Global Security and Intelligence Studies

Volume 2
Number 1 *Fall 2016*

Article 4

2016

Anonymous Versus ISIS: The Role of Non-state Actors in Self-defense

Andrew Colarik
Massey University

Rhys Ball
Massey University

Recommended Citation

Colarik, Andrew and Ball, Rhys (2016) "Anonymous Versus ISIS: The Role of Non-state Actors in Self-defense," *Global Security and Intelligence Studies*: Vol. 2 : No. 1 , Article 4.
Available at: http://digitalcommons.apus.edu/gsis/vol2/iss1/4

Anonymous Versus ISIS: The Role of Non-state Actors in Self-defense

Andrew Colarik[A] & Rhys Ball[B]

The use of cyberspace by terrorist organizations for command and control activities, recruitment and the dissemination of training materials is of ongoing concern for state actors. This is especially true because the nature of cyberspace makes efforts to limit and/or eliminate it exceedingly difficult. With the emergence of non-state actors such as the Islamic State of Iraq and Syria (ISIS) openly using cyberspace to spread its ideology and activities, other non-state actors such as the hacktivist group Anonymous have declared their intention to attack them anywhere they find them in cyberspace. This paper initially examines the cyberspace activities and capabilities of ISIS and Anonymous, and their roles and relationship as non-state actors. We then explore the notion of applying just war theory to non-state actors in self-defense, and propose a number of likely outcomes from our analysis.

Key words: *Terrorist, Cyberspace, Islamic State of Iraq and Syria, Anonymous, Non-state Actor, Just War Theory*

Introduction

> *The ultimate goal of stratagem is to make the enemy quite certain, very decisive, and wrong.*
>
> Barton Whaley, *Stratagem: Deception and Surprise in War,* 1969, p.135.

> *I call this whole thing the rise of the chaotic actor… [but] whoever fights monsters, should see to it that they themselves don't become one.*
>
> Joshua Gorman in *How Anonymous Hackers Changed the World*, May 2014.

The composition of actors who affect the national security of a nation-state can be both numerous and complex. The interaction between entities such as government agencies, nongovernmental organizations, citizen militias, media,

[A] Senior Lecturer, Centre for Defence and Security Studies, Massey University, Auckland, New Zealand
[B] Lecturer, Centre for Defence and Security Studies, Massey University, Auckland, New Zealand

doi: 10.18278/gsis.2.1.3

insurgencies, and other influential actors can affect how states operate in this global space. Additionally, this interaction between entities within the nation-state is making it increasingly more difficult for state actors to interact with other state actors in a cohesive and consistent manner. The influence of non-state actors on national security both within and without the state is becoming more problematic in an increasingly globalized space that challenges our traditional understandings of Just War Theory.

The role of information and communications technology and its resulting contribution to globalization is facilitating the rise of non-state actors in asserting themselves in ways that were once reserved for state actors alone. Technology increasingly enables the movement of non-state actors into multiple state jurisdictions and cross-border activities. The use of cyberspace by terrorist organizations for command and control activities, recruitment, and the dissemination of training materials is of on-going concern for state actors, and creates a new battlespace outside traditional state borders and jurisdictional lines toward interventions. With the emergence of non-state actors such as the Islamic State of Iraq and Syria (ISIS) openly using cyberspace to spread their ideology and activities, other non-state actors such as the hacktivist group Anonymous have declared their intention to attack them anywhere they find them in cyberspace.

In this paper, we examine how non-state actors are beginning to compete with other non-state actors in cyberspace, and consider how the Just War Theory of self-defense might apply to this domain. We consider this emerging phenomenon of non-state actors in conflict with each other by paying particular attention to the recent confrontation between ISIS and Anonymous and ask what implications can be derived from the emergence of competing non-state actors who consider themselves beyond the sovereignty of state actors. In conclusion, we further ask whether it is reasonable that they be allowed to conduct battle in the cyberspace domain within the previously established rules of Just War Theory or whether states should create new rules and adapt these into their respective national security strategies.

