Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts

Ralph Martins

ABSTRACT

Warfare in the physical world, both asymmetrical and conventional, has occurred throughout history. However, war in cyberspace is a more recent phenomenon, and there is still much to be explored and understood. Because cyberspace is inherently asymmetric, many lessons learned from asymmetric warfare in the physical world also apply to cyber conflicts. This article will examine the online battle waged by Anonymous against ISIS and analyze five asymmetrical characteristics of cyber conflicts: the vulnerability of conventionally-powerful actors to attacks from relatively weaker adversaries, the unconventional nature of offensive tactics, the low level of intensity of those tactics, the ability of actors to organize and aggressively operate in an extremely decentralized manner, and the strategic goal of breaking willpower or forcing a change of policy. Understanding the asymmetrical nature of cyber conflicts and applying appropriate lessons learned will lead to a more effective defensive posture against cyber-aggressors and facilitate a more secure operating environment in cyberspace.

INTRODUCTION

War in cyberspace is a recent phenomenon, as the first computer networks were implemented only in the mid-20th century. In early 2015, the world for the first time witnessed a public declaration of war by a non-state actor that operates almost exclusively in cyberspace—the collective known as Anonymous—as they openly challenged the Islamic State and their online resources and operations. This conflict has waged on into 2017 [1], and it serves to highlight the many similarities between asymmetrical conflicts in the physical world and conflicts carried out solely online. As a result, many lessons learned from fighting kinetic wars against asymmetrical foes also apply to the fight against non-state actors in cyberspace. This article will examine this battle

Ralph Martins has over twenty-one years of professional experience as a management consultant and a United States Marine leading teams in the cyber security, cyber warfare and intelligence fields. As a consultant, he has served clients in the Department of Defense and Intelligence Community, and as a Marine, has served in Iraq, Africa, and Cuba, among other locations. He holds graduate degrees in Engineering Management and Military Studies from George Washington University and American Military University respectively and is currently pursuing graduate studies in International Relations at Harvard University. He maintains a number of professional certifications including the Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), and Project Management Professional (PMP).

and analyze the five asymmetrical characteristics of cyber conflicts that make cyberspace an inherently friendly environment for asymmetrical conflicts.

Who Are Anonymous? Why Do They Matter?

Anonymous is a hacktivist collective,[2] a network of loosely affiliated individuals, groups and other entities with little to no structure, organization or membership requirements that attacks targets in cyberspace and is motivated by various causes often related to freedom of information and human rights. Historically, Anonymous' favorite targets can be categorized as the "big three": big business, big government, and big religious organizations.[3] Anonymous describes itself as having "a very loose and decentralized command structure that operates on ideas rather than directives."[4] Major Anonymous operations are typically driven and guided by a very small group of core members relying on their ability to convince other potential supporters of the worthiness of the proposed cause—a process that has historically caused internal friction and disagreement.[5]

Anonymous' most common online tactics include website defacements, distributed denial-of-service (DDoS) attacks, unauthorized account access, and data exfiltration. To execute DDoS attacks, Anonymous members use publicly available tools such as Gigaloader, JMeter, Low-Orbit Ion Cannon (LOIC), and botnets.[6] Their tactics are frequently illegal and often cause damage to their targets. As one expert notes,

> "...downtime that lasts for hours or days can cost companies thousands in lost revenue or extra bandwidth cost. Participating in a DDoS attack is also illegal, breaking the Computer Fraud and Abuse Act in the United States as well as the 2006 Police

> and Justice Act in the United Kingdom; in both countries, perpetrators face a maximum penalty of ten years in prison." [7]

While DDoS attacks and the defacement of websites require precious resources (such as time and money) to restore networks, systems, and data to their original state, the more important result is the attention drawn by such attacks. This is where Anonymous makes its most significant impact. The group influences public opinion and government policies by training the proverbial spotlight on its chosen issues through the use of cyberattacks. As an example, Anonymous took on the repressive regime of Tunisian President Zine El Abidine Ben Ali in January of 2011 via the use of DDoS attacks, website defacement, the sharing of cybertools with dissidents, and facilitating the flow of information into and out of the country in support of the rebels. [8] Shortly after Anonymous initiated its online involvement, Ben Ali dissolved his government and fled to Saudi Arabia. However, around the same time that Ali's regime was collapsing, the Islamic State was beginning to actively and aggressively oppose the fledgling Iraqi democracy, terrorize Iraqi citizens and spreading its violence to neighboring Syria.

