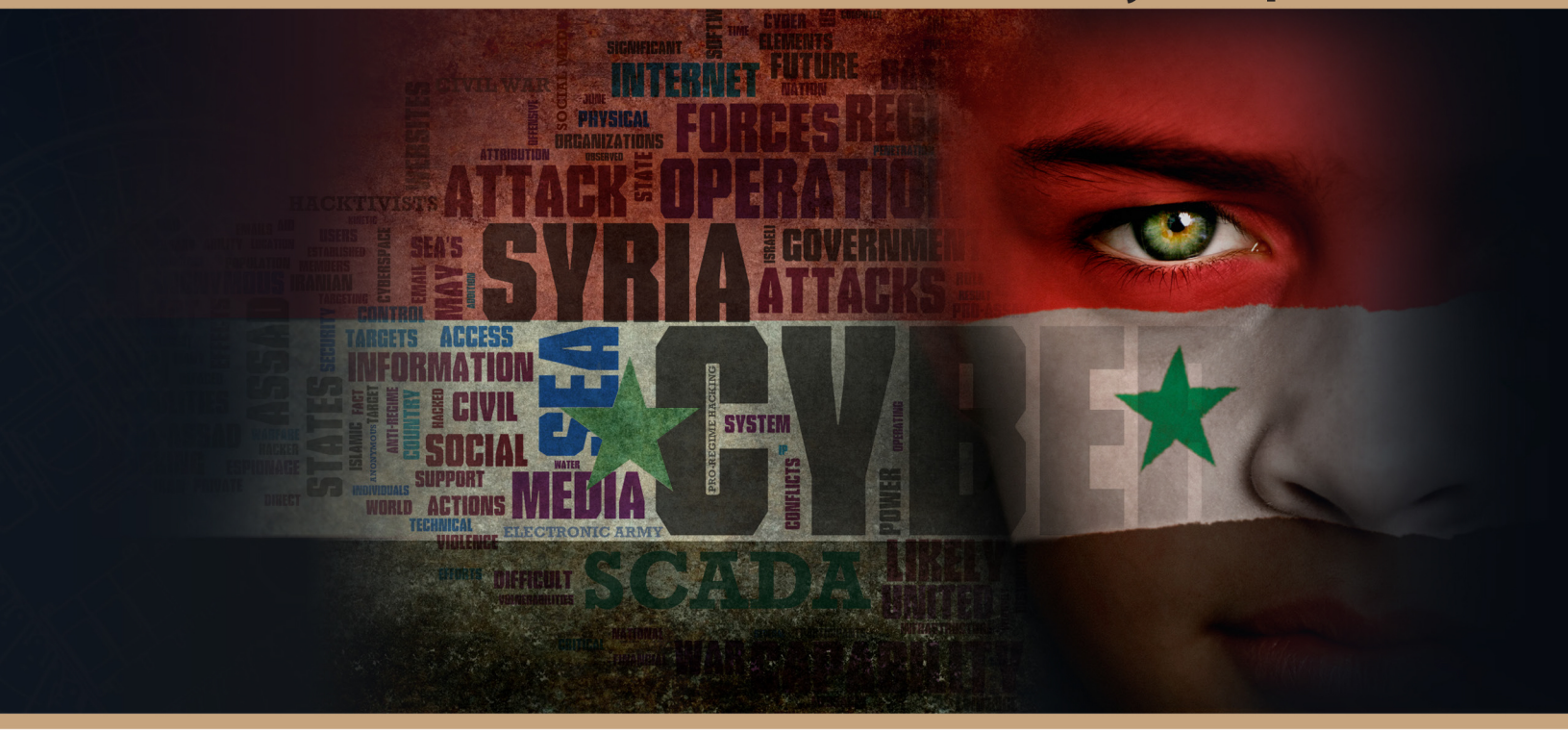
THE CYBER DIMENSIONS OF THE SYRIAN CIVIL WAR

Implications for Future Conflict

National Security Perspective



Edwin Grohe

APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

THE CYBER DIMENSIONS OF THE SYRIAN CIVIL WAR

Implications for Future Conflict

Edwin Grohe

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

This National Security Perspective contains the best opinion of the author(s) at time of issue.
It does not necessarily represent the opinion of JHU/APL sponsors.

NSAD-R-14-007

Contents

The Arab Spring spread across the Middle East and North Africa in 2011, spawning protests, demonstrations, and violence in many nations, including Syria. The uprising in Syria escalated to full-scale civil war, intensifying across multiple domains: conventional warfare between government forces and opposition groups, proxy warfare by foreign fighters and Islamic extremists fighting for religious reasons, chemical warfare, and cyber operations. Perhaps most alarming was the use of chemical weapons, a form of warfare largely banned by international agreement since the end of World War I.[1] The well-documented evidence of the Syrian government's use of chemical weapons brought unprecedented international scrutiny of the violence inside Syria.[2] Cyber operations, however, have not been as widely studied.

This paper describes cyber operations known to have been used during the Syrian uprising from January 2011 until December 2013. The cyber operations of pro-regime forces, anti-regime forces, and nations providing support, as well as US involvement and its effects on these cyber operations, are discussed as a basis for drawing observations and implications for future conflicts.

