Proceedings of the National Conference
On Undergraduate Research (NCUR) 2016
University of North Carolina, Asheville
Asheville, North Carolina
April 7-9, 2016

Counterterrorism or Vigilantism? The Cyber War Between ISIS and Anonymous

Amy Thomas and Rachel Drummond
Politics and Geography Department
Coastal Carolina University
Conway, SC 29526 USA

Faculty Advisor: Dr. Joseph Fitsanakis

Abstract

On November 15, 2015, two days after the Paris attacks that killed and wounded hundreds, the cyber hacking group Anonymous declared war on the Islamic State of Iraq and Syria (ISIS), the militant group that claimed responsibility for the attacks. Within a week, Anonymous had taken down 20,000 ISIS-related Twitter accounts. It also accused Internet service providers that host ISIS websites of collaborating with the militant organization. In response, ISIS warned that they "will respond to the threat" and published advice on how to counteract hacking attacks by Anonymous. Since 2011, when Anonymous declared war on the United States government, the group has had a less than amiable relationship with US intelligence and security agencies. By 2013, US authorities had arrested many key members of the group; but Anonymous continued to launch cyber attacks against government servers, defacing federal websites and releasing the private information of government officials. Given the adversarial relationship between the US and Anonymous, what are the ramifications for US national security of Anonymous declaring war on ISIS? Could this development potentially provide the US with an advantage in the broader war against ISIS? To answer this question, this paper will examine the Anonymous-ISIS war under the prism of two disciplines, Counterterrorism and Information Assurance. It will argue that, regardless of its outcome, the cyber war between Anonymous and ISIS is detrimental to US concerns. This unfolding confrontation between two non-state actors with a history of criminal activity is unlikely to follow conventional counterterrorism guidelines. Despite the shared goal of the US and Anonymous to destroy ISIS, Anonymous is employing vigilante tactics that undermine the international system of law and order. Such vigilantism, even if successful, can be expected to subvert the principles of information assurance, on which the very idea of cyber security is based.

Keywords: ISIS, Anonymous, Cyber warfare

1. Introduction

On November 15, 2015, two days after the Paris attacks that killed and wounded hundreds7; the cyber hacking group Anonymous declared war on the Islamic State of Iraq and Syria (ISIS), the militant group that had previously claimed responsibility for the attacks2. Within a week, Anonymous had taken down 20,000 ISIS-related Twitter accounts5. It also accused Internet service providers that host ISIS websites of collaborating with the militant organization. In response, ISIS warned that they "will respond to the threat" and published advice on how to counteract hacking attacks by Anonymous. Since 2011, when Anonymous declared war on the United States government, the group has had a less than amicable relationship with US intelligence and security agencies22. By 2013, US authorities had arrested many key members of the group24; but Anonymous continued to launch cyber attacks against government servers, defacing federal websites and releasing the private information of government officials4.

Given the adversarial relationship between the US and Anonymous, what are the ramifications for US national security of Anonymous declaring war on ISIS? Could this development potentially provide the US with an advantage

in the broader war against ISIS? To answer this question, this paper will examine the Anonymous-ISIS war under the prism of two disciplines, Counterterrorism and Information Assurance. It will argue that, regardless of its outcome, the cyber war between Anonymous and ISIS is detrimental to US concerns. This unfolding confrontation between two non-state actors with a history of criminal activity is unlikely to follow conventional counterterrorism guidelines. Despite the shared goal of the US and Anonymous to destroy ISIS, Anonymous is employing vigilante tactics that undermine the international system of law and order. Such vigilantism, even if successful, can be expected to subvert the principles of information assurance, on which the very idea of cyber security is based.

2. Definitions

It is essential for the comprehension of this paper that terrorism is clearly defined. The phenomenon of terrorism has many conceptual descriptions, making it hard to define because it is not a "physical entity that has dimensions to be measured, weighed, and analyzed"25. However, all definitions conclude with the same general thought, namely that the purpose of terrorism is to achieve a political goal, with religion involved only during the most recent wave of terrorism, namely since the 1980s. Intimidation and coercion are used to instill fear in a population, in order to influence the policy of a government. Mass destruction, kidnapping, and assassination are just some of many terrorist tactics.