The Rise of ISIS

The Islamic State in Iraq and Syria (ISIS), also known as ISIL, Daesh or simply the Islamic State, is a Sunni militant group attempting to create a worldwide caliphate. [9] ISIS can trace its beginnings to 1999, when a Jordanian militant named Abu Musab al-Zarqawi, who had previously met and been influenced by Osama bin Laden, formed a group called Jamā'at al-Tawhīd wa-al-Jihād (The Organization of Monotheism and Jihad). In 2004, Zarqawi renamed the group Tanzīm Qā'idat al-Jihād fī Bilād al-Rāfidayn, although it was known as al-Qaeda in Iraq. [10] The group merged with several other similar organizations over time and went through two significant leadership changes. Zarqawi and several subsequent leaders were killed by US and coalition action, and in 2010, Abu Bakr al-Baghdadi assumed command. Baghdadi leads an organization that, in the opinion of one expert, "has exploited these technologies more successfully than any of its contemporaries in the Islamist world." [11]

Throughout its history, ISIS has proven to be especially adept at leveraging cyberspace and, more specifically, social media in order to conduct the full lifecycle of terrorist operations. [12] Through their online operations, ISIS operatives recruit members, issue operational instructions, disseminate propaganda, and, more directly related to their ultimate goal, provoke fear in an attempt to change the behavior and policy of their targets. [13] As one defense analyst notes,

> Although the overarching message is fear, the Islamic State's propaganda machine has two distinct functions. In the jihadist organization's aggressive territorial expansion, its social media postings have served a role once filled by leaflets air-dropped ahead of invading armies, sowing terror, disunion, and defection. Meanwhile, its messaging to the wider global community, however gruesome to many

> viewers, serves largely to bind the militants of the Islamic State more tightly together—and rally more sympathetic Westerners to its cause. Both these functions rely almost exclusively on media platforms that were nonexistent a decade ago. [14]

ISIS has effectively incorporated online resources into almost every facet of what it does. However, just as cyberspace provides ISIS with a highly effective conduit for operation, it also provides opportunities for opponents to counter these efforts.

What Is Asymmetrical Warfare?

Asymmetrical warfare is a conflict between actors whose military capabilities and power are so unevenly matched that the weaker side must resort to low-intensity, indirect and unconventional tactics and strategies to oppose its stronger opponent(s). However, weaker belligerents in an asymmetrical war do not typically seek the total eradication of their opponents, as is often the goal for conventional belligerents. Instead, the objective of the weaker power—often a revolutionary movement, insurgency, terrorist group or other resistance effort—can range from forcing a change in policy to completely wresting away political power from a government. Recent examples of asymmetrical battles include Al Shabaab's struggle against the Somalian government, the Kurdish fight for autonomy against several Middle Eastern nations and the ongoing conflict between Hezbollah and Israel. ISIS's fight against Iraq and Syria is another example of an asymmetrical war.

Upon analysis, it is possible to identify trends and common characteristics of asymmetrical battles in the physical world that differentiate them from conventional wars. Five of the more significant features of these conflicts are: the imbalance of power between belligerents, the reliance of asymmetrical forces on unconventional tactics, the relatively low intensity of these unconventional tactics, the decentralized nature of asymmetrical forces, and the asymmetric force's ultimate goal of breaking its enemies' strategic willpower in order to bring about the change in policy or collapse of an entire government. These elements can be further described as follows:

Imbalance of power: The catalyst for asymmetrical warfare is the clash of two unevenly matched adversaries. The entity with more conventional power–often (but not necessarily) a nation-state–typically maintains a significantly more potent conventional military capability and has access to greater resources and more advanced technology than the weaker force. It is this imbalance of power that compels the weaker force to leverage unconventional tactics to have any chance of opposing the stronger power. Specifically, when an adversary is significantly more powerful to the degree that a conventional battle would be a futile effort, unconventional tactics become necessary.