The Syrian Civil War

The statistics of the Syrian civil war as of November 2013 are staggering: of a total population of approximately 22.5 million, the death toll in the conflict exceeded one hundred thousand, more than two million refugees fled Syria, and an estimated four million refugees are still displaced inside the country itself.[3] Violence escalated quickly, as Bashar al-Assad struggled to remain in power and various opposition forces attempted to depose him, as had happened to heads of state in Egypt and Tunisia. The scale of violence in Syria exceeded even that of the uprising in Libya, where the North Atlantic Treaty Organization (NATO) intervention occurred before the Qaddafi regime's backlash could reach full strength.[4]

In the early stages of the Syrian conflict, fighting occurred largely between Syrian government forces supporting Bashar al-Assad and the Free Syrian Army, the military force of the National Coalition for Syrian Revolution and Opposition Forces (commonly known as the Syrian National Coalition), the primary opposition group that emerged in 2011. Similar to the war in Iraq, the civil war in Syria attracts foreign fighters and Islamic extremists. The largest group of Islamic fighters is the Islamic Front, which now numbers more than forty-five thousand fighters from seven different factions.[5] Although the Islamic Front and the Free Syrian Army have a common goal of removing Assad from power, the groups are certainly not allied. The Islamic Front aims to install an Islamic state in Syria vice a secular one.

US policy toward the crisis in Syria has evolved over the course of the war. In the beginning, policy makers

[1] See "Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. Geneva, 17 June 1925." See also "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction Geneva, 3 September 1992." Also see Organisation for the Prohibition of Chemical Weapons, the United Nations (UN)-affiliated organization appointed to implement the UN Chemical Weapons Convention entered into force in 1997 (http://www.opcw.org/). On October 14, 2013, the Chemical Weapons Convention entered into force for the Syrian Arab Republic, making it the 190th state party to the treaty. Syria deposited its instrument of accession with the UN secretary-general on September 14, 2013.

[2] Many news articles contain information about the civil war and the use of chemical weapons. For an overview, see Christopher Blanchard, Carla Humud, and Mary Beth Nikitin, "Armed Conflict in Syria: Overview and U.S. Response" (Washington, DC: Congressional Research Service, January 14, 2014).

[3] "Syria's Civil War: Key Facts, Important Players," *CBC News*, April 3, 2014, http://www.cbc.ca/news2/interactives/syria-dashboard/. See also Internet World Stats, "Syria Internet Usage, Broadband and Telecommunications Report."

[4] Marc Lynch, "How Syria Ruined the Arab Spring," *Foreign Policy*, May 2, 2013.

[5] "Syria Crisis: Guide to Armed and Political Opposition," *BBC News*, December 13, 2013.

debated whether the violence in Syria warranted US troop deployment directly into the area of conflict, but national will and weariness from recent wars, in addition to concern over the level of involvement of Islamic extremists in the conflict, influenced public opinion against such action.[6] However, the use of chemical weapons in the summer of 2013 renewed the prospect of direct US involvement and sparked debate among US allies. The United States is currently supporting international effort to remove chemical weapons from the country and is providing support to the Syrian National Coalition to displace the Assad regime. A recent resurgence of Islamist fighters is causing the United States to rethink its policy on that support.[7]

The Role of Social Media

The Assad regime expelled all journalists at the beginning of the uprising in 2011. For foreign media organizations, reentry into the country has been difficult and fraught with danger. In 2012, at least twenty-eight journalists were killed, and another twenty-one were abducted while covering the war.[8] Because of the dangers and difficulty with access, media organizations began reporting from outside the country but depended on information coming from within, leading to their increased reliance on raw amateur video uploaded to social media sites. Anyone in the war zone has the potential to become a correspondent as long as they have some type of video recording device, such as a video camera or a smartphone, and an Internet connection. Syrian state-run news agencies, amateur reporters aligned with the opposition forces, nonaligned Syrian citizens, and foreign visitors race to release information about events inside Syria. As a result, an overwhelming amount of information is available to mainstream news organizations.[9]

Validating the authenticity of such amateur videos from inside Syria is difficult for organizations with little to no physical presence there. Reports allege some of the violence was staged. Videos alleged to be false include one that depicts soldiers being buried alive and another showing regime supporters pouring fuel on prisoners and setting them on fire. Bashar al-Assad has challenged the United States' use of such videos, using interviews and his own social media presence on Facebook, Twitter, and Instagram[10] to refute some of the alleged evidence of violence that he is accused of ordering.[11]

Pro-Regime Cyber Operations—The Syrian Electronic Army

Aside from news organizations and videos on social media, the most prominent actor in the cyber realm that has affected the Syrian civil war is a group called

[6] "Islamic Front Gains Reduce U.S. Options in Syria, Further Undermine Prospects for Upcoming Geneva II Summit," *IHS Jane's Defence Weekly*, December 12, 2013.

[7] Damien McElroy, "Saudi Arabia Warns It Will Act against West's Policy in Middle East," *Telegraph*, December 18, 2013.

[8] Zeina Karam, "Syria's Civil War Plays Out on Social Media," *Denver Post*, October 20, 2013.

[9] Ibid.

[10] Ibid.