Anonymous, is a cyber vigilante "brand or collection" and they claim to "be everything and nothing" meaning that the term "group" is inapplicable19. They define their reason for existence as protecting the freedom of information, especially cyber information. They state that "We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us"18. They use an anonymous membership system and members within the organization are called Anons21,10. They also have an anonymous voting mechanism to select their targets and impose their beliefs, all in hopes of furthering their political goal of freedom of speech and freedom to access information. One of the main aspects of their ideology surrounding the attacks is shown by Olsen's portrayal of the organization; "if you disagree with their beliefs your website may become a target"19 This is important as it shows that Anonymous are indiscriminate in their attacks and focus on an entity's beliefs and actions rather than who they are, (governments and other cyber groups are not exempt). There is no structured leadership system within Anonymous, making it an adaptable and elusive organization. Anonymous was born in the 4chan, an anonymous online bulletin board that focused on "ruining the reputations of individuals and organizations by revealing embarrassing private information"10, In essence the roots of Anonymous stem from an online bulletin created for recreational hacking that turned into a political campaign after communication and collaboration of various hackers on the site.

"Their sociology is a labyrinth", the planning process of attacks is incoherent and can be "devilishly confusing"10. To be a part of Anonymous is to "follow a series of related principles. Anonymous follows a spirit of humorous deviance, works through diverse technical means, is built on an anti-celebrity ethic and intervenes politically"10. Anonymous was actually stating their foundations in the reverse; they stand for morality, accountability, freedom of speech (which is "non-negotiable"10), and freedom of the public to access all information. These goals are reiterated on their main website "Anonops" which is the base of their chat room communications system. They state on their website that "We must all speak out against the obliteration of our privacy by governments everywhere and to stop the persecution of activists by vindictive governments" 10.

Such philosophy points to a adherence to crypto- anarchism in which they "espouse the use of strong encryption to enhance individual privacy, while at the same time opposing its use by state and corporate entities, which they consider inherently oppressive and conspiratorial"11. This philosophy seems to accurately describe the driving force behind Anonymous and their ongoing operations against both governmental and non-governmental entities that they view as corrupt and/or violating people's' civil liberties or human rights. To them this philosophy goes beyond the basic definition of opposing state and corporate entities, and includes individuals who are impacting the rights of others, including but not limited to rapists, pedophiles and government officials.

The focus of Anonymous' declaration of war is ISIS, an Islamist terrorist organization that formed out of an off-shoot of al-Qaeda; it was once called "al-Qaeda in Iraq" before morphing into what is now known as ISIS. ISIS is one of the "most brutal and richest terrorist organizations today"20. al-Qaeda has "demonstrated an ability to develop and support terrorist attacks beyond their immediate geographical locations" with "groups emerging as threats to regional stability" and other Western security25. ISIS on the other hand is concerned primarily with internal conflicts and controlling territory in their immediate geographical locations. "ISIS had the opposite strategy (of al-Qaeda), they were focused on their people and all brutal acts were inflicted on their own people"17. There are various dates that

have been noted as the founding of this organization, the literature is not very clear on that25. Under the leadership of Abu Bakr Al-Baghdadi, today ISIS uses terrorist tactics to instill fear as a way of achieving their political and religious goal of establishing an Islamic Caliphate in Iraq and the Levant6. They have recently begun using the internet to further their recruitment and attack capabilities16. ISIS is driven by their devout following and extreme interpretation of Sharia law, a strict version of the laws described within the Quran; these laws control the social, private, legal and political aspects of a person's life and are enforced by a religious council. The group's theology is based on a militarized version of Islam, which stems from al-Qaeda5. ISIS desire to enforce Sharia law on the populace, surpassing al-Qaeda has made them an appealing target of Anonymous, as it stands for the repression of the personal freedoms that Anonymous bases its ideology on.

