center). These combine to (right) create the TOCIR nexus highlighting the more complete abilities this union has then each group has independently.

FACTORS INFLUENCING TOCRI NEXUS FORMATIONS

For this problem, the context of the SoS is focused on drivers that bring about the nexus, or potentially keep it apart. These include such factors as the ethnicity of the groups, money, proximity, country and regional influencing factors, fear of interdiction, counter-terrorist actions, and contrasting motivations (Table1). Nuances on these factors on the SoS is explored in greater detail in the following table.

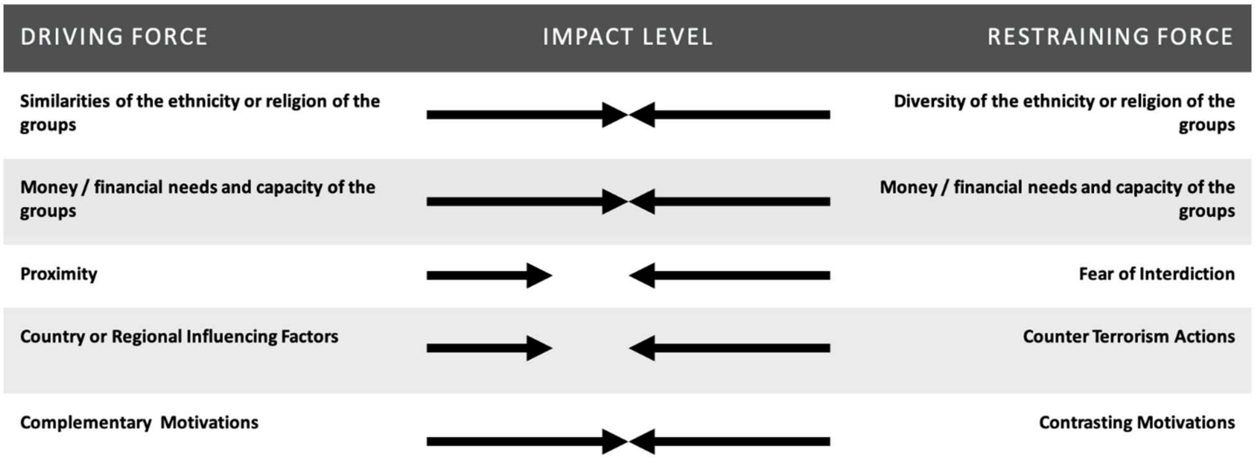
Table 1 Contextual Factors Influencing TOCRI Nexus Formations

Contextual Factor	**Description of the factor**	**Responses to the factor**	**Processes to monitor the factor**
Diversity or similarities of the ethnicity or religion of the groups	Diverse ethnicity or religion can reduce the willingness for groups to support other groups (e.g., Sunni and Shiite). In contrast, groups with similar beliefs or backgrounds will often support other groups (e.g., the Al Qaeda in India moving into Myanmar provide protection against the Muslim cleansing).	Many groups are working to become more ethnically tolerant of allowing for partnerships to develop between or across groups. We have seen this with the changes in the African terrorist organizations who are working to create a broader ISIS presence despite local tribal issues.	Beyond witnessing actions in opposition to other groups in or in support of other groups, witnessing these changes externally will be difficult. However, leveraging these actions can help to anticipate other changes in how ethnic and religious diversity impact the TG nexus.
Money / financial needs and capacity of the groups	Many threat groups, specifically those linked to criminal organizations, are financially motivated (e.g., drug cartels in Central America (Member, 2018)). This motivation can often override the fear of interdiction or other potential restraining forces of the joining of forces.	Not all threat groups are well funded and able to 'buy' the support of other groups. Many are working to acquire their own funding sources, such as drug trafficking or other illicit actions. Much like any organization, the resources are not infinite and can be a limiting factor in using money to bridge capabilities and technical means between groups.	Tracking funding streams and movement of money and illicit goods can help to determine where financial links between various threat groups may exist.
Proximity	There have been witnessed accounts of recruitment between individual criminals and terrorist organizations in prisons in both Asia and the EU. Most of these terrorists are returning foreign fighters. As such, there is likely an avenue for building a nexus between TGs when in close proximity. In contrast, the Taliban pushed out ISIS from Afghanistan successfully for many months, that is until there was a split within the Taliban and ISIS was able to use this to gain a foothold.	Proximity seems to be a positive driver for the joining of forces in the long term despite a short term potential to create a greater rift.	As with most of these contextual factors, there is a great deal of system darkness, however, monitoring TG actions and statements can provide insight regarding proximity.
Country or Regional Influencing Factors	These factors define stressors within a country or region that may make individuals more susceptible to radicalization or groups willing to work with others. Stressors include economic downturn, corruption, crime rates, terrorist actions, and marginalized pockets of the population.	These stressors, based on discussions with counterintelligence experts and terrorism experts (Terrorism), 2010), often create a hot spot for radicalization or terrorist actions within a country, region, or even an area within a city.	Many of these can be monitored externally by looking at the country or regional issues. There are several global indices (such as the corruption perception index, fragile state index, or the political terrorist scale) that can help provide some secondary information on these influencing factors.
Fear of Interdiction	The security of materials and equipment (direct interdiction) and the concern of a more forceful response against a group are strong influences on whether an entity is willing to use or support the use of a WMD.	Fear of interdiction may reduce the willingness to support other groups (specifically in helping to acquire WMD materials). This may also reduce the willingness to align with a group based on the potential ramifications of allegiance.	This is an interesting factor in that it is very personal; specifically, a group may choose to support actions while an individual within the group may not. As such, this will be a difficult factor to monitor. This is also a driver for why subject matter experts have believed we have not witnessed this nexus previously; however, this fear may be reducing (Hutchinson, 2007).