[11] Social media videos present two basic problems: 1) identification of the individual who posted the video and 2) determining the integrity of the video itself. Discovering the real identity of the individual who posted the video is nearly impossible. People can post videos to social media via one of several identification schemes: anonymity (not being known by any name); nonymity (not being known by any label or identifying characteristic, even anonymity); pseudonymity (being known by a false name); polynymity (being known by multiple names); or eponymity (being known by a real name). Even those who post eponymously can do so under false credentials. See Eleni Berki and Mikko Jäkälä, "Cyber-Identities and Social Life in Cyberspace," in *Social Computing: Concepts, Methodologies, Tools, and Applications*, ed. Subhasish Dasgupta (Hershey, PA: IGI Global, 2010), 92–104. The perceived integrity of the video itself is based on identification of the individual who posted it, perception of that individual's trustworthiness, and video analysis; however, videos posted to social media are still subject to authenticity problems.

the Syrian Electronic Army (SEA). The SEA is a pro-regime hacking group whose activities range from public outreach to destructive cyber attack and exploitation, with some evidence suggesting cyber espionage. From its beginning in May 2011, the SEA has had close ties to Bashar al-Assad himself, with several founding members belonging to the Syrian Computer Society (SCS), the organization responsible for introducing information technology (IT) to Syrian society.[12]

The SCS was founded in 1989 by Bassel al-Assad, Bashar al-Assad's older brother. Bassel had both a technical and a military background and was being groomed to succeed his father as president of Syria.[13] After Bassel died in a 1994 car accident, Bashar assumed control of the SCS.[14] Bashar, influenced by the Western lifestyle he had experienced while studying ophthalmology in London, wanted to modernize Syrian society.[15] Throughout his tenure at the SCS, his only public role before becoming president of Syria in 2000, he wanted to introduce computers and the Internet into Syrian life but stated often and openly that this introduction needed to be gradual and carefully controlled.[16] Syria has seen growth in the number of computer Internet users since Bashar assumed the role of president, but the numbers pale in comparison to those of modern Western societies. In 2000, there were an estimated thirty thousand Internet users in Syria, or roughly 0.2 percent of the population. In 2012, there were more than five million Internet users, but still only 22.5 percent of the population.[17] By comparison, the US Internet usage rate was 78.1 percent of the population in 2012.[18]

The Assad regime filters the Internet for fear of the advantages knowledge and communication might provide to the population, which likely contributes to the limited Internet penetration in Syria.[19] Not only does the Assad regime control access to information inside Syria, including state-run news agencies, but it also aims to control its image externally. Syria is not the only country that asserts this type of control.

The SEA was created to provide a "pro-Assad counter narrative to news coming out of Syria."[20] As a counter to the stories of violence that were emerging from Syria, most of the SEA's early activities involved spreading pro-Assad messages throughout social media outlets via spamming and other nondestructive means. In addition, the SEA used its public Facebook page to recruit new members and run a virtual "hacking academy," distributing instructions and malware for computer exploitation and distributed denial-of-service (DDOS) attacks.[21] The DDOS software was specifically designed to attack four news websites the SEA claimed were hostile to the regime: Al Jazeera, BBC News, Orient TV, and Al Arabia. The fact that the DDOS software was already loaded to attack selected targets implies that the SEA has the ability to develop its own tools from publically known vulnerabilities.

Although the SEA's initial actions mostly resembled social media and public affairs activities, there were

[12] Nicole Perlroth, "Hunting for Syrian Hackers Chain of Command," *New York Times*, May 18, 2013.

[13] Mimi Dwyer, "Think Bashar al Assad Is Brutal? Meet His Family," *New Republic*, September 8, 2013.

[14] Jillian Scharr, "What Is the Syrian Electronic Army?," T*om's Guide*, August 29, 2013.

[15] Majid Rafizadeh, "Assad's Family: The Unrecognized Nuances and the Politics," *Huffington Post*, May 13, 2013.

[16] Jon B. Alterman, *New Media, New Politics? From Satellite Television to the Internet in the Arab World* (Washington, DC: The Washington Institute for Near East Policy, 1998). See p. 40 referring to an Arabic publication by Ibrahim Hamidi and Rania Ismail, "Asad's Son to al-Hayat: The Internet Is a Double-Edged Sword," *al-Hayat*, October 12, 1997, p. 1.

[17] Internet World Stats, "Syria Internet Usage, Broadband and Telecommunications Report."

[18] Internet World Stats, "Internet Usage Population and Telecom Reports for the Americas."

[19] Khaled Yacoub Oweis, "Syria Expands 'Iron Censorship' over Internet," *Reuters*, March 13, 2008.

[20] Perlroth, "Hunting for Syrian Hackers Chain of Command."

[21] "Syrian Electronic Army: Disruptive Attacks and Hyped Targets," *Information Warfare Monitor*, June 25, 2011.

early signs that the group might have some capability for cyber attack. The SEA's first demonstrated cyber attack capability came in a well-publicized event in June 2011 when it defaced more than 130 websites, most of which were random targets. Many of the websites displayed embedded photos and full-color messages supportive of Bashar al-Assad; some of them displayed simple text messages. Ninety-five of the defacements resolved to a single Internet Protocol (IP) address. This suggests that the SEA exploited a single vulnerability (exploitation) in a server that hosted all of those websites, vice individually hacking each one.[22] Many of those websites were defaced on May 13, 2011, by a hacker who claimed to be Iranian. This suggests early collaboration between the SEA and Iranian hackers.[23]

Also in June 2011, the SEA exploited and defaced the websites of a member of the Israeli Knesset, an Israeli travel organization, the Center for Small Business Development in Israel, and the Israel Chemical Society. Many of these websites did not contain political content and were likely chosen because of their vulnerability; they resolved to the same IP address as sites that had been hacked on June 4, 2011, suggesting that the SEA simply waited a few days to announce its attacks.[24] It also hacked the French website of the French embassy in Damascus, posting pro-Assad messages. At the end of June 2011, the SEA hacked forty-one United Kingdom-based websites; once again, many of the targeted websites resolved to a single IP address, suggesting server exploitation. The websites were replaced with a message to the British people requesting that they stay out of Syria's business.[25]