Just War Theory and Non-state Actors

The international system that emerged out of the Peace of Westphalia in the mid-seventeenth century has relied on state actors and their willingness to recognize sovereign territory and borders. There have been challenges to these states and borders since then, but recent conflicts enabled by emerging cyber capabilities present further obstacles to conventional paradigms and the historic legacies like the Sykes-Picot agreement of the last century (Dodge 2014). In the world of cyber-conflict, the question of cost in blood and treasure are terms that still apply even though the cost is not necessarily a physical one. The mass violence seen in previous wars as well as its impact at home is certainly not as severe in contemporary conflicts, but its proportionality and probability of success remain significant to the affected populations.

Just War Theory consists of *Jus ad Bellum*—the acceptable justifications for going to war in the first place, and *Jus in Bello*—the standard of conduct and activity during that period of conflict. Jus ad bellum contends that for any resort to war to be justified, a state must have the right reasons for war (Dipert, 2010). Just-war theorist Brian Orend (2008), in the *Stanford Encyclopedia of Philosophy* states that some of the most frequently mentioned right reasons—or "just causes" include "self-defence from . . . attack; the defence of others from such; the protection of innocents from brutal, aggressive regimes; and punishment for a grievous wrongdoing . . .". Orend adds:

> *An important issue in just cause is whether, to be justified in going to war, one must wait for the aggression actually to happen, or whether in some instances it is permissible to launch a pre-emptive strike against anticipated aggression.*

The remaining Just War Theory requirements contend that motivations for war or conflict must be morally appropriate; war can only be embarked on if the decision has been made by those who have the authority to do so, has been done by a proper and acceptable process, and publicly announced. As opposed to *Jus ad bellum*, *Jus in bello* may cause some real problems for the international community of states and numerous non-state actors. Just how one might hold those in breach of these principles accountable—especially when anonymity applies? Even more difficult in the cyber battle space context, how can we discriminate those innocent users caught up in any escalation from those legitimate targets through the use of "weapons" such as a Distributed Denial of Service (DDOS) or a disseminated malware attack? A deliberate DDOS attack would be taking "deliberate aim at civilians." That being said, Orend (2008) importantly tells us that "almost all wars since 1900 have featured larger civilian, than military, casualties." In the twenty-first century cyber-domain, while ethically unjustifiable, this is still likely to remain true.

Cyber conflict is becoming increasingly more attractive as a method of "first resort" and a real challenge to the just cause question becomes whether "first strike" cyber-attacks could or should be considered an act of defense from aggression? Targeting critical infrastructure that is managed or controlled via computer networks is now a very real "first strike" option. If we take their efforts and capabilities to date, as well as their language, Anonymous certainly believes that targeting ISIS is worth an effort. And, in particular, where do the likes of Anonymous sit with this dilemma? The use of weapons in cyberspace in a conflict may challenge the proportionality component to Just War Theory. Posner and Sykes (2004) suggest that a just war may proceed only if the benefits are proportional to the costs incurred. In a cyber-war between Anonymous and ISIS, the limits of proportionality may become too big when a nonviolent stratagem is employed against an extremely violent opponent. There may be a kinetic response to a digital attack or disclosure that results in loss of life and is clearly out of proportion. Just how far is a nonviolent non-state actor prepared to go in a war of self-defense? What sacrifices are they willing to make for their cause? Is this the "red line" that distinguishes whether a state actor actively or passively sides with the nonviolent non-state actor? Further examination of some of the activities conducted by Anonymous to date might provide a glimpse of what the organization might, or might not, be capable of doing if it engaged in a full-blown cyber conflict with ISIS.

