ICIT Analysis: The Wound Collectors

Profiling the Self Radicalized Lone-Wolf Terrorist

June 2016

Authors

James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (Researcher – Institute for Critical Infrastructure Technology)

ICIT Briefing: The Anatomy of Cyber-Jihad
June 29, 2016
Washington D.C.

Join ICIT experts as we discuss the findings of this publication and identify solutions to protect our critical infrastructures and our way of life.

http://icitech.org/event/the-anatomy-of-cyber-jihad-cyberspace-is-the-new-great-equalizer/

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Table of Contents

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Introduction:

The lone wolf is a self-radicalized, homegrown terrorist fueled by an extremist perspective of a distorted ideological variant. Whether they be Islamic Jihadists or far right/left anti-government activists, these contorted dogmatic mutations are merely a centralized point of focus for a deeper psycho-social affliction in the individual. Acts of domestic terrorism in the West are escalating at an alarming rate and due to the instant gratification provided by the internet and social media, there is no perspective, no matter how extreme, that is not readily available in the form of forum, chat or propaganda to the individual who ventures to find it. At this time, lone wolf attacks and attackers have sparked public, political and law enforcement curiosity due to the, seemingly, random and independent action of a self-radicalized extremist with modest or no ties directly to the group in which they proclaim the action to be dedicated. A more comprehensive understanding of the perplexing composition of the lone wolf is a mandatory prerequisite to creating lasting strategies to combat the escalation of this profound domestic threat. Certain events have garnered more media coverage, such as:

- September 2013, Aaron Alexis killed 12 people at the Washington Navy Yard
- November 2014, Larry McWilliams fired more than 100 rounds at four government buildings in Austin, Texas
- July 2015, John R. Houser killed two people and wounded nine others at a movie theater in Lafayette, Louisiana
- October 2015, Christopher Harper-Mercer killed 9 of his peers at Umpqua Community College in Oregon
- December 2015, Syed Rizwan Farook and Tashfeen Malik, husband and wife, killed 14 people at a holiday office party in San Bernardino, California
- June 2016, Omar Mateen killed 49 people and injured 53 others at the Pulse nightclub in Orlando, Florida.

All of these tragedies, and numerous others, were committed by troubled American citizens, against their own people, with little or no help from foreign influences. These threat actors were lone-wolves. The Georgetown University National Security Critical Issue Task Force (NSCITF) defines lone-wolf terrorism as: "*The deliberate creation and exploitation of fear through violence or threat of violence committed by a single actor who pursues political change linked to a formulated ideology, whether his own or that of a larger organization, and who does not receive orders, direction, or material support from outside sources*." Decades ago, radicals could be monitored through the group meetings they attended, the purchases that they made, and the information (blueprints, instruction books, etc.) that they sought. Now active membership in organized hate groups is in decline because the internet affords troubled minds

a thick layer of anonymity and numerous websites, forums, and message boards, where they can self-radicalize and learn dangerous information. The Southern Poverty Law Center studied 63 incidents that occurred between April 2009 and February 2015, and found that a domestic terrorist attack or foiled attack occurred almost every 34 days and that lone-wolf threat actors were behind almost three-fourths of the attacks. Anti-government extremists perpetrated roughly half of the incidents, while white supremacists or Islamic extremists perpetrated the remainder. Lone-wolves join these communities and ideologies because they want to escape their lives and express their internal frustration, rage, and resentment, in service to a cause more meaningful than their existence. A lone-wolf threat actor is the result of a lifetime of hate, anger, and loneliness. Joe Navarro, one of the founders of the FBI's Behavioral Analysis Unit refers to lone-wolf extremists as "wound collectors". There are three distinct stages in their development: ideation, isolation, and action.

Development

Early Development
Domestic terrorists are not the sole product of an ideology, of the mental health system, or of the American society; rather, they are the cumulative amalgamation of numerous contributing factors, congealed into a troubled mind, and expressed through acts of violence. Many, but not all, lone-wolf terrorists exhibit some, or all, of the following characteristics: a mental illness, anxiety, vocational problems, high-stress levels, problems with intimate partner relationships, social awkwardness, violent communications, and high intelligence. All lone-wolves lack empathy for their fellow humans. These tendencies develop over a lifetime, not an instant.