Contextual Factor	**Description of the factor**	**Responses to the factor**	**Processes to monitor the factor**
Counter-Terrorism Actions	Counter-terrorism actions include specific acts to disrupt or destabilize the group's ability to operate.	Counter-terrorism actions may force locational changes, leadership changes, or disrupt the team's ability to operate within each group as well as between the groups.	Counter-terrorism actions are difficult to monitor -by-design- until after the action has taken place and the impact on the threat group or groups witnessed.
Contrasting Motivations	Groups, who may look from the outside to have similar goals and mechanisms, may, in fact, have contrasting motives and tactics. For example, drug cartels may be less willing to support terrorist actions toward the US in part due to the impact of any US destabilization on their ability to sell illicit drugs in the US.	The impact of contrasting motives can create an unwillingness to work together at any point but could actually cause groups who were working jointly to separate (e.g., the Revolutionary Armed Forces of Colombia (FARC) and the National Liberation Army Colombia (ELN)).	Understanding some of the more hidden contrasting motivations will be difficult to monitor. There have been cases where groups that externally appear to align actually fight each other, and groups that appear to have opposing ideals work jointly. As with most of the other contextual factors, monitoring will need to be tailored to the actions taken.

Each of these contextual factors has an impact on the system that is driving or restraining. A force field diagram is based on the concept of forces driving behavior, these forces can be drivers - forces that are pushing toward the behavior - or restrainers – forces that are blocking behavior (Adams, 2011). In considering a TOCRI nexus, there are driving forces that are pushing a toward this nexus and restraining forces that are helping to prevent this nexus. The following figure (Figure 2) provides a summary of these factors' type of impact and level.

Figure 2 Force Field Diagram, the length of the arrows reflects the level of impact driving the nexus (left to right) or restraining the nexus from being created (right to left). Where the arrows are equal the driving and restraining forces are almost equal. Where gaps between the forces exist the force, the restraining force is not pushing directly on the driving force, this would allow the driving force to become stronger.



DRIVING FORCE	IMPACT LEVEL	RESTRAINING FORCE
Similarities of the ethnicity or religion of the groups	→←	Diversity of the ethnicity or religion of the groups
Money / financial needs and capacity of the groups	→←	Money / financial needs and capacity of the groups
Proximity	→ ←	Fear of Interdiction
Country or Regional Influencing Factors	→ ←	Counter Terrorism Actions
Complementary Motivations	→←	Contrasting Motivations

CONCLUSION

Small scale demonstrations of WMD acquisitions/productions have occurred in Japan (Danzig, 2012), the US (Thuras, 2014), Syria (Strack, 2017), as well as a handful of others. A global review of terrorist attacks (1970 to 2018) indicates that just over 300 (0.2%, out of the nearly 200,000 attacks reported in the Global Terrorism Database) utilized WMD material with only hundreds of impacted individuals[2] (National Consortium for the Study of Terrorism and Responses to Terrorism, 2020). Each of these attacks was conducted by a single threat actor or individual group rather than through a combined effort. The objective of this analysis is to develop a framework that facilitates understanding of the forces influencing the formation of such a TOCRI nexus.