Non-state Actors Versus Non-state Actors in the Cyber Battle Space

Definitions abound to exactly what cyber-war looks like. The concept is increasingly considered, challenged, debated, accepted, rejected, and embraced. However, some parties are not convinced that war, which is essentially destructive and leads to widespread loss of life, can be waged in cyber-space, nor can cyber-conflict ever be described as "cyber-war" until such time as there is direct and real "loss of life." Others contend that cyber-war, or cyber-conflict, is confined to what has been described as cyber-intelligence, cyber-espionage, cyber-disruption, and cyber-sabotage; activities which can be—and are—undertaken independently or in the context of a war. There are parties that claim that the effect of cyber-warfare is not destructive in the real world and therefore not war like (Wisniewski 2013, Valeriano and Maness 2012, Singel 2010). While cyber-attacks thus far have not directly killed people or significantly damage property, it can be a vehicle for such results. Economically, cyber-attacks may be able to cripple a nation in such a manner that it may have a similar effect to a sustained physical attack upon its industrial base or other facets of the economy (Ruus 2008). In that sense, cyber-war can have similar outcomes or impacts upon a nation as a real war would, and therefore an impact on non-state actors as well.

In 2008, the U.S. National Intelligence Council posited that by 2025 "Cyber and sabotage attacks on critical US economic, energy, and transportation infrastructures might be viewed by some adversaries as a way to circumvent US strengths on the battlefield and attack directly US interests at home" (DNI 2008, 97). Thus, squeezing or negating resources available to, or used by, non-state actors is a method which is used to degrade the economic—and therefore political—capacity of those particular actors. Traditionally, such action requires multistate actor collaboration. For example, there is some obvious reluctance for airstrikes to target ISIS-controlled oil installations. The environmental impact of such was there for all to see during the 1991 Gulf War. Most of the ISIS-controlled oil sold on the open market is smuggled through Turkey. Challenges for Ankara are numerous; porous borders, economic interdependence, political weakness, fear of reprisal, sectarian and ethnic divisions all contribute to Turkey being unwilling and/or unable to comply (Snyder 2014, Akyol 2014, Crompton 2014, Hawramy et al 2014, Giglio 2014, Hager 2014, and Sullivan 2014). Water resources in the region can also be used as both a source of revenue or bargaining chip for state actors and non-state actors alike. Again, Turkey plays a major role here. Turkey closed the Ataturk dam on the Euphrates in August 2014 and reduced water supplies to Syria and Iraq, which led to threats from ISIS. ISIS itself has used water and electricity as a weapon, cutting off the Euphrates water supplies to the Anbar Province in Iraq and electricity to parts of the Damascus region in Syria (Halevy and Yashar 2015). Activities such as the above are founded in the physical realm. However, the

[1] The question of Prisoners Of War (POWs) must surely fill the likes of Anonymous with dread. We have already seen that ISIS does not abide by the rules—certainly not Geneva Convention standards—in relation to management of prisoners and "enemy combatants." Having said this, an equal response by the hacktivists' were they to do so, would, of course, violate *Jus in Bello* and the question of reprisal action.

vulnerability vector for disruption and/or destruction is available via the cyber battle space. More precisely, physical reprisals may provoke additional cyber-triggered responses such as a Stuxnet-derived virus that disables the Supervisory Control and Data Acquisition (SCADA) system supporting these infrastructures (Matrosov et al 2010).

Known ISIS Cyber Capabilities

Outside of revenue sources, communications are considered by many to be critical infrastructure. The use of social media assists ISIS to spread its message and gain support and recruits (Klausen 2015 and Bakke 2014). Tens of thousands of foreign fighters are thought to have immigrated to ISIS strongholds; many have come to fight directly as a result of enablers like social media, Internet chats, and other online news and propaganda systems. This online recruitment has both reached and appealed to all demographics, irrespective of gender, status, and location (Taylor 2015). It has also delivered a strong and highly compelling message. As a result, many have gone and more will go (Wood 2015). In an effort to counter such foreign fighter flows, a number of Western countries have enacted legislation to make such activity illegal, and engaged in various programs to identify those who intend to travel, as well as those contemplating such, and stop both. The results have not been altogether effective (Sengupta 2014). Additionally, human rights advocates like Deputy Human Rights Watch director Andrea Prasow opine that such surveillance not only denies the very right to travel, but more importantly may promote a situation where citizens of a state might be "prosecuted for their thoughts and their beliefs, but not their actions" (Lynch 2014).