Although the June attacks included three IP addresses of servers in the United States,[26] the first recognized US hacking by the SEA is the group's defacing of the University of California at Los Angeles website. The website temporarily hosted a simple text message supportive of Bashar al-Assad.[27] After this attack, the SEA defaced Harvard University's website with pro-Assad multimedia messages.[28] The Harvard attack was in September 2011 and was similar to the June attacks, with embedded photos and full-color messages. However, this time, the defaced website looked similar in format to the original website, suggesting that the SEA was experienced with web design software.[29]

In 2013, as Syrian internal strife became more violent, the SEA changed methods and membership, becoming more of a "loose hacking collective, than a state-sponsored brigade."[30] Ties to Assad were still apparent, but because the SEA was not an official government entity, there was doubt as to how much control Assad had over the group. Cyber attacks became more targeted and increasingly more malicious, with hackers stealing credentials through spear-phishing. These techniques are effective against "soft" cyber targets and allowed the SEA to engage in pro-Assad defacing of public websites and spamming campaigns against entities that were perceived to be hostile to the Assad regime.[31] Several attacks garnered international attention, including attacks on the *Washington Post*, the *New York Times*, *National Public Radio*, *CBS News*, *Al Jazeera*, *BBC*,

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] "Syrian Electronic Army Defaces 41 Web Sites, One UK Government Web Site," *Information Warfare Monitor*, June 29, 2011.

[26] "Syrian Electronic Army: Disruptive Attacks and Hyped Targets."

[27] Bruce Sterling, "Syrian Electronic Army Invades University of California Los Angeles," *Wired*, July 6, 2011.

[28] Tara Merrigan, "Harvard's Website Hacked by 'Syrian Electronic Army,'" *Harvard Crimson*, September 26, 2011.

[29] Ibid.

[30] Perlroth, "Hunting for Syrian Hackers Chain of Command."

[31] Kenneth Geers et al., *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks* (Milpitas, CA: FireEye, 2014).

the *Daily Telegraph*, the *Financial Times*, and the US Marine Corps website, among others.[32] Perhaps the most damaging attack was the hacking of the Associated Press Twitter account, achieved by a spear-phishing campaign against reporters at the news organization.[33] SEA hackers posted false news of explosions at the White House and injury to President Obama. Because of the speed at which social media news travels, the Dow Jones Industrial Average dropped 127 points within two minutes but quickly rebounded when the story proved false.[34]

It is unclear whether the SEA's rudimentary tactics are by choice or are because of the group's limitations, but the SEA likely intends to have a more strategic impact. In May 2013, it attempted to access and attack an Israeli computer network that controls the water system in Haifa, Israel,[35] possibly in retaliation for an Israeli airstrike targeting Iranian missiles near Damascus in early May 2013.[36] The SEA's "proof" of the attack itself is suspect—screenshots of a water system with Hebrew labels. Examining the images reveals that they are from the SCADA (supervisory control and data acquisition) software system IRRInet Control Center (ICC) made by Mottech Water Management Limited (http://www.mottech.com/). The screenshots do not seem to display a real water system; rather, they likely show an Israeli farm. It is important to note, however, that the ICC software is capable of remotely controlling valves, pumps, and water flow. Despite the fact that the SEA did not gain access to the Haifa municipal water control system, it may have demonstrated a capability to gain control of a SCADA system by using default passwords. These actions imply intent to have real effects in the physical world delivered through the cyber domain.[37]

There are other elements suggesting the SEA has the ability to use the cyber domain to cause physical effects. "Paralleling the group's boisterous, pro-Syrian government activity has been a much quieter Internet surveillance campaign aimed at revealing the identities, activities and whereabouts of the Syrian rebels fighting the government of President Bashar al-Assad."[38] The SEA exploited and stole data from three different communications systems that could contain information on the Assad regime's opponents. Targets of the SEA attacks included the web-based telephone directory Truecaller[39] as well as the Internet communications services Tango[40] and Viber.[41] Pro-Assad cyber forces also delivered spyware, disguised as an encryption service for Skype, to targeted computers, demonstrating new technical prowess.[42] These types of cyber operations are classified as espionage and demonstrate an improved capability for pro-Assad cyber forces. How that capability was improved is unknown. The information obtained through this espionage is also unknown, but access to communications paths, conversations, and personal computers of opposition

[32] Ibid.; Robert Windrem, "Syrian Electronic Army Seen as a 'Nuisance' Not a Serious Cyber Threat," *NBC News*, October 8, 2013; Cory Bennett, "Syrian Electronic Army Comes after U.S. Military," *FedScoop*, September 3, 2013; and Perlroth, "Hunting for Syrian Hackers Chain of Command."

[33] Christopher Mims, "How the Syrian Electronic Army Hacked the AP—And Who Are These Guys Anyway?," *Quartz*, April 23, 2013.

[34] Paul Vigna, "Stocks Plunge, Quickly Recover, on Fake Tweet," *MoneyBeat* (blog), *Wall Street Journal*, April 23, 2013.

[35] AhlulBayt News Agency (ABNA), "Syrian Electronic Army Hacks Israel's Main Infrastructure Control System (SCADA)," May 8, 2013. See also Elad Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?" *Water Simulation*, June 5, 2013.

[36] Dominic Evans and Oliver Holmes, "Israel Strikes Syria, Says Targeting Hezbollah Arms," *Reuters*, May 5, 2013.

[37] Salomons, "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?"

[38] Perlroth, "Hunting for Syrian Hackers Chain of Command."

[39] Anupika Khare, "Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts," *iDigital Times*, July 19, 2013.