Unconventional tactics: Unconventional tactics are those that diverge from traditional, standard, direct combat operations. On a traditional battlefield, they include covert action, hit-and-runs, ambushes, subversion, harassment, and the

heavy use of improvised weapons and explosives. This type of combat often requires the ability to blend into an indigenous population so fighters can operate clandestinely and wait for opportune times to strike. Unconventional tactics require fighters to utilize creativity, flexibility, adaptability, extreme mobility, deception, and patience. Unconventional weapons are often cheap, easy to improvise and require less formal training than conventional weapons.

Low intensity: By relying on unconventional tactics, an asymmetrical force, by definition, chooses to forego the use of more conventional and potent tactics, as using these tactics against a conventionally stronger enemy would be unlikely to result in victory. Instead of attempting to precipitate mass casualties and destruction and ultimately land a killing blow, an asymmetrical force aims to wear down the stronger adversary with smaller attacks, often more frequent but lower in intensity.

Decentralization: Asymmetrical forces in the physical world do not have a traditional hierarchical shape in their organizational structures. They are composed of networks of individuals and smaller cells with varying degrees of connectivity to each other. These networks are, by their very nature, resilient and difficult to destroy. And while cells can be eliminated, they can also be easily reconstituted. Each cell is self-sufficient, and destroying the greater organization's leadership does not necessarily render the components (individuals and cells) of that network incapable of operating.

Breaking strategic willpower: Unlike in conventional war, the goal of an asymmetrical force is not the total destruction of its enemy's forces or even the significant degrading of its enemy's ability to fight. Instead, unconventional fighters are often employed as part of a long-term plan to achieve submission, capitulation or retreat by breaking the will of the enemy on a strategic level. It is the willpower of leadership that is the real target of the asymmetrical fighter.

Anonymous and Its Online War on ISIS

Anonymous has been waging an online war against ISIS since 2015—a conflict that demonstrates the asymmetrical nature of cyberspace. This war began with a violent attack in the physical world by a related group. In January 2015, members of Al Qaeda in the Arabian Peninsula (AQAP) carried out several attacks within the city of Paris, highlighted by the shooting at the *Charlie Hebdo* newspaper office.[15] Anonymous responded to these attacks by launching Operation Charlie Hebdo, promising a "massive" response in retribution and immediately taking down a French extremist website.[16] Shortly thereafter, Anonymous expanded its attacks to other related militant targets in cyberspace as it initiated Operation ISIS and took down 1,500 ISIS-associated Twitter and Facebook accounts, claiming, "From now on, there [will be] no safe place for you online—you will

be treated like a virus, and we are the cure. We own the internet now." [17] Following the November 2015 ISIS attacks in and around Paris that killed 130 people, Anonymous again declared a new war on ISIS and announced Operation Paris to "defend our values and our freedom." [18] One member of Anonymous summarized the organization's perspective on ISIS as follows: "We believe that [sic] all of us combined, we can show the world that ISIS does not have as much power as it claims it does and show the world that if ordinary people can fight ISIS [successfully] then the governments of the world certainly can." The member continued, "ISIS is a plague on the internet and humanity." [19] While Anonymous' war against ISIS has had its struggles and some members have claimed to have given up the battle, [20] for many supporters it will continue for the foreseeable future. [21]

An analysis of Anonymous' online conflict with ISIS exhibits the five characteristics of traditional asymmetrical forces enumerated earlier. First, Anonymous is taking on an adversary that is clearly stronger regarding conventional power and has access to greater resources. ISIS brought in $2 billion in 2014 [22] causing it to be labeled the world's "richest terror group" [23] and the "best financially endowed terrorist organization in history." [24] Anonymous, on the other hand, has no meaningful budget. Instead, it relies on occasional donations [25] and largely operates by crowdsourcing volunteers of various skill levels to participate in its operations on an ad-hoc basis. [26] Despite this apparent limitation, Anonymous has demonstrated hacking capabilities to such a degree of sophistication that its ability to confront ISIS online is highly regarded and some experts even consider Anonymous to be a serious challenge to ISIS's online operations. [27] This aspect of the conflict, in particular, demonstrates that cyberspace can be "a great equalizer." [28]