The use of cyber space by terrorist or extremist organizations for command and control activities, recruitment, and the dissemination of training materials is of on-going concern for state actors. This is especially true in that the nature of cyberspace makes efforts to limit and/or eliminate its use by such group exceedingly difficult. With violent non-state actors like ISIS openly using cyberspace to spread its ideology and activities, other non-state actors such as Anonymous have declared their intention to attack those actors anywhere they can be found in cyberspace. But just what are the capabilities for this battle —and can Anonymous really go "mano a mano" with ISIS in this sense?

When reviewing the reported hacking incidents by ISIS and its supporters, it appears that their capabilities are primarily in the areas of compromising password security for publically accessible accounts and any associated databases used to support them (Gorman 2015, Keys 2015 and AFP 2015). Other reported hacking consisted of webpage defacement and small-scale denial of service attacks against government websites (Akbar 2015). Finally, and more significantly, there are reports that ISIS has been deploying digital surveillance tools within its geographic domain. The use of keyloggers and IP sniffers at Internet cafes, and the creation of an email malware used in an attempt to reveal IP addresses have been reported (Scott-Railton and Hardy 2014, Stormark 2014). It is understood that the ISIS "religious morals" police force called

"*Hisba*" has been using such technologies to counter the use of the Internet's anonymity in protesting the on-going brutality (March and Revkin 2015).

To accomplish the above attacks requires only moderate computer expertise when combined with existing hacking tools available throughout the World Wide Web. On the basis of these reports, it would be easy to conclude that ISIS does not appear to have the required computer skills to pose a serious threat to those outside their geographic domain. However, given this base of knowledge and the resources to recruit and employ more sophisticated tools and people, one must not disregard the potential for ISIS to become a clear and present danger in cyberspace. There are many anarchists, mercenaries, and states with the skills needed to do great harm in cyberspace. Given the condition that their interests align or worse that their ideological foundations find common ground, the prospect of ISIS fully utilizing cyberspace to commit widespread harm is very real. Therefore, the outstanding prevailing issues would be:

- What is the learning curve for existing ISIS supporters in the cyber domain and how long would it be before their capacity to harm individuals and infrastructures reaches a tipping point?
- To what degree can ISIS leverage its occupied geography to identify and conscript those with cyber capabilities?
- What is the possibility that state actors provide training and support to further cyber conflict?

We agree that there is significant concern over ISIS' use of the Internet to disseminate its mission and promote global recruitment. More importantly, as it consolidates more and more of its regional position, it will have the ability to put resources into accelerating its cyber capabilities. This will likely result in the recruitment of cyber-savvy "foreign fighters" to provide the skills with which to launch large-scale distributed attacks on infrastructures throughout the world (Radio Free Europe/Radio Liberty 2015).

Anonymous Cyber Capabilities

Largely composed of users from numerous Internet forums and chat rooms, Anonymous is currently the most well-known "hactivist" group. Utilizing its "do-ocratic" membership approach to identify what it believes to be just causes, its members employ a wide-range of attacks on a wide range of targets, from official government websites to corporate email servers belonging to low-profile criminal organizations, high-profile groups, and individuals. Most research suggests that the group was first established in the mid-2000s, bringing together the first "hackers" of the 1980s with those of the twenty-first century generation (Singer and Friedman 2014, 83). Anonymous' anonymity and notoriety have also, paradoxically, increased its profile. The efforts of Anonymous since 2007 to right–wrongs and to bring misdeeds to light have evolved exponentially.