After claiming responsibility for the Paris attacks16, ISIS attracted the ire of Anonymous who are directing their cyber capabilities against the Islamist group. This can be described as a form of cyber warfare, which is understood in this paper as the use of the internet and information technologies to carry out politically or socially motivated attacks, disabling and/or defacing official websites and/or networks, sabotaging social services and stealing damaging information from another entity. The actions of a nation-state or international organization which are involved in cyber warfare, involve attempting to damage the networks and information of another country. Anonymous has carried out cyber attacks on the US government, leaking stolen classified documents to the general public in order to further their political freedom of speech, and access to information. Some experts, like Michael Steinbach, the head of the Federal Bureau of Investigation's (FBI) counterterrorist division, have argued that Anonymous declaring cyberwar on ISIS is counter-terrorism9, which is the use of political and military activities to prevent terrorism18, Steinbach states that the actions of Anonymous are often viewed as vigilante tactics that undermine the international regulation of law and order. Vigilantism is when an individual or group takes the law into their own hands defying set methods of law and order.

3. Main Thesis

The cyber war between Anonymous and ISIS began on November 15, 2015. Anonymous' declaration of war on ISIS captured international interest as it signifies a new approach in combating the terrorist group. Instead of a war involving traditional military strikes, in the form of a state actor going after a non-state actor, this is a war between two non-state actors in the cyber domain15. This is a new and unexplored territory. With two actors that are answering to no higher law than themselves in the conduct of war, and do not acknowledge the traditional rules of engagement, it is difficult to predict the risks involved. This raises the question of whether the actions of Anonymous are counterterrorism or a form of vigilantism that undermines the international system of law and order. Pertaining to that, is the war between Anonymous and ISIS detrimental or beneficial to the interests of the US? The stance of this paper is the latter of the two, based on the fact that it endangers the information assurance process of the US. Information assurance is the process of protecting information systems, such as computer and technology systems, ensuring the integrity, availability, authentication, confidentiality and nonrepudiation of these systems.

In the short term, Anonymous's attacks may take ISIS offline, deter their recruitment efforts and help the US combat ISIS in the cyber domain, furthering US interests. We argue that Anonymous' targeting of ISIS social media accounts will benefit the US interests of deterring ISIS' online recruitment efforts. This has been demonstrated by Anonymous' ability to disable 20,000 ISIS Twitter accounts18. On the other hand, Anonymous could also act in ways that are detrimental to US interests. The detrimental effects this cyber war could have on US interests are due in part to the combative history between the US and Anonymous, which began in 2012, when Anonymous declared war on the US. The declaration of war was issued in response to the "Stop Online Piracy Act" sponsored by Republican Representative Lamar Smith of Texas. According to the US Congressional record, Rep. Lamar's proposal is "an act that authorizes the attorney general to use a court order against a US directed foreign internet site, facilitating online piracy to cease and desist further activities constituting specified intellectual property offenses under the federal criminal code"14.

The fact that Anonymous has declared war on the US government and ISIS, during the same period that the US has declared war on ISIS, creates a triangular relationship that, we argue, places the US information assurance system at risk. Part of the risk stems from the fact that the information flow on the World Wide Web can be crossed easily with two non-state actors hacking into one another's systems and then hacking into the US government systems at the same time. That allows for the crossing and accidental sharing of stolen US government documents, servers and networks. Such crossing of networks becomes detrimental if ISIS is able to access the same routes, codes and

processes that Anonymous may have used to hack US government networks. Such a triangulation would in turn lead to ISIS accessing US government servers, and could thus allow ISIS the breach the US government's information systems. We also argue that, due to the nature and objectives of Anonymous, this cyberwar may be short-lived and pose a greater threat to information assurance, due to the fact that the information both actors (ISIS and Anonymous) gather is scattered throughout the World Wide Web with no protective measures to secure, collect or monitor the distribution of data. We conclude that, overall, the cyber war between Anonymous and ISIS, whether vigilantism or counterterrorism, is detrimental to US interests and the US Information Assurance system.