Second, Anonymous has a highly decentralized presence and leverages the talents of its members from around the world in its online fight against ISIS. The organization has been described as an "online global brain of community users" [29] and a "decentralized online community of users" [30] who expend effort "promoting collaborative global hacktivism" [31] and who are "based around the world and hail from every walk of life." [32] However Anonymous might be characterized, it lacks the well-defined organizational structure that would be expected in other groups of similar size. Nowhere is this more evident than in the fight against ISIS. As one think tank researcher describes it:

> Like most hacktivist groups, #OpISIS is ostensibly flat and leaderless, though day-to-day operations are sustained by a few dozen long-serving members who form the concrete core of the movement. In turn, they guide the efforts of hundreds of volunteers. Fragmentary groups tend to focus on different things (taking down websites, tagging Twitter accounts, locating propaganda videos, infiltrating jihadi forums), their roles converging and diverging at random. The result is organic and more than a little chaotic. But it works. [33]

Anonymous leverages cyber-attacks conducted by individuals and teams spread across the globe,[34] and although collaboration occurs, few, if any, of the participants launching the attacks are physically collocated, and most do not know each other.[35]

Third, the online tactics, techniques and procedures used by Anonymous against ISIS fit the definition of unconventional. Anonymous has used online mockery,[36] disruption of communications,[37] counter-propaganda efforts,[38] and disruption of finance[39] to thwart ISIS operations and try "to shut down their ability to talk to the public."[40] Furthermore, online attacks are in themselves unconventional in that attack skills are simple and inexpensive to acquire. This is made evident by the fact that hackers-for-hire are relatively cheap[41] and, despite Anonymous' lack of an operational budget, some of its most elite members have executed "devastating" attacks on high-profile targets are self-taught.[42]

Fourth, the online conflict between Anonymous and ISIS is low-intensity, and Anonymous is making use of tactics that are intended to wear down support for ISIS and its effectiveness over time.[43] Nothing Anonymous has done or can do online (DDoS, website defacements, propaganda dissemination) will likely result in the death of ISIS members or large-scale physical destruction of their resources. This is simply due to the constraints of cyberspace—the inability to create kinetic effects (kill people or break things) via online attacks. All of this means that there will likely not be any powerful or decisive blow, but rather a continuous series of many small, disruptive attacks.

Fifth, because Anonymous knows it cannot destroy ISIS through cyberspace, it instead seeks to contribute to the effort to break its willpower by restricting its operations and eroding its capabilities. Twitter is an effective tool for ISIS propaganda,[44] and an Anonymous-affiliated group has claimed responsibility for shutting down over 70,000 ISIS Twitter accounts.[45] In November of 2015, Foreign Policy noted that Anonymous and its cohorts "claim to have dismantled some 149 Islamic State-linked websites and flagged roughly 101,000 Twitter accounts and 5,900 propaganda videos" and then described Anonymous as postured to combat ISIS via the Twitter "town square" and the depths of the deep web.[46]

The Asymmetrical Nature of Cyberspace

Perhaps similar to Billy Mitchell's struggle to convince and educate his contemporaries about the potential application of air power in the early 20th century, there is a learning curve to climb in understanding and institutionalizing the knowledge about the operations of cyber actors and the inherent nature of online combat. It stands to reason that as everything from military weapon systems to everyday objects in our lives are increasingly interconnected and reliant on information systems, vulnerabilities and available attack vectors will increase accordingly and therefore so will the frequency and effects of attacks. Anyone who wishes to assert power and influence in the modern, globalized world must recognize and prepare for this obvious trend.