In August 2011, a group of local Mexican Anonymous hackers launched Operation PAPERSTORM, an effort to "out" those members of the local Veracruz government that the "hacktivists" knew were in collusion with the Los Zetas narco-traffickers. Following the murder of an internet blogger by Los Zetas in another Mexican state, Anonymous launched a DDOS attack against websites linked to the state government of Veracruz in protest of the "soft-response" from local officials, but also threatened to publish a vast archive of emails detailing the corrupt relationships between the cartel and various network partners online. In response, Los Zetas hired cyber-experts to help "reverse hack" Anonymous in order to identify some of its members. One such hacktivist was ultimately identified, kidnapped, and threatened with execution. This real Mexican "stand-off" was resolved when Anonymous agreed not to release the material, and in exchange, the kidnap victim was freed with an accompanying warning from Los Zetas that they would kill 10 people for every name Anonymous should subsequently chose to publicize (Singer and Friedman, 84–86 and Rexton Kan 2013, 40). Paul Rexton Kan, who wrote extensively of the exchange, described the stalemate as one of ". . . two clandestine non-state groups [who] stared each other down in the digital domain" (40). More importantly, he highlights the different benefits and values non-state actors see in the Internet and the information age:

> *The members of Anonymous see cyberspace as a type of commons that should be accessible to all.… Los Zetas, on the other hand, do not view cyberspace through an ideological lens but through an operational lens*

With the Anonymous–Los Zetas "stand-off" firmly in mind, we turn to the question of how vulnerable might Anonymous see itself—real or perceived—because of ISIS' very existence? Anonymous has a number of options that it might use in a nonviolent or nonkinetic manner, in order to defend the Anonymous "state". Anonymous published a "Declaration of War" because ISIS strikes at the very heart of what those in Anonymous believe in; that of freedom of expression and freedom of speech (Makuch 2014 and Chen 2014). While the conflict continues to progress and evolve, perhaps the real issues to be considered are as follows:

- Can Anonymous maintain this nonviolent approach (denial of service, release of information, etc.) and how far could they go?
- How effective could Anonymous be and is this the way forward?
- Should states embrace such action from nonviolent non-state actors, encourage such activity even, or is it opening up a "Pandora's box" of interpretations, debates on thresholds?
- What constitutes an "enemy," control of resources, or are we far too early into this "battle in the cyber domain" construct for us to get anywhere near beginning to understand what we are dealing with now?

Escalation Options: How Far Can Anonymous Go?

Largely as a result of the incident with Anonymous, Los Zetas embarked on a greater effort to increase their cyber capabilities by recruiting and coercing computer engineers and university students to assist with their cyber-crime efforts. This, combined with surveillance technology provided by Los Zetas' stable of government, law enforcement, and military co-optees and collaborators, enabled the group to counter the threat presented by Anonymous. Known for its ruthlessness, the cartel responded by carrying out actions that would ensure the Anonymous threat would not present itself ever again. The hacktivists backed down because to follow through with their actions was not worth the potential cost in lives. Singer and Friedman (118-126) suggest that this particular incident make us think about cyber-war theory, especially the limits of state actors in dampening or preventing such conflict from escalating. Rexton Kan (41-43) adds that cyber conflict presents a paradigm within the cyber-world and without the state. Both authors express concern about the evolving iteration of nontraditional actors in this far more asymmetric twenty-first century.

For example, in 2007, the Department of Homeland Security (DHS) put together a team of "hired hackers" and conducted an experiment to destroy a large generator via cyber-attack (East et al 2009, 67–81). Four years later, the experiment, known as the "Aurora Generator Test", was declassified and the impressive video footage released, showing how a cyber-attack could destroy a large diesel generator that was linked to a mock electricity grid. The attack, using a computer program to modify circuit breakers, was enough to see the generator self-destruct. Might the oil infrastructure that ISIS controls be vulnerable to such attacks—covert sabotage? And if the state, or state actors, for whatever reason be unable or unwilling to carry such activity, then might the likes of Anonymous be prepared to "step up to the plate?"

In early February 2015, a Five-Country Ministerial Communique was released after a meeting of top government ministers from the "Five-Eyes" nations of the United States, Great Britain, Canada, Australia, and New Zealand (Five-Country Ministerial Communiqué 2015). The single emphasis of the Communique concerned the shared efforts necessary to counter the threat from violent extremism. Ministers identified the need to develop proactive strategies to address these groups and their "use of . . . internet and social media platforms" and stressed the importance of a "sustained and aggressive approach" to counter such challenges.[2] The Ministers suggested that opportunities to work with commercial companies might achieve this end. Could we add other non-state actors to this new twenty-first century coalition?