There is no definitive profile for lone-wolves; however, every lone-wolf lies on the same spectrum and exhibits some of the characteristics within the profile. Lone-wolf tendencies are the result of a lack of socialization and the formation of meaningful interpersonal relationships in early development. Often, this begins in early childhood or adolescence, with a poor home life. Sometimes one or both parents are physically or mentally abusive; in other cases, guardians are negligent. In either situation, their internal familial structure is weak and the child develops devoid of strong emotional attachments. The term "lone" is in lone-wolf for a reason beyond their independence in their actions. These threat actors have a history of being "loners," "quiet," or "losers." They are often remembered as uncharismatic silhouettes in the far corners of memories. Their detachment and lack of developed interpersonal skills makes them either the targets of schoolyard bullies or the bane of social crowds, often both. Their stunted development and their isolation often lead to emotional or psychiatric instability. The subject becomes comfortable with thoughts or acts of violence against themselves or others.

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Developing lone-wolves used to retreat into their rooms or to isolated areas to escape the suffocating purgatory of their lives, until they were old enough to escape with all of their pent-up hatred. Now, these troubled minds turn to online communities, propaganda, and message boards, for immediate escape and acceptance. As a result of the ubiquity, availability, and pervasiveness of the internet, the age of lone-wolf threat actors is decreasing and they are entering the ideation stage earlier in life.

Later Development

The lone-wolf attacker often experiences four periods that cause them to enter the ideation stage after early development. First, they experience some form of grievance. This feeling of being persecuted, bullied, threatened, injured, or broken may stem from early development, or it may derive from disenfranchisement later in life. As a result, they experience depression as a form of restlessness, despair, or suicidal temptation. An unfreezing event, a crisis where there is perceived or experienced major loss, such as loss of relationship, loss of vocation, public humiliation, or failure or loss of status, causes them to project their grievances as an act of depression onto a manifested target and enter the ideation stage. Essentially, the severances of the connections that bind the individual to society leave them with little to lose; thereby freeing them to commit radical actions. Finally, usually before the cycle, or between the isolation and action stages, the subject familiarizes themselves with firearms and other weapons.

Background checks and other similar mechanisms have not yet prevented lone-wolves from legally obtaining firearms. Individuals like Mateen, who had neither a criminal past nor a record of diagnosed mental illness, are difficult to detect. Nevertheless, detection is not impossible. The FBI investigated Mateen twice and interviewed him three times for connections to domestic terrorism. Mateen had a history of weapons training, he worked as an armed security guard, and he had applied to be a police officer. Even if he passed the check and was permitted to purchase the handgun and long gun that he did prior to the Pulse shooting, the check could have thrown up a red flag that would have informed law enforcement to watch his activity.

The Stages of Lone-Wolf Development

Ideation

Sixty-eight percent of lone-wolf attacks that occurred between April 2009 and February 2015 were conducted by males, between the ages of 20 and 49, and 59% used firearms that were legally purchased within two months of the attack. In contrast, violent criminals are typically within the age range of 15-24 years. The older range of ages suggests that the lone-wolves spend years absorbing radical ideology before finally turning belief into action and committing

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

acts of violence. Due to the advent of the internet, potential threat actors have greater access to polarizing material that they can use to self-radicalize earlier and faster, which explains why recent threat actors have been younger than the range. Law enforcement has less time to detect, deter, or prevent lone-wolf activities on an individual basis. The availability of material and the permutations of jihadist and anti-government ideologies means that law enforcement also must monitor significantly more threats across numerous additional channels and threat vectors. The most effective way to prevent threats from developing is for citizens and law enforcement to detect threats in the ideation stage and initiate monitoring or counter measures before the threat further develops.