4. Argument

We argue that Anonymous' targeting of ISIS social media accounts will benefit the US interest of deterring ISIS online recruitment efforts. "The use of social media has brought ISIS efficient results and accomplishments, especially in recruiting youth worldwide"23. Additionally it is the efficient use of social media that has allowed ISIS to disseminate their ideology and goals so rapidly and efficiently23. In combating this it makes sense to allow another organization that is just as, if not more efficient in the use of social media and the mass media. When Gabriella Coleman gave her brief on Anonymous to the Canadian Security Intelligence Service (CSIS) in 2012, she was interrupted by "the resident anthropologist who specialized in Middle East terrorism. 'The anthropologist explained that jihadists were impressed by the level of media attention' that Anonymous attained"10. Who better then to defeat this technologically savvy jihadist organization, than the ones who impressed them with their use of social media sites to enhance their global recognition and attention? This equal match-up is due not only to the terrorist organizations use of Anonymous' success online as a blueprint, but also because of the age of the groups' members. Both Anonymous and ISIS are primarily composed of millennials who are technologically savvy and equally attached to social media for their day-to-day operations and activism23. This leads into the next point we found when looking into the benefits Anonymous' targeting of ISIS.

According to Michael Steinbach, the head of the FBI's Counterterrorist Division, the "sheer volume of posts" put out by ISIS on a daily basis is a "full time job and a challenge to monitor"9. This is where Anonymous has an advantage, since their only objective is to monitor, deface and disable online sites. Since declaring war on ISIS, they have proven that they are capable of disrupting the stream of online messages ISIS is able to post8. As Anonymous is a flexible, widespread organization it is able to attack ISIS sites from varying IP addresses, using complex techniques and to shift through the volume of data at a pace faster than that of the US Intelligence Community8. By 2011 Anonymous "had operations and dedicated IRC channels for Italy, Venezuela, Brazil, Syria, Bahrain, Tunisia, Egypt and Libya"10. This shows how widespread their operational capabilities are and the scope of their membership. Add to that the mere fact that they were already established in Syria before the rise of ISIS, meaning they had a strategic advantage in the cyber world compared to the US. Anonymous' targeting of ISIS recruitment accounts has the ability to deter ISIS recruitment methods at a higher efficiency rate than the US intelligence community. Due to their highly unregulated structure that allows them an advantage in counterattacks, they can't be crippled if one aspect of their system is compromised. Though unconventional, it has the ability of furthering the US interest of deterring ISIS recruitment through social media.

We also argue that the US information assurance system is at risk due to the triangular relationship between the US, ISIS and Anonymous. Anonymous has the capability to retrieve sensitive US government documents, as they proved after declaring war on the US government in 2012. The routes and IP addresses they used to gather that information may still be available on their servers. The leaking of information by Edward Snowden and their subsequent attacks on the US, due to this leaked information in 2013, led to the revival of Anonymous, after "numerous hackers associated with Anonymous were in prison cells"10. On their website Anonops, Anonymous states that "Edward Snowden is a brave individual fighting for what he believes in and words cannot express how thankful we are for what he has done. We can only hope that this leak helps to aid those who have been so wrongly prosecuted in their legal battles"4. As they attack ISIS social media accounts, IP addresses and servers, ISIS will counterattack and adapt to the threat. As ISIS does this, there is the risk that ISIS will be able to access US government documents that have been stored on Anonymous' servers. The risk of ISIS being able to use and/or hack the routes previously used by Anonymous to hack US government servers, is also a concern as it puts the US information assurance system at risk by both ISIS and Anonymous.