History tells us that engagement like this has been done in the past and, in all likelihood, continues today. During the 1980s, as computers started to form connected networks, accessing such networks via clandestine means gave intelligence services an opportunity for further methods of penetration. An early example was the KGB-sponsored German hackers who penetrated several hundred computer systems connected to the U.S. Military's MILNET networks (Price 2014, 55). And it seems that state actors recruiting third-party experts or specialists in order to access, deny, and disrupt adversaries and national security threats have not changed. Investigations into the FBI's use of one of Anonymous' very own—Hector "Sabu" Monsegur, ultimately discovered that this informant and third-party hacker who had been working for the government since his arrest in 2011 was responsible for coordinating several hundred computer attacks and penetrations against Anonymous members themselves, as well

[2] Five-Country Ministerial Communiqué, released February 6, 2015.

as websites operated by the governments of Iran, Syria, Brazil, and Pakistan (Mazzetti 2014).[3]

In an opinion piece in ForeignPolicy.com in early March 2015, commentator Emerson Brooking (2015) suggested that the very people who should be charged with countering ISIS, "dispersed, rapidly regenerative online presence," should be digital natives themselves. Brooking considered that Anonymous was perfect for the job, and should be supported with resources to do so, including paying those individuals with the online currency "Bitcoin." He added "As a rule, hacktivists despise bullying, hypocrisy, and fundamentalism. The Islamic State couldn't present a clearer target." The prevailing concern is the means by which non-state actors such as Anonymous might be co-opted into serving national and international interests to do what state actors cannot or would not do. Coercion or monetary incentives are probably to go against the social tenets that Anonymous' member espouse and may have serious future sustainability consequences for the group. In an interview with a member of the Anonymous collective known as "Nix," who also provides legal support for those being prosecuted for hacking, the authors were told that "one of the main attractions to being a part of Anonymous is a sense of empowerment to right wrongs."[4] Having turncoats or hired guns greatly diminishes this sense of shared social activism. If we return to Anonymous' first principles, it is their unrelenting moral stance on issues and rights and its ability to disclose massive amounts of information on associations and activities that has propagated its renown. Thus, Nix added "In response to Anonymous' disclosures that directly benefit society, perhaps a Cyber Samaritan Law would benefit a nation state's efforts to limit wrongful prosecutions" (2015). Such a law would limit an activist's liability; allow government deniability; conserve judicial resources; and provide better targeted prosecutions. Could state actors embrace such a direction?

Conclusions

In his article, Brooking (2015) mentions that engaging in such activity, or sanctioning the recruitment of hacktivists like Anonymous, would challenge what we would consider to be the "international norms." But things have changed. Surely these rules are not necessarily applicable in the non-state actor realm? Can we embark on a new set of rules that takes us back before Westphalia, to the days when Indian strategic thinker Kautilya first introduced the "Mandala theory" of state security—"the enemy of my enemy is my friend"(Rangarajan 1992)? Rexton Kan concludes that the Anonymous versus Los Zetas "stand-off" was not anticipated and suggests that cyber-conflict and the future of cyber-warfare is only limited by the human imagination. At some stage, he adds, it is likely to transition from online embarrassment and discomfort, to off-line and real—death and destruction. Clearly should such novel methods be utilized by non-state actors, they must be met with equally creative policies and strategies from security agencies.

[3] Monsegur had been partly responsible for the penetration and theft of information belonging to the Texas-based Stratfor Global Intelligence provider. Interestingly, neither Monsegur, nor any of the Anonymous felons was charged with cyber-attacks on any of these foreign websites.

[4] Nix interview conducted with authors on April 12, 2015.