[40] Chloe Albanesius, "Tango Messaging App Targeted by Syrian Electronic Army," *PCMag*, July 23, 2013.

[41] Warwick Ashford, "Syrian Hacktivists Hit Second Mobile App in a Week," *Computer Weekly*, July 24, 2013.

[42] Perlroth, "Hunting for Syrian Hackers Chain of Command."

personnel could reveal their tactics, techniques, procedures, or, even more important to the Assad regime, identities and locations. Targeting opposition forces through their IP addresses, coupled with geolocation services such as Google maps, puts those targets at risk of kinetic attack.

Opposition forces suspect that these cyber intelligence efforts have also begun to target foreign aid workers.[43] This targeting shift likely occurred because opposition forces became aware that their physical locations were being detected through the SEA's use of IP addresses. Opposition forces have subsequently developed operational security practices that may have complicated the intelligence efforts against them. Pro-Syrian cyber forces now have to take advantage of less secure-minded aid workers, tracking their actions and physical locations instead of those of the opposition forces. Aid workers are usually located in close proximity to opposition forces, possibly enabling the Assad regime to direct lethal strikes against the opposition forces by using locations of aid workers.

There is also another pro-Assad hacking group operating in the cyber realm, the Security Lions Hackers (SLH). Like the SEA, the SLH has a Facebook page and conducts public affairs outreach. Unlike those of the SEA, the SLH attacks are much less publicized, and therefore, the group's capabilities are largely unknown. Also unlike the SEA, which attacks mostly Western media services, the SLH attacks random sites. One known victim is the US College Hockey Online fan forum, which was defaced with pro-Assad messages in September 2013. The large number of operators in the cyber domain makes it difficult to determine exactly who is doing what, but the SLH attacks demonstrate that the SEA is not the only pro-regime hacker group in Syria.

[43] Ibid.

Anti-Regime Cyber Operations

Aside from using the Internet and social media to post videos of violence, opposition forces inside Syria have used the cyber domain against the Assad regime less frequently than pro-Assad hackers have used this domain against the opposition. An anti-regime hacker used information and malware from the SEA's Facebook page in 2011 to coordinate his own DDOS attacks against regime websites. The malware was repurposed to attack four pro-regime websites: those of the General Organization of Radio and TV, the Addounia TV station, and two Syrian news agencies.[44]

One particularly embarrassing incident for the regime was the release of private e-mails between Bashar al-Assad and family members and advisers. Anti-regime forces used credentials that were either passed from a regime insider or guessed by an anti-regime hacker to monitor a private e-mail account Bashar al-Assad used to communicate outside of the normal government network.[45] Anti-regime forces quietly monitored the e-mail account hoping to find some critical piece of information that would discredit the regime. That critical piece of information worth revealing the anti-regime force's espionage was not found; however, a collection of these e-mails was eventually published by news agencies such as the Guardian and the anti-secrecy group WikiLeaks. The e-mails emerged in early 2012 and painted an unflattering picture of the dictator. Through the e-mails, it was apparent that Bashar al-Assad and his family were circumventing extensive sanctions to spend hundreds of thousands of dollars on luxury items while his country was mired in a violent rebellion. Assad appeared to make light of

[44] "Syrian Electronic Army: Disruptive Attacks and Hyped Targets." The anti-regime hacker's website is located at http://xacker.wordpress.com/. Posts ended in April 2011.

[45] Robert Booth, Mona Mahmood, and Luke Harding, "Exclusive: Secret Assad Emails Lift Lid on Life of Leader's Inner Circle," *Guardian*, March 14, 2013; and Ilan Ben Zion, "Hacking Assad…as Easy as 1,2,3,4," *Times of Israel*, September 6, 2012.

reforms he promised to quell the uprising while he ignored advice from friends that he and his wife flee Syria and seek asylum in Qatar. There was evidence that Assad was taking advice from Iran. The e-mails also revealed Assad's awareness of the importance of public outreach via social media and intervening in public online discussions—actions similar to those taken by the SEA.[46]

The anti-regime forces' access to the e-mail account was cut off in February 2012, about the same time a US-based hacker group, Anonymous, hacked into multiple e-mail accounts in Syria.[47] Anonymous announced that it had accessed an e-mail server at the Syrian Ministry of Presidential Affairs, which offered access to many e-mail accounts. Anonymous was able to access the server and e-mail accounts, which had a relatively easy password of 12345, underscoring the need for stronger passwords for all users.[48] The release of Assad's e-mails was likely a result of this hacking by Anonymous.

Anonymous is a leaderless hacking collective that prides itself on anonymity—hence the group's name. It ascribes to many different causes as dictated by its members. Anonymous is not homogenous in purpose. Actions for a particular cause are called operations, and Anonymous has an ongoing "Operation Syria," which initially targeted both the opposition groups inside Syria as well as the Assad regime. As the conflict escalated, evidence suggested to Anonymous that Assad was more of a threat to Internet freedom in Syria and more guilty of violence against innocent people than the opposition. Anonymous then concentrated its efforts against the government of Syria and aligned itself with anti-regime forces.[49] As a part of its operation, Anonymous attempted to hack and subsequently "out" members of the SEA. Outing fellow hackers by publicly posting information about them is seen as the worst offense among hacking groups in the ambiguous world of hacktivist cyber operations. Members of the SEA denied that they were hacked and that the named people were affiliated with the group.[50] Anonymous currently controls the former "hacking academy" established by the SEA.[51]

In addition to Anonymous, which operates in the domain with shifting allegiance, there are other hacktivists operating with clearer motives. A US-based hacker known by the pseudonym Oliver Tucket has hacked targets in Syria in an effort to obtain information that might be damaging to Bashar al-Assad. According to reports by the *Washington Post*, Oliver Tucket is upset at the publicity that the SEA receives for its less-than-skillful hacking activities and by the actions of the Assad regime. Oliver Tucket has hacked at least one government server in Syria, accessed documents, read e-mail traffic, and redirected websites and mail services in an effort to discredit the government of Syria.[52] The involvement of Anonymous and Oliver Tucket in the Syrian conflict underscores the fact that anyone can participate, regardless of political affiliation or geographic location.