The ideation stage begins with the development of a fixation on a specific grievance against a target who the subject feels harmed or committed an injustice against them. Often, the fixation is the projection of years of grievances and wounds onto a tangible target or target group who committed limited or no harm to the individual. Because the subject withholds internal anger or resentment from their development stage, they use the target as a manifested outlet and then they adopt an ideology or belief structure that allows them to rationalize those feelings against that target. Once they believe their own justification, they begin to spread the adopted views to their limited number of family or friends. In absence of either, the subject may contact strangers on the street or join a form of social activism (pamphletting, protesting, etc.) to extend their message. Those that they reach out to usually dismiss the ideas as nonsense, uncomfortable opinions, or idle banter. Consequently, the subject begins to withdraw and become less vocal with those in their lives. Eventually, the subject becomes physically or emotionally isolated.

Isolation

The subject seeks an online community to validate their views. Once they find a website or forum to reinforce their vitriolic mentality, they begin a steep decline. Without a rational source, such as friends or family to dissuade or challenge the thoughts, the subject begins to actively communicate with likeminded individuals. Internal arguments within the community and oppositional forces cause the subject to become entrenched in their beliefs. As they self-radicalize online, efforts to detect or predict their activity become increasingly difficult because they move to different forums, transition to more secure communication channels, or migrate further into the deep net.

A two-year study of extremists conducted by the Intelligence Project identified ten characteristics shared by killers who were active online. All of those monitored were unemployed or had difficulty holding employment. All engaged in a form of public activism at some point in their development. Many of the subjects had a history of domestic violence or

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

incidents at their homes. Social science suggests that there may be a correlation between domestic violence and lone-wolf attacks. An analysis of FBI data on mass shootings from 2009 to 2015, revealed that 16% of lone-wolf attackers, had a history of domestic violence. Additionally, 57% of lone-wolf threat actors include at least one family member in their victims. Each subject posted on more than one message board, blog, or website. They frequented these channels for at least 18 months prior to their actions. On the sites, they exhibited antagonistic or argumentative behavior with other users. There was an increase or decrease in their posting patterns in the months prior to the attacks. Each discussed violence as an acceptable and justified solution to their grievances. Weapons were also actively discussed. Finally, a specific "enemy," usually members of another race or the government, were identified as the source of their problems. Extremists in this state of mind develop a significant amount of anxiety and inner turmoil as their mind obsesses and fixates on their ideology and "enemy." Eventually, the only way to relieve the anxiety is to harm or kill someone.

Action

The subject may stew on their mental state for years or decades while they acquire weapons, scope out targets, and plan their attacks. The lone-wolf may delay action by victimizing friends and family or by perpetrating other, smaller crimes. They may even convince others or themselves for a time that the plan is only a hypothetical expression of frustration upon which they will never act. At this stage, lone-wolf threat actors are nearly ready to cause serious harm. Ironically, this is also the most difficult time to detect their intent. It is the responsibility of friends, family members, and others to report indications of an impending incident to law enforcement instead of dismissing or discounting individuals who try to recruit or who try to preemptively justify their actions. For instance, Omar Mateen's second wife, Noor Salman reportedly knew of her husband's plans and may have even helped him scope out venues to attack. If she had reported his activities to law enforcement, then 49 deaths and 53 injuries could have been prevented.

Contributing Factors

Ideology

Lone-wolf threat actors are not solely driven by ideology. Eliminating ideology will not prevent lone-wolf attacks. Ideology is simply the outlet that the internal radicalization is expressed through. Ideology does provide a sense of self and a sense of purpose that troubled individuals have difficulty finding in other facets of their lives. Ideology can act as a social motivator that polarizes the individual to act on internal biases and hatred. Ideology does not cause an impairment of will. In most cases, the lone-wolf actor has a stronger will than the majority of

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

devout followers of an ideology; this is because the lone-wolf is using the ideology as a vehicle to justify their actions rather than a crutch to find a sense of greater purpose or meaning. Without the specific ideology such as conspiracy theories, Islam, racism, etc., the threat actor would find another channel to slowly turn than passion into hatred into terrible action. Across the globe, there are approximately 1.2 billion Muslims and 2 billion Christians. Of each group, a few hundred thousand members carry radical views. Of that small percentage, only a fraction of a fraction commits violent acts because they recognize that opinions are cheap, opinions are numerous, and that such actions are costly, disruptive, and likely violate the tenets of their religion.