This paper is only an initial look at the development of such a framework. The research team is optimistic that continued work in this domain will help to solidify a methodology that can be used by those working in counting WMD threats. The driving and restraining forces (and associated contextual factors) of TOCRI nexus creation are the building blocks to a framework that will support looking at the interactions between different threat actors and their motives, capabilities, and technical means. As a result, this way of thinking can help support better anticipatory thinking regarding emerging behaviors.

[2] WMD material was defined as Chemical, Biological, or Radiological listed under the Weapons Type within the database.

WORK CITED

Adams, K. M. (2011). Perspective 1 of the SoSE methodology: framing the system under study. *Int. J. System of Systems Engineering, Vol. 2, Nos. 2/3*, 163-192.

Angelina, S. (2011). *The Connection Between Terrorism and Organized Crime: Narcoterrorism and the Other Hybrids.* Macedonia: Faculty of Security, Skopje.

Basu, A. (2005). *Social network analysis of terrorist organizations in India.* Retrieved from Research Gate: https://www.researchgate.net/publication/228962297_Social_network_analysis_of_terrorist_organizations_in_India

Danzig, R. S. (2012). *Aum ShinrikyoInsights Into How Terrorists Develop Biological and Chemical Weapons.* Center fro a New American Security .

Global Initiative Against Transnational Organized Crime. (2020). *Crime Terror Nexus*. Retrieved from Global Initiative Against Transnational Organized Crime: https://globalinitiative.net/initiatives/nexus-oc-ct/

Hassan, H. (2018). *The True Origins of ISIS*. Retrieved from The Atlantic: https://www.theatlantic.com/ideas/archive/2018/11/isis-origins-anbari-zarqawi/577030/

History . (2018). *Al Qaeda*. Retrieved from 21st Century Topics: https://www.history.com/topics/21st-century/al-qaeda

Hutchinson, S. O. (2007). A Crime-Terror Nexus? Thinking on Some of the Links between Terrorism and Criminality. *Studies in Conflict and Terrorism*, 1095-1107.

Keating, C. K. (2011). Systems of systems engineering: prospects and challenges for the emerging field . *Int. J. System of Systems Engineering Vol. 2 Nos. 2/3*, 234-256.

Kennedy, L. S. (2019). How India's Most Notorious Crime Lord Became Pakistan's Honoured Guest. *InsideOVER*.

National Consortium for the Study of Terrorism and Responses to Terrorism. (2020, 01 15). *Global Terrorism Database*. Retrieved from START: https://www.start.umd.edu/data-tools/global-terrorism-database-gtd

National Institute of Justice. (2011). *The Evolustion of Transnational Organized Crime*. Retrieved from National Institute of Justice: https://nij.ojp.gov/topics/articles/evolution-transnational-organized-crime

Olson, J. (2019). Professor Texas A&M (former CIA). (Caskey, Interviewer)

Paquette, D. W. (2020). Al-Qaeda and Islamic State groups are working together in West Africa to grab large swaths of territory. *The Washington Post*, pp. https://www.washingtonpost.com/world/africa/al-qaeda-islamic-state-sahel-west-africa/2020/02/21/7218bc50-536f-11ea-80ce-37a8d4266c09_story.html.

Strack, C. (2017). The Evolution of the Islamic State's Chemical Weapons Effort. *CTCSENTINEL Vol 10 Issue 9*, 19-24.

Terrorism, S. (2010). General Terrorism Discussions. (S. Caskey, Interviewer)

Thuras, D. (2014). *Atlas Obscura.* Retrieved from The Secret's in teh Sauce: Bioterror at the Salsa Bar: http://www.slate.com/blogs/atlas_obscura/2014/01/09/the_largest_bioterror_attack_in_us_history_began_at_taco_time_in_the_dalles.html