However, cyberspace is more than just a new warfighting domain that will be increasingly conducive to conflict over time. Its makeup is such that it is inherently asymmetrical, as exhibited in the online skirmish between Anonymous and ISIS, and this characteristic is a critical point in understanding the cyberwars of the future. Cyberspace is designed so that actors with relatively little conventional power can impose meaningful effects on significantly more powerful adversaries. Analyst John Arquilla once noted that "The destructive and disruptive power of small groups and even individuals—in the physical world as well as in cyberspace—just keeps growing." [47] Scholar P.W. Singer recently noted, "Today, it is the United States that has the conventional edge on its adversaries, and thus many of its attackers see cyberattacks as their asymmetric way to work around a power imbalance." [48]

The same highly interconnected architecture of the Internet that allows billions of people around the world to communicate instantaneously also allows for a planet full of potential attackers, making extreme geographic decentralization a standard feature of cyber armies. Hostile actions in cyberspace are also unconventional in nature, as described by retired Army General Wesley Clark: "There is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril." [49] But while online attacks are quick, frequent and can be persistent, they are also as yet unable to replicate the kinetic effects of combat in the physical world. With few rare exceptions, such as the tangibly destructive power of Stuxnet, [50] virtually all conflicts in cyberspace are of low intensity and will, therefore, require a protracted, persistent and committed effort to degrade capabilities and erode willpower over time. By recognizing all these asymmetrical features of cyber warfare, it will become easier to develop strategies to counteract and mitigate threats in cyberspace.

NOTES

1. Chris Summers, "Hacker accesses ISIS's radio channel and taunts Abu Bakr al-Baghdadi by saying: 'Mosul will be liberated'", January 13, 2017, http://www.dailymail.co.uk/news/article-4116338/Hacker-accesses-ISIS-s-radio-channel-taunts-Abu-Bakr-al-Baghdadi-saying-Mosul-liberated.html.

2. The term hacktivist, a portmanteau of hacker and activist, has been credited by some to the former hacker group Cult of the Dead Cow. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* New York: Oxford University Press, 2014, 77.

3. Quinn Norton, "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down," Wired, July 3, 2012, http://www.wired.com/2012/07/ff_anonymous/.

4. ANON OPS: A Press Release, ANONNEWS, December 10, 2010, http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf.

5. Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulSec, Anonymous and the Global Cyber Insurgency,* New York: Little, Brown and Company, 2012, 92 – 99.

6. bid., 74.

7. bid., 64.

8. Quinn Norton, "2011: The Year Anonymous Took On Cops, Dictators and Existential Dread," *Wired,* January 11, 2012, http://www.wired.com/2012/01/anonymous-dicators-existential-dread/.

9. Matt Bradley, "ISIS Declares New Islamist Caliphate: Militant Group Declares Statehood, Demands Allegiance From Other Organizations," *The Wall Street Journal,* June 29, 2014, http://www.wsj.com/articles/isis-declares-new-islamist-caliphate-1404065263.

10. Lawrence Joffe, "Abu Musab al-Zarqawi obituary," *The Guardian,* June 8, 2006, http://www.theguardian.com/news/2006/jun/09/guardianobituaries.alqaida.

11. Hisham Melhem, "Keeping Up With the Caliphate: An Islamic State for the Internet Age," *Foreign Affairs,* November/December 2015, https://www.foreignaffairs.com/reviews/keeping-caliphate.

12. Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied Media," *New York Times,* August 30, 2014, http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html.

13. Faisal Irshaid, "How Isis is spreading its message online," *BBC News,* June 19, 2014, http://www.bbc.com/news/world-middle-east-27912569; M.L. Nestel, Gilad Shiloach and Amit Weiss, "ISIS Forums Share Pipe Bomb Instructions for Attacks on NYC, Las Vegas," *Vocativ,* September 16, 2014, http://www.vocativ.com/world/isis-2/isis-pipe-bomb-attack-america/; Shiv Malik et al, "Isis in duel with Twitter and YouTube to spread extremist propaganda," *The Guardian,* September 24, 2014, http://www.theguardian.com/world/2014/sep/24/isis-twitter-youtube-message-social-media-jihadi; "Flames of War - AMAZING battle footage," LiveLeak video, 55:14, posted by "KIWalid," September 20, 2014, http://www.liveleak.com/view?i=5c2_1411222393.

14. Emerson Brooking, "The ISIS Propaganda Machine Is Horrifying and Effective. How Does It Work?," *Defense in Depth* (blog), Council on Foreign Relations, August 21, 2014, http://blogs.cfr.org/davidson/2014/08/21/the-isis-propaganda-machine-is-horrifying-and-effective-how-does-it-work/.