Mental Health

There is a substantial gap between belief and action. A significant number, but not all, lone-wolf threat actors suffer from diagnosable mental illnesses. Common symptoms are anger control problems, obsession, depression, and suicidal thoughts or tendencies. The threat posed by lone-wolf activists can be reduced by collecting better intelligence and training law enforcement more effectively, but it can also be reduced by improving our behavioral health system and increasing the quality and availability of those services. A severely troubled individual capable of lone-wolf attacks is in the most need of access to high quality, non-stigmatized behavioral health and ancillary services when they experience the violent or isolationist tendencies that lead to self-radicalization. Only a minority of people with mental illnesses are even remotely violent; however, some studies have indicated that within terrorist populations, a larger percentage of lone wolf terrorists are found to be mentally ill than group-oriented terrorists. Mental health patients sometimes describe their actions after the fact as compelling delusions, citing phrases such as "I was not myself" or "I was out of my mind." Lone-wolf threat actors do not exhibit this characteristic. They premeditate, plan, and execute their agendas. This demonstrates that mental health is not the cause of their actions, but like ideology and access to weapons, is merely a contributing factor in the puzzle that is the mind of a lone-wolf threat actor.

Propaganda

 Jihadist propaganda and anti-government manifestos convince troubled individuals to believe that they can be the sole soldier who turns the tides of war, exposes the great evil, or strikes a devastating blow to the enemy. As a result, lone wolf attacks are conducted on behalf of the cause without direction or communication with the group. The jihadist propaganda machine is well resourced and ubiquitous across social media and the internet. Its propaganda calls for lone-wolf actions, glorifying the actions by deluding troubled minds into believing that they can serve a greater cause through their actions and thereby have a meaningful impact on a

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

community that wants and accepts them. Racist and anti-government militants are similarly attracted to numerous conspiracy message boards, publications, and sites for the self-gratifying communities of fellow isolationists who congregate there.

Researchers at the University of Miami studied second-by-second longitudinal records of online support for ISIS propaganda since its formation in 2014. They found that lone wolf supporters only remained alone for a few weeks at most before they were drawn into larger communities, referred to as aggregates. They studied 196 pro-ISIS aggregates consisting of over 108,086 individual followers between January 1, 2015 and August 31, 2015. By the end of August, the number of lone wolf and aggregate participants numbered 134,857. With their data, the researchers were able to model the propaganda transfer network and discern a few preliminary conclusions. Anti-ISIS agencies can prevent the formation of large pro-ISIS online groups by breaking up smaller ones. If anti-ISIS agencies are not active or not active enough, ISIS support grows exponentially into super aggregates of smaller groups. Further, When ISIS networks are not fragmented fast enough, a piece of propaganda can spread at a rate proportional to the speed of the channel times the probability of follower-to-follower transmission, divided by the rate of follower recovery. The rate of fragmentation must exceed this ratio to prevent the diffusion of materials. Essentially, by actively targeting small aggregate communities before they merge into larger communities, law enforcement can combat threats. They can stymie the polarization of lone-wolf threat actors and they can preempt the formation of resilient complex terror networks.

The most effective mechanism for limiting lone-wolf activism is to restrict access to the propaganda online. Anonymous and US Cyber Command are already conducting cyberattacks against ISIS's infrastructure. Jihadist Twitter accounts, forums, and communication channels are likewise targeted. The State Department has also started to empower those living in the affected regions to launch counter-propaganda campaigns to dispel the allure surrounding ISIS. The United States has also targeted ISIS's financial resources to reduce its ability to pay its fighters. The combination of these efforts have reduced ISIS's recruitment and its distribution of propaganda; however, propaganda is cheap, the internet is vast, and lone-wolf threat actors are waiting for the right cause to lure them to action. As long as extremist organizations such as ISIS or anti-government movements exist, they will continue to produce propaganda and infect the minds of troubled individuals.