Whether we like it or not, non-state actors are now a part of a new and emerging battle space. Where the state's power was near absolute, cyberspace has enabled a means for non-state actors to effect change in the physical world. Because of this, non-state actors are increasingly becoming problematic to state actors unless their interests align. Perhaps this is precisely the reason why states might wish to task non-state groups with activities that allow a significant degree of deniability while furthering shared goals. So, what if the state were to sponsor such activities? Between the 1970s and 1990s we saw the concept of state-sponsored terrorism—could the same apply in a state-sponsored cyber-sense? What we are seeing today might be a way in which Superpowers use non-state actors to carry out operations against each other—deniability, clandestine or covert operations—if they are not doing so already. In its targeting of ISIS' cyber presence, what would be the outcome if Anonymous were to become more robust and aggressive, and have an element of "deniable protection" from a supporting state actor in its cyber activities? Providing incentives for aligning interests is something worthy of further examination but we must also consider the fallout such actions may bring as well.

There is a likely but unknown degree of escalation in this battle space that is about to emerge, and creative policies and strategies should be the carefully developed to mitigate unexpected outcomes. To this we add that there must be "bold" and "novel" approaches to addressing the threat that other non-state actors might make in these cyber-conflicts. But there are some limitations, or tolerances, to this aggressive, pro-active imagination that must be considered, and these challenges to existing legal, ethical, and moral practices within the security space must be equally considered now. In the words of former British intelligence "Mandarin" Sir David Omand "providing for public security is an exercise in risk management, not risk elimination" (Omand 2010, 250). We believe that the paradigm of state actor reliance for self-defense is one that is already evolving into another form, and as such, the time for considering the role of non-state actors in self-defense is upon us.

References

AFP. 2015. "French TV Channel Restarts Full Operations After 'Unprecedented' ISIS Hack." *The Straits Times*, April 10.

Akbar, Jay. 2015. "'Death to France. Death to Charlie': Pro-ISIS Hackers Launched 'Unprecedented' Wave of Cyber-Attacks on 19,000 French Websites." *MailOnline*, January 15.

Akyol, Mustafa. 2014. "The Truth About Turkey and Islamic State Oil." Al Monitor, September 22.

Anonymous. 2014. "How Anonymous Hackers Changed the World." [Video file], May 29. https://www.youtube.com/watch?v=Q6o7lEKloJc (accessed March 29, 2015).

Bakke, Kristin. 2014. "Help Wanted? The Mixed Record of Foreign Fighters in Domestic Insurgencies." *International Security* 38 (4): 150–187.

Brooking, Emerson. 2015. "The U.S. Government Should Pay Anonymous in Bitcoin to Fight ISIS." *ForeignPolicy.com*, March 3.

Chen, Adrian. 2014. "Anonymous No More: The Celebrated Hackers Represent the Worst of Techno-Utopianism." *The Nation*, December 1/8.

Crompton, Paul. 2014. "Sales of Black Market Oil Surge in Middle East." *Al Arabiya News*, July 29.

Dipert, Randall. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics* 9 (4): 384–410.

Dodge, Toby. 2014. "Can Iraq Be Saved?" *Survival: Global Politics and Strategy* 56 (5): 7–20.

East, Samuel, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. 2009. "A Taxonomy of Attacks on the DNP3 Protocol." In *Critical Infrastructure Protection III*: 67– 81

Giglio, Mike. 2014. "This is How ISIS Smuggles Oil." *BuzzFeed News*, November 4.

Gorman, Ryan. 2015. "Alleged ISIS Cyber Terrorists Infiltrate Media Twitter Accounts, Post Sensitive Information and Documents." *Aol.com*, January 6.

Hager, Emily B. 2014. "ISIS' Dark Oil Trade." *New York Times*, December 1.

Halevy, Dalit and Ari Yashar. 2015. "ISIS's War of Water and Electricity." *Israel National News* February 18.

Hawramy, Fazel, Mohammed Shalaw, and Luke Harding. 2014. "Inside Islamic State's Oil Empire: How Captured Oilfields Fuel Isis Insurgency." *The Guardian*, November 19.

Keys, Matthew. 2015. "Exclusive: 'Cyber Caliphate' Unmasked as Lone Algerian Hacker." *The Desk, Journalism and Social Media by Matthew Keys*, February 10.