Currently, there is no new information concerning the cyberwar between Anonymous and ISIS. This lack of information could be viable intelligence in itself, or just a lack of interest from news media, as it is not the latest

breaking news. The American Press institute defines a good story as "complete and comprehensive, containing verified information from varied sources and perspectives, therefore exhibiting more expertise and enterprise"3. Something that proves difficult for those reporting on the Anonymous and ISIS cyber war, as there are few dependable sources of information or a defined structure of what is happening. This is due to cyber warfare being a new, under-studied action. Therefore, the cyber war between Anonymous and ISIS may be continuing, just behind scenes, or out of public knowledge due to lack of reporting interest. However, it is still a concern of professionals of the US security and information assurance system. This is due to the unknowns produced by the uncertainty surrounding this cyber war. This uncertainty creates implications for national security policy, as a nation tries to mitigate threats posed to its strategic interests. Such mitigation of threats includes "the discovery of new resources and technologies... and the fact that states have a particular strategic interest in its ability to effectively promote and defend the broad range of its national interests"12. This ability is inhibited when it comes to the unknowns involved in the cyber war between Anonymous and ISIS.

We also argue that due to the nature and objectives of anonymous, this cyberwar may be short lived and pose a greater threat to information assurance; the information both actors (ISIS and Anonymous) gather is scattered throughout the web with no protective measures to secure, collect or monitor the distribution of the data. Anonymous has a history of jumping from target to target and/or from one cyber war to another. This has recently been shown in the lack of announcements concerning their cyber war against ISIS, but also in their declaration of war on Donald Trump at the end of 2015 after his proposal of "banning Muslims from entering the US"13. They appear to now be focusing their media coverage on this cyber war instead of their cyber war with ISIS13. There is no clear evidence as to whether or not they continue working on a war once they deem another threat important enough to declare war on. Anonymous' structure is "incoherent and like a room full of cats that can't be leashed. Ideas rise or fall based on their ability to garner supporter"24. This shows that their indecisive nature comes from the structure of their organization and is inherently difficult to mitigate. This is shown in their varying attacks that occur simultaneously such as, attacking these entities in February 2016; North Korean systems for their satellite launching, a local US government to state their purpose of existing, and their attack on the pro-rape group 'Return of Kings'".

On the other hand, their cyber war with ISIS may not be short lived, due to the fact that it has become a personal attack. Coleman states that "Anonymous is composed of people who decide to act together and separately to take a stand"10. They are also specific when it comes to their targets, Serracino-Inglott states that, "Operations don't simply spring out of the ether and can be easily linked to a particular network, such as AnonOps, AnonNet, or Voxanon to take three of the most important ones today"21. Serracino-Inglott also confirms that "there are regular participants" in these chat rooms21. Brian Knappenberger stated that "They're sort of protectors of the Internet. This is their territory, and if it's abused, they're personally offended24". Just as with their war concerning the US government, ISIS has infringed on the freedoms surrounding the cyber world, making this a war that seems less likely to leave the forefront of their minds anytime soon. Also, they are unlikely to leave ISIS alone anytime soon as their main prerogatives for existing are, "No war - No religions - No politics - No financial power - for a Better World"1.

5. Conclusions

In conclusion, we assert that, if the war between ISIS and Anonymous is short-lived, the communication among members of Anonymous and the concern of securing data retrieved would be a lower priority, compared to what would occur if it was a long term objective of the group that was revisited on a regular basis. However, due to the structure of Anonymous, it is less likely that the operation would be completely forgotten or compromised by ISIS attacks. "A common metaphor used to describe Anonymous is that of the Hydra, the dangerous mythical creature with many heads that cannot be killed. Just like the hydra's many heads, each Anon5 or sub-group of Anonymous operates with relative autonomy and destroying any single one is useless"21. Consequently, despite their faults and the risk they pose to the US information assurance system, Anonymous may be better suited than the US government to fight ISIS, as they have an asymmetrical advantage that the US does not; there is no one leader, person or area to target. In that sense, the US and ISIS are similar despite ISIS being nominally a non-state actor. They still have a hierarchical system, like the US, and their cyber divisions are consolidated. Anonymous, however, is able to immediately get back online after an attack, due to their diverse and multifaceted system of operation, allowing them to be more effective at fighting Anonymous. This is in comparison to the US, which uses a single hierarchy-based system, that if attacked would take longer to go back online and incur more damage than the system used by Anonymous.