Those seduced by jihadist or anti-government propaganda are troubled individuals who are desperate for a sense of purpose, a community, or an escape from their internal or external conflict. These individuals want to feel important in some way. They want to justify their hatred, bias, or resentment through a cause larger than themselves, within a community of

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

peers. In a sense, they crave the literal power that they feel when they choose a target and plan the attack. They crave the euphoria over the decision of who lives and who dies, because it affords them a level of control that they do not have in their average life. Prior to extreme self-radicalization, lone-wolf attackers tend to adopt an affinity for weapons and the power that they associate with them.

Conclusion

The new landscape of warfare is a convergence of the cyber and the physical. One side will fight for a perversion of extremist ideology; the other side will fight for its right to exist. Digitized information warfare and propaganda will be used in unison with scattershot lone wolf attacks by one opponent while the larger more technologically sophisticated side will continue to depend on traditional outdated mechanisms of combat that yield inferior results. This new war will be fought on the terms of highly maneuverable techno-guerrillas while world power giants clumsily fumble about as old alliances crumble and new powers are erected by sheer will, and a willingness to do anything and everything necessary in order to achieve a distorted version of global domination.

This new war is first and foremost a battle for the mind of a psycho-architype that is fueled by propaganda that will satisfy all ranges of rhetorical intrigue and violent curiosity. This propaganda, packaged and delivered via all layers of cyberspace, is calibrated with the intention to steer the mentally unstable, socially isolated and emotionally fractured target toward an ideology with the aim to capitalize off this malicious insider who is ready to consummate the violent threats that they have broadcasted to family, friends and virtual peers. Lone wolf actors pose the most devastating insider threat to the general population at large.

What is the solution to the conundrum of federal "bureaucracy paralysis" whose totem pole chain of power creates the illusion of action while the individual's lack of action is camouflaged in the chain of command? State sponsored theatrics such as signs stating "If you see something, say something" do little more than cultivate the illusion of security and introduce new elements of paranoia that only distract law enforcement attention from investigating those with true telltale signs of an active threat. An update in general law enforcement education, the localized and federal monitoring of online activity by those on forums that truly pose a threat to national security and a revolution in meaningful threat sharing are the embryonic starting point for erecting defenses that truly combat the lone wolf threat.

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Contact Information

Legislative & Executive Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agency Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Sources:

CBS News:

http://www.cbsnews.com/news/orlando-shooting-omar-mateen-father-seddique-mateen-taliban-god-punish-gays/

Mother Board:

http://motherboard.vice.com/read/what-is-a-lone-wolf-terrorist

New York Times:

http://www.nytimes.com/2016/06/16/world/americas/control-and-fear-what-mass-killings-and-domestic-violence-have-in-common.html?rref=us

http://www.nytimes.com/interactive/2015/10/03/us/how-mass-shooters-got-their-guns.html?_r=0

Psychology Today:

https://www.psychologytoday.com/blog/stop-the-cycle/201501/lone-wolf-terrorists-and-mental-illness

https://www.psychologytoday.com/blog/the-modern-mind/201410/the-making-lone-wolf-terrorist

Taylor and Francis Online:

http://www.tandfonline.com/doi/abs/10.1080/19434472.2015.1070189

Terrorism Analysts:

http://www.terrorismanalysts.com/pt/index.php/pot/article/view/240

University of Maryland:

https://www.start.umd.edu/publication/toward-profile-lone-wolf-terrorists-what-moves-individual-radical-opinion-radical-action

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

YouTube:

https://www.youtube.com/watch?v=M7tpWFF0KtQ

https://www.youtube.com/watch?v=FI8ANFm3p1s

https://www.youtube.com/watch?v=dytL0a5YePw

ICIT | Institute for Critical
Infrastructure Technology

The Cybersecurity Think Tank