[46] Robert Booth, Mona Mahmood, and Luke Harding, "Exclusive: Secret Assad Emails Lift Lid on Life of Leader's Inner Circle," *Guardian*, March 14, 2013.

[47] Ibid.

[48] Zoe Fox, "Anonymous Hacks Syrian President's Email," *Mashable*, February 7, 2012.

[49] Anonymous has its own website as well as a number of outreach platforms including Twitter, Tumblr, and YouTube. Press releases regarding Operation Syria can be found on the group's various public outreach sites. However, most of these sites are blocked by enterprise IT services. Some Anonymous tactics include DDOS attacks, which can use unsuspecting "zombie" computers as launch points for attacks, unbeknownst to the computers' owners. Visitors to the Anonymous website risk their computers becoming infected with malware that will then make their computers part of the Anonymous zombie network.

[50] Michael Stone, "Anonymous Hacks Syrian Electronic Army: Operation Syria Engaged," *Examiner.com*, September 2, 2013.

[51] The website https://www.facebook.com/school.hacker displays Anonymous's iconic Guy Fawkes mask (accessed February 7, 2014).

[52] Andrea Peterson, "Here's How One Hacker Is Waging War on the Syrian Government," *The Switch* (blog), *Washington Post*, August 28, 2013.

Effects of US Involvement on the Cyber Domain

Although the United States can use all elements of national power [diplomatic, informational, military, economic, financial, intelligence, and law enforcement (DIMEFIL)] to affect Bashar al-Assad and his regime, it has not used all elements. Some of those elements have second- and third-order effects in the cyber domain and support the Syrian National Coalition's effort to remove Assad from power. However, a recent resurgence of the Islamic Front has raised the possibility of an extremist regime in Syria, which could be more threatening to the goals of Western nations than Bashar al-Assad's remaining in power.[53]

The application of elements of national power, such as attempts to remove chemical weapons, economic sanctions to include an embargo, and financial assistance to those victims of the Syrian civil war, are aimed at influencing the Syrian regime and its ability to threaten the region; however, the same elements of power have also affected the cyber domain in the following ways.

The economic sanctions have directly affected the Syrian civil war as well as the cyber dimension of the war, but sanction violations have occurred. However, there is evidence that violations and violators are pursued. In October 2011, a US company discovered that thirteen of fourteen of its Internet filtering devices shipped to a distributor in Dubai and intended for the government of Iraq had made their way to Syria and were being used by the Syrian government to filter the general population's Internet access. After it completed a voluntary investigation, and with knowledge that its product had been illegally imported to Syria, Blue Coat Systems, Incorporated of Sunnyvale, California, blocked updates to its devices operating in Syria, which eventually numbered more than thirty.[54] Eventually, the Dubai-based distributor of Blue Coat Systems hardware, Computerlinks FZCO, was fined $2.8 million for illegally delivering the devices to Syria.[55] In another example of sanctions enforcement, Network Solutions, LLC seized more than seven hundred domain names that the US Office of Foreign Asset Control had registered to entities tied to the Assad regime. After the seizure, the domain names remained unusable to elements of the Assad regime, forcing them to change their online presence.[56]

As for the financial aid that the United States is providing to the Syrian opposition, this is meant, in part, to enhance "the linkages between Syrian activists, human rights organizations, and independent media outlets."[57] Specific media outlet support includes "training for networks of citizen journalists, bloggers, and cyber-activists to support their documentation and dissemination of information on developments in Syria; and technical assistance and equipment to enhance the information and communications security of Syrian activists within Syria."[58] Given that the Syrian government, likely through the SEA, has been conducting cyber espionage against opposition forces, this influx of technology and training will likely improve the operational security of opposition forces and frustrate the regime's efforts to find, fix, target, and track them through cyberspace. This financial assistance to bloggers and cyber activists is also in direct opposition to the support that the SEA has provided Syria for pro-regime outreach purposes.

[53] McElroy, "Saudi Arabia Warns It Will Act."

[54] Jennifer Valentino-Devries, Paul Sonn, and Nour Malas, "U.S. Firm Acknowledges Syria Used Its Gear to Block Web," *Wall Street Journal*, October 29, 2011.

[55] Steve Stecklow, "Dubai Firm Fined $2.8 Million for Shipping Blue Coat Monitoring Gear to Syria," *Reuters*, April 25, 2013.

[56] Brian Krebs, "Trade Sanctions Cited in Hundreds of Syrian Domain Name Seizures," *Krebs on Security*, May 8, 2013.

[57] Department of State, "U.S. Government Assistance to Syria—Fact Sheet," September 7, 2013.

[58] Ibid.

Observations

The study of cyber operations in the Syrian civil war reveals several key points that can be potentially applied to future conflicts. Some of these observations apply to past conflicts or other events, and some are unique to the Syrian civil war.