Klausen, Jytte. 2015. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38 (1): 1–22.

Lynch, Colum. 2014. "The Islamic State Makes Electronic Surveillance Respectable Again." *ForeignPolicy.com*, September 24.

Makuch, Ben. 2014. “Anonymous-Affiliated Hackers Have Declared War on the Islamic State.” *Motherboard.vice.com*, June 30.

March, Andrew F. and Mara Revkin. 2015. “Caliphate of Law: ISIS’ Ground Rules.” *Foreign Affairs*, April 15.

Matrosov, Aleksandr, Eugene Rodionov, David Harley, and Juraj Malcho. 2010. “Stuxnet Under the Microscope.” *ESET Internet Security* LLC, September. https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

Mazzetti, Mark. 2014. “F.B.I. Informant Is Tied to Cyberattacks Abroad.” *New York Times*, April 23.

New Zealand Government. 2015. *Five-Country Ministerial Communiqué*. February 6.

Omand, Sir David. 2010. *Securing the State*. London: Hurst.

Orend, Brian. 2008. “War.” In Edward N. Zalta, eds, *The Stanford Encyclopedia of Philosophy* (Fall 2008 Edition). http://plato.stanford.edu/entries/war/

Posner, Eric A. and Alan O. Sykes. 2004. “Optimal War and Jus Ad Bellum.” *U Chicago Law & Economics, Olin Working Paper No. 211*.

Price, Douglas R. 2014. “Guide to Cyber-Intelligence.” *The Intelligencer, Journal of U.S. Intelligence Studies* 21 (1) (Winter 2014–2015): 55-60.

Radio Free Europe/Radio Liberty. 2015. “Foreign Fighters in Iraq and Syria.” *Radio Free Europe/Radio Liberty*, January 29.

Rangarajan, L.N. 1992. *Kautilya: The Arthashastra*. New Delhi: Penguin Books.

Rexton Kan, Paul. 2013. “Cyberwar in the Underworld: Anonymous Versus Los Zetas in Mexico.” *Yale Journal of International Affairs* 8 (1) (Winter 2013): 40-51.

Ruus, Kertu. 2008. “Cyber War I: Estonia Attacked from Russia.” *European Affairs 9 (1-2)* (2008). Columbia International Affairs Online.

Scott-Railton, John and Seth Hardy. 2014. “Malware Attacks Targeting Syrian ISIS Critics.” *The CitizenLab*, University of Toronto, Munk School of Global Affairs, December 18. https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/.

Sengupta, Somini. 2014. “Nations Trying to Stop Their Citizens from Going to Middle East to Fight for ISIS.” *New York Times*, September 12.

Singel, Ryan. 2010. “White House Cyber Czar: ‘There Is No Cyberwar.’” *Wired Magazine*, March 4.

Singer, P.W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Snyder, Stephen. 2014. “ISIS is Selling Cheap Oil to its Enemies — From Syria’s Government to the Kurds.” *Pri News*, September 16. Stormark, Kjetil. 2014. “Hunt for America’s Spies.” *Hate Speech International*, December 1.

Sullivan, Paul. 2014. “The Energy-Insurgency Revolution Nexus: An Introduction to Issues and Policy Options.” *Journal of International Affairs* 68 (1) (Fall/Winter 2014): 117-148.

Taylor, Adam. 2015. “Gun-toting Women Sell Jihadist Recruitment Message.” *Washington Post*, March 28.

United States National Intelligence Council (DNI). 2008. *Global Trends 2025: A Transformed World*. Washington DC: National Intelligence Council.

Valeriano, Brandon and Ryan Maness. 2012. “The Fog of Cyberwar; Why the Threat Doesn’t Live Up to the Hype.” *Foreign Affairs*, November 21.

Whaley, Barton. 1969. *Stratagem: Deception and Surprise in War*. Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology.

Wisniewski, Chester. 2013. “Comment: There’s No Such Thing as Cyber War.” *Infosecurity Magazine*, August 1.

Wood, Graeme. 2015. “What ISIS Really Wants.” *The Atlantic*, March.