15. "Charlie Hebdo Attack: Three Days of Terror," *BBC News,* January 14, 2015, http://www.bbc.com/news/world-europe-30708237.

16. "Anonymous - #OpCharlieHebdo" YouTube video, 2:58, posted by "Anonymous France," https://www.youtube.com/watch?v=oqbwqmb8P00, accessed September 25, 2016; Guest, Untitled, Pastebin, http://pastebin.com/Pdj2Z0wC, accessed October 24, 2016; Rose Troup Buchanan, "#OpCharlieHebdo: Anonymous Take Down French Extremist Website After Threatening 'Retribution' for Charlie Hebdo Attacks," *The Independent,* January 12, 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/opcharliehebdo-anonymous-take-down-french-extremist-website-after-threatening-retribution-for-9972013.html.

NOTES

17. Wang Wei, "Hacktivist Group Anonymous (#OpISIS) Takes Down Islamic State (ISIS) Social Media Accounts," *The Hacker News,* February 8, 2015, http://thehackernews.com/2015/02/anonymous-isis-cyber-attack.html; Rick Gladstone, "Activist Links More Than 26,000 Twitter Accounts to ISIS," *New York Times,* March 31, 2015, http://www.nytimes.com/2015/04/01/world/middleeast/activist-links-more-than-26000-twitter-accounts-to-isis.html?mtrref=undefined&mtrref=www.nytimes.com&_r=0; Andrew Griffin, "Paris Attacks: Anonymous Vows to Avenge Charlie Hebdo Shootings with Cyberattacks on Islamist Websites," *The Independent,* January 9, 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-vows-to-avenge-charlie-hebdo-shootings-with-cyberattacks-on-islamist-9968813.html; Guest, #OpISIS- Twitter/Facebook, *Pastebin.*

18. Keely Lockhart and Myles Burke, "#OpISIS: Why Anonymous has declared an online war against Isil - in 90 seconds," *The Telegraph,* December 11, 2015, http://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-Why-Anonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html.

19. E.T. Brooking, "Anonymous vs. the Islamic State," *Foreign Policy,* November 13, 2015, http://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/.

20. Russell Brandon, "The Anonymous 'War on ISIS' Is Already Falling Apart," *The Verge,* November 23, 2015, http://www.theverge.com/2015/11/23/9782330/anonymous-war-on-isis-hacktivism-terrorism; Jesse Hirsch, "After Orlando, Anonymous Vows To Leave ISIS Alone," Good, June 14, 2016, https://www.good.is/articles/anonymous-says-peace.

21. Simon Parkin, "Operation Troll ISIS: Inside Anonymous' War to Take Down Daesh," *Wired,* October 6, 2016, http://www.wired.co.uk/article/anonymous-war-to-undermine-daesh.

22. Jose Pagliery, "Inside the $2 Billion ISIS War Machine," *CNN Money,* December 11, 2015, http://money.cnn.com/2015/12/06/news/isis-funding/.

23. Jack Moore, "Mosul Seized: Jihadis Loot $429m from City's Central Bank to Make Isis World's Richest Terror Force," *International Business Times,* June 11, 2014, http://www.ibtimes.co.uk/mosul-seized-jihadis-loot-429m-citys-central-bank-make-isis-worlds-richest-terror-force-1452190.

24. Pagliery, "Inside the $2 billion ISIS war machine."

25. Anthony Cuthbertson, "Operation Isis: Ghostsec Hackers Launch Crowdfunding Campaign in Fight Against Islamic State," *International Business Times,* July 29, 2015, http://www.ibtimes.co.uk/operation-isis-ghostsec-hackers-launch-crowdfunding-campaign-fight-against-islamic-state-1513104.

26. Anthony Cuthbertson, "Anonymous #OpParis: Hacktivists Publish 'Noob's Guide' for Fighting Isis Online," *International Business Times,* November 17, 2015, http://www.ibtimes.co.uk/anonymous-opparis-hacktivists-publish-noobs-guide-fighting-isis-online-1529173.