Social media plays a role in conflict. Even in a nation with as little Internet penetration as Syria, social media and amateur reporting can (and, in the case of Syria, did) augment or surpass reporting of mainstream news organizations. When news organizations lose the ability to cover a story, social media can fill the gap. Both sides of the conflict used social media outlets to spread their view of the events inside Syria. However, authenticating and interpreting what is observed in social media can be difficult, if not impossible.

Even Syria has a cyber force. One would not expect a nation with as little Internet penetration as Syria to have an established cyber force. More developed and connected nations likely have an easier time recruiting cyber-smart individuals to work in the IT sector because more of the population is exposed to the technology. Syrian society in general has little exposure to the Internet; therefore, it would seem difficult for the regime to develop a large cadre of cyber-smart people that have the ideological alignment required to conduct operations in support of the regime, yet the regime recruited such individuals. Despite the SEA's indirect ties to the regime of Bashar al-Assad, it seems clear that the group is a de facto national cyber force conducting cyber operations on behalf of the regime. It is not clear, however, whether Syria has cyber doctrine or has established chain of command over the SEA.

Even a fledgling cyber force can have effects. Despite its humble beginnings as a public affairs organization, the SEA has gained worldwide attention with its cyber attacks against Internet-based media organizations and social media. Although SEA's cyber operations are viewed mostly as nuisance attacks with no real effect on the outcome of the conflict, the progression of the SEA's capability over such a short period of time is concerning to outside observers. The group's demonstrated cyber espionage capability, coupled with real-time geo-location services, conducted against opposition forces and activists makes it clear that cyberspace can enable targeting in the physical world, whether by merely identifying targets or by performing some of the find, fix, target, and track parts of a kill chain. Although there are no confirmed deaths in Syria as a direct result of cyber operations, it is likely that cyberspace–geo-location combined actions resulted in kinetic attacks on opposition forces. The demonstration of the SEA's SCADA penetration capability is also alarming because its cyber operations skill level is relatively unsophisticated.

The cyber domain provides anonymity. As noted, anyone can pose as anyone else in social media. There are advantages and disadvantages to this ambiguity. It can be disadvantageous to someone who is being truthful and seeking trust, and it can be advantageous to those who are trying to appear more trustworthy than they are. For the user, authentication of what is observed in social media can be difficult, if not impossible.

The difficulty in attributing a cyber attack to a specific person, group, or nation-state offers actors the opportunity to take offensive action without attribution. The SEA takes responsibility publicly for most of its cyber attacks, making attribution relatively easy; however, its individual members' identities are still largely unknown. Anyone can enter the cyber domain during a conflict—individuals like Oliver Tucket with an ideological motivation, hacking groups like Anonymous with varied political objectives, semi-state-sponsored hacking collectives like the SEA, and nation-states themselves. Identifying who is conducting a cyber attack requires more than determining the location where the action originated; even that location may be several Internet hops (even several countries) away from the actual attacker's location. The presence of a multitude of actors with

a multitude of motivations makes it difficult to know exactly what is going on in the domain and who is responsible. When the SEA acts in the cyber domain, the government of Syria reaps the benefit of the group's actions but can deny involvement when those actions are discovered. This ambiguity of actor and purpose not only obfuscates the objective of the cyber action but muddies the ability of victims to retaliate. Proving attribution can be difficult and may require that the attributor reveal computer forensic capability the victim prefers to keep hidden.

The targets of cyber attacks in the Syrian civil war were not limited to the cyber assets of the direct participants. After initial random targeting, most of the SEA's targets were private social media or news companies that reported stories that painted the Assad regime in an unfavorable light. The SLH targets appear to have little to do with the Syrian civil war or Bashar al-Assad. Although there was no direct military value in any of these targets, websites of media organizations can affect the public's opinion of a conflict.

Direct participants in the cyber operations of the Syrian civil war were only limited by capability. The SEA and the SLH seemed to target anything and everything that they had the ability to exploit and attack, either through technical means or via credentials obtained through spear-phishing. The cyber espionage conducted by both pro-regime and anti-regime forces was likely at the upper limit of their technical capabilities. The SCADA penetration demonstrated by the SEA, if that was the SEA's intent, could have led to physical damage in the real world if they had penetrated a target of value. It is important to note that this penetration was enabled by the SCADA system administrator's use of default passwords, rather than by an elevated technical capability of the SEA. If the SEA had the opportunity and capability to cause damage to valuable cyber targets, it likely would have.

Indirect participants in the cyber operations of the Syrian civil war had significant capability but chose to withhold destructive cyber operations. Russia and Iran are alleged to play a role in the cyber operations of the Syrian civil war and may have provided the SEA with enhanced cyber capability. However, despite the capability of these states, there is no evidence of significant cyber attack in the Syrian conflict. This may signify that these indirect participants have withheld cyber technical and operational knowledge from the SEA and the Assad regime because of policy; Russia and Iran certainly have capability to cause great destruction via cyber means.

Financial and economic elements of power can have effects against cyber operations. Embargoes, economic sanctions, and financial aid are powerful tools in the US nonmilitary arsenal and can be effective at limiting the efficacy of an adversary's kinetic capabilities. Cyber tools, both hardware and software, have different properties that can make them more or less difficult to contain. For example, whereas a Blue Coat ProxySG 9000 (the filter that Syria illegally acquired during the US embargo) can cost hundreds of thousands of dollars, identifying the device on a manifest and preventing its sale is much easier than doing the same for the K9 Protection suite, which is available for sale on the Internet and can be transferred electronically. US aid that provides training, software, and hardware to Syrian opposition forces is likely countering some of the effects of the Syrian surveillance program and promoting free speech.