Despite the obvious benefits, Anonymous still poses a risk to the US information assurance structure due to it being

a technically unsecure operating system with no official mechanism in charge to protect classified US documents and information channels. Their systems are delegated to one web page currently4. However, this website has only been in use since 2010 when they were forced to switch servers. The website states that they came under "counterattack and had to switch from "IRC of skidsr.us., to ChatNPlay," who then "threw them overboard" and they created their own URL of AnonOps4. This turnover from site to site, shows the unreliability of information assurance within the group and that, although Anonymous' systems are multifaceted and able to reform quickly, they are still subject to counterattacks which cause them to abandon sites and move their platforms frequently.

The last conclusion of our research is that despite the gains made by Anonymous in the cyber war against ISIS, there is a clear distinction between vigilantism and counterterrorism efforts. Anonymous may have an advantage in the cyber war against ISIS due to their hydra-like structure21; however this is also their disadvantage. They are trying to defeat ISIS and simultaneously promote freedom of speech, press and a free internet by' mob rule', the "control of a political situation by those outside the conventional or lawful realm, typically involving violence and intimidation" (Oxford Dictionary). This is a weak and caveated system that employs vigilantism instead of counterterrorism. "Anonymous is indeed a vigilante organization"21 and we have to agree with that assessment; they answer to no state authority, their actions are preplanned and premeditated, and are in line with their minimally defensible values21. They are ostensibly motivated by justice and/or for the good of the larger community, and although their actions are not violent in the traditional sense, they do use harmful tactics to punish those they deem necessary of punishment. These factors of vigilantism and how Anonymous fits into this category are expanded upon in the writings of Serrancino- Inglott21. Due to this classification, it is unlikely that Anonymous can be relied upon to coordinate with US, state ran counter terrorism methods, which by definition are political or military activities designed to prevent or thwart terrorism. Such differing goals, methods and motivations are what imped Anonymous and the US working together to defeat ISIS online and highlight the threat posed to the US information assurance system by Anonymous.

6. References

1. Alexanderson, Christian. "'Anonymous' Hackers May Have Infiltrated York County Government Website." PennLive. February 5, 2016. Accessed February 16, 2016. http://www.pennlive.com/news/2016/02/anonymous_hackers_infiltrate_y.html.
2. Almasy, Steve, Pierre Meilhan, and Jim Bittermann. "Paris Massacre: At Least 128 Die in Attacks." CNN. November 14, 2015. Accessed March 14, 2016. http://www.cnn.com/2015/11/13/world/paris-shooting/index.html.
3. "What Makes a Good Story? - American Press Institute." American Press Institute RSS. Accessed February 25, 2016. https://www.americanpressinstitute.org/journalism-essentials/makes-good-story/.
4. "About Us." AnonOPs Anonymous Operations. Accessed February 25, 2016. https://anonops.com/about.html.
5. "Anonymous Claims to Have Taken down 20,000 IS Twitter Accounts." BBC. November 20, 2015. Accessed February 10, 2016. http://www.bbc.co.uk/newsbeat/article/34877968/anonymous-claims-to-have-taken-down-20000-is-twitter-accounts.
6. "What Is 'Islamic State'?" BBC News. December 2, 2015. Accessed February 10, 2016. http://www.bbc.com/news/world-middle-east-29052144.
7. "Paris Attacks: Who Were the Victims? - BBC News." BBC News. November 27, 2015. Accessed March 14, 2016. http://www.bbc.com/news/world-europe-34821813.
8. Brown, Michael A., and Daniel M. Gerstein. "Anonymous vs. ISIS: Wishing the Vigilante Hackers Luck Against the Murderous Jihadists." Anonymous vs. ISIS: Wishing the Vigilante Hackers Luck Against the Murderous Jihadists. December 14, 2015. Accessed February 12, 2016. http://www.rand.org/blog/2015/12/anonymous-vs-isis-wishing-the-vigilante-hackers-luck.html.
9. Brown, Pamela, and Wesley Bruer. "FBI Counterterror Chief's Worries about ISIS in U.S." CNN. February 3, 2015. Accessed February 14, 2016. http://www.cnn.com/2015/02/03/politics/fbi-isis-counterterrorism-michael-steinbach/index.html.
10. Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*.
11. Fitsanakis, Dr. Joseph. "UNDERSTANDING WIKILEAKS." UNDERSTANDING WIKILEAKS. January 6, 2011. Accessed March 28, 2016. http://www.rieas.gr/research-areas/editorial/1400-understanding-wikileaks.
12. Freeman, Charles W. *Arts of Power: Statecraft and Diplomacy*. Washington, DC: United States Institute of Peace Press, 1997.
13. Gibbs, Samuel. "Anonymous Collective Declares 'total War' on Donald Trump, Again." The Guardian. March