27. Ari Levy and Anita Balakrishnan, "What can Anonymous really do to ISIS?," *CNBC,* November 18, 2015, http://www.cnbc.com/2015/11/18/what-can-anonymous-really-do-to-isis.html; Evan Schuman, "Anonymous Just Might Make All the Difference in Attacking ISIS," Computerworld, November 16, 2015, http://www.computerworld.com/article/3005475/cyberattacks/anonymous-just-might-make-all-the-difference-in-attacking-isis.html.

28. Mary Louise Kelly, "ISIS Uses Cyber Capabilities To Attack The U.S. Online," *NPR,* April 25, 2016, http://www.npr.org/2016/04/25/475631277/isis-uses-cyber-capabilities-to-attack-the-u-s-online.

29. "Anonymous definition," *Technopedia,* https://www.techopedia.com/definition/27213/anonymous-hacking, accessed October 24, 2016.

30. Ibid.

31. Ibid.

32. Brooking, "Anonymous vs. the Islamic State."

33. Ibid.

34. Ibid.

35. Rick Gladstone, "Behind a Veil of Anonymity, Online Vigilantes Battle the Islamic State," *New York Times,* March 25, 2015, http://www.nytimes.com/2015/03/25/world/middleeast/behind-a-veil-of-anonymity-online-vigilantes-battle-the-islamic-state.html.

NOTES

36. Jasper Hamill, "Anonymous' Four Weirdest Tactics in ISIS Cyber-War: Here's How Hacktivists Are Undermining the Extremists," *The Mirror,* November 19, 2015, http://www.mirror.co.uk/news/technology-science/technology/anonymous-four-weirdest-tactics-isis-6859278.

37. John Shammas, "Anonymous Hacker Reveals How They Will Destroy ISIS and Its Ability to Carry Out Terror Attacks," *The Mirror,* December 1, 2015, http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-6931331.

38. Chris Smith, "Hackers vs. Terrorists: How Anonymous Wants to Beat ISIS, *BGR,* November 30, 2015, http://bgr.com/2015/11/30/anonymous-hackers-isis-terrorists-war/.

39. Hamill, "Anonymous' Four Weirdest Tactics."

40. Callum Borchers, "Operation ISIS: Anonymous Member Discusses How Group Is Waging War on Militant Group," *The Independent,* November 28, 2015, http://www.independent.co.uk/life-style/gadgets-and-tech/news/operation-isis-anonymous-member-reveals-how-they-are-waging-war-on-the-militant-group-a6752831.html.

41. Cale Guthrie Weissman, "9 Things You Can Hire a Hacker to Do and How Much It Will (Generally) Cost," *Business Insider,* May 8, 2015, http://www.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5.

42. Josh Halliday, "Lulzsec Mastermind Sabu: An Elite Hacker and Star FBI Informant," *The Guardian,* March 6, 2012, https://www.theguardian.com/technology/2012/mar/06/lulzsec-mastermind-sabu-hacker-fbi-informant.

43. Hamill, "Anonymous' Four Weirdest Tactics."

44. Brooking, "The ISIS Propaganda Machine Is Horrifying and Effective."

45. CtrlSec, Twitter post, November 13, 2015, 5:10 AM, https://twitter.com/CtrlSec/status/665109376684961792.

46. Brooking, "Anonymous vs. the Islamic State."

47. John Arquilla, "Beware the Few," *Foreign Policy,* April 16, 2013, http://foreignpolicy.com/2013/04/16/beware-the-few/.

48. P. W. Singer, "How the United States Can Win the Cyberwar of the Future," *Foreign Policy,* December 18, 2015, http://foreignpolicy.com/2015/12/18/how-the-united-states-can-win-the-cyberwar-of-the-future-deterrence-theory-security/.

49. Wesley K. Clark and Peter L. Levin, "Securing the Information Highway," *Foreign Affairs,* November/December 2009, https://www.foreignaffairs.com/articles/united-states/2009-11-01/securing-information-highway.

50. Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *Washington Post,* February 16, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html; Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired,* January 8, 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/; Mark Thompson, "Iranian Cyber Attack on New York Dam Shows Future of War," *Time,* March 24, 2016, http://time.com/4270728/iran-cyber-attack-dam-fbi/.