System users represent a weak point in cybersecurity. The system user remains a constant vulnerability in cybersecurity. The SEA's crude tactics were based on easily guessed (or default) passwords, careless system users that clicked on links in spear-phishing e-mails, and systems with exploitable vulnerabilities. System users must remain vigilant so that they do not fall victim to such malicious activity, especially when that system controls critical infrastructure, is a trusted news organization's public outreach platform,

or contains the private communications of a public figure. To prevent unauthorized access, even the best network hardware and software still require proper cyber hygiene and well-trained users who are conscious of operations security.

Implications for Future Conflict

Although drawing implications for the future from one case study can—and should—lead to debate and counterargument, the use of cyber operations during the Syrian civil war suggests several implications for future conflicts that are difficult to ignore.

Internet-based social media is a useful tool with many purposes, but authenticating its content can be nearly impossible. Social media can affect the opinions of participants in and observers of a conflict. As each side races to get its view of events into social media, truth can be a victim. Thus, we can anticipate that social media will be a prominent source of both accurate and false information in future conflicts. Trusted journalistic sources will be the de facto method of choice for individuals to form opinions about future conflicts. Making foreign policy decisions that affect the life and death of individuals based on videos and postings that cannot be authenticated is inherently unwise. Thus, governments will undoubtedly continue to rely on their intelligence assessments, which include analysis of social media, as a basis for formulating foreign policy.

The US government and private companies will continue to suffer minor cyber attacks, especially if their cyber infrastructures are seen as a way to influence public opinion or national policy. In the case of a state response to minor cyber attacks against private companies within its borders or control, the options are unclear. If the attacks are acts of international vandalism attributable to a state, redress would normally be sought through the International Court of Justice (ICJ), the judicial organ of the United Nations that has competency over legal cases between states that consent to the court's jurisdiction.[59] Article 2(4) of the United Nations Charter prohibits "the threat or use of force against the territorial integrity or political independence of any state," which is now widely understood to include any use of force, including certain acts within the cyber realm.[60] A successful claim will require technical proof of attribution, which may be difficult because cyber actors can obfuscate their identities. Even if the attacks emanated from a physical location inside a state, proving that they are intentional acts of the government is difficult and will likely require all-source intelligence capability beyond that of the cyber domain. Such capability may include intelligence sources that the state wants to keep hidden.

Even if attribution is proven, and the cyber attack is known to have been the intent of a government, international norms of retaliation are not yet established for vandalism by a nation-state. US past practices have been to simply absorb minor attacks and increase security; this de facto policy of restraint will likely continue into the future and may create an international norm for such attacks.

Occasional demonstrations of cyber capability to deter future cyber aggression can be useful. Responding to a cyber attack with a cyber counterattack invites mistakes. As Martin Libicki observes, "In cyberspace what the attacker does, what he thinks he did, and what the defender thinks he did may all be different. The defender can only react to what he thinks the attacker did."[61] Every target offers differences in operating system, port

[59] Article 34, Statute of the International Court of Justice, http://www.icj-cij.org/documents/?p1=4&p2=2.

[60] Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts," in *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Research Council, 2010), 151–178.

[61] Martin Libicki, *Managing September 12th in Cyberspace* (Santa Monica: RAND Corporation, March 21, 2013).

configuration, patches, intrusion detection systems, anti-virus software, firewalls, and more. The variables in a cyber target are numerous and can affect how a piece of malware operates or does not operate. If a victim responds without positive attribution, there is risk of being tricked into attacking a third party and thereby gaining a new adversary.

Responding to cyber attack in the cyber domain also reveals capability. The United States undoubtedly has significant cyber forensic capability, as well as an array of offensive cyber capability, but it must maintain a balance between uses of those capabilities and the risk of exposing them. Any action taken against a relatively minor adversary might alert a more significant adversary to US capabilities, thereby allowing adversaries time to create defenses against the displayed tactics. States must keep in mind that use of offensive cyber capabilities in future conflicts will have repercussions on government and private networks located within their territories. This phenomenon is known as blowback.[62] Potential cyber capabilities of the adversary, vulnerabilities in one's own security, and resilience of network infrastructure must be accounted for in future conflict.

On the other hand, there is a deterrence argument to be made. Franz-Stefan Gady argues that "at the lowest level, one way to increase the deterrence factor vis-à-vis adversaries is to have a more systematic public display of nation states' cyber-war capabilities. This can have a greater deterrence effect on non-state actors operating in the service of Iran and Syria, because they will have a clearer understanding of the forces arrayed against them. It can also make 'signaling'—conveying the intentions of a state through a particular policy or move—easier, since a better understanding of capabilities reduces the likelihood of misguided policies."[63] There is also the possibility of instilling in an adversary the belief that if the United States was able to attack once, it could likely repeat the effect, despite any advances in defensive measures enacted as a result.

Limited cyber operations to promote Internet freedom or conduct humanitarian operations could change the perception that cyber attack is always malicious. Many countries limit their citizens' access to the Internet, filtering information and using malware to spy on opposition forces. Through their own actions, such countries create vulnerabilities that the United States likely has the means to exploit. For example, US financial support is being used to enhance the ability of journalists, bloggers, and cyber activists to spread the word about what is occurring in Syria, but there is more action that could be taken. A coordinated offensive cyber operation to bring open Internet into Syria could occur. The United States likely has the offensive cyber capability to modify the filtering parameters of the Blue Coat proxy servers to give the Syrian populace unfiltered access to information.[64] This line of operation is aligned with the US ideological stance on freedom of speech and is consistent with other US efforts in Syria