15, 2016. Accessed March 28, 2016. http://www.theguardian.com/technology/2016/mar/15/anonymous-declares-total-war-on-donald-trump-again.

14. "H.R.3261 - 112th Congress (2011-2012): Stop Online Piracy Act." H.R.3261. Accessed February 25, 2016. https://www.congress.gov/bill/112th-congress/house-bill/3261.

15. John, Tara. "Anonymous Launches 'Biggest Operation' Against ISIS in Response to Paris Attacks." Time. November 16, 2015. Accessed February 25, 2016. http://time.com/4114182/anonymous-paris-attacks/.

16. Luna Shamieh and Szenes Zoltan, "The Propaganda of ISIS/DAESH through the Virtual Space", Defense Against Terrorism Review, 7 (1), 7-31 (2015). http://www.tmmm.tsk.tr/publication/datr/volume10/02-ThePropaganda_of_ISIS_DAESH_through_VirtualSpace.pdf

17. Luna Shamieh and Szenes Zoltan, "The Rise of Islamic State of Iraq and Syria (ISIS)", Defense Against Terrorism Review, 14(4), 363-378 (2015). http://uni-nke.hu/uploads/media_items/aarms-vol-14_-issue4_-2015.original.pdf

18. Mastroianni, Brian. "Anonymous vs. ISIS: Who Has the Upper Hand in Social Media War?" CBSNews. November 24, 2015. Accessed February 25, 2016. http://www.cbsnews.com/news/anonymous-vs-isis-social-media-war/.

19. Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and, 2012.

20. Sekulow, Jay. *The Rise of ISIS: A Threat We Can't Ignore*. 2014.

21. Serracino-Inglott, Philip. "Is it OK to be an Anonymous?." *Ethics & Global Politics* 6, no. 4 (December 2013): 217-244. *Political Science Complete*, EBSCO*host* (accessed March 31, 2016).

22. Smith, Gerry. "FBI Agent: We've Dismantled The Leaders Of Anonymous." The Huffington Post. August 22, 2013. Accessed March 14, 2016. http://www.huffingtonpost.com/2013/08/21/anonymous-arrests-fbi_n_3780980.html.

23. Tawfeeq, Mohammed, and Chelsea J. Carter. "Officials: ISIS Recruiting on the Rise in Sunni Areas of Iraq." CNN. August 11, 2014. Accessed February 10, 2015. http://www.cnn.com/2014/08/09/world/meast/iraq-isis-recruit/index.html.

24. Times, High. "Anonymous Unmasked." The Huffington Post. June 1, 2014. Accessed February 10, 2016. http://www.huffingtonpost.com/high-times/anonymous-unmasked_b_5065038.html.

25. White, Jonathan R. *Terrorism and Homeland Security: Jonathan R. White*. Belmont, CA: Wadsworth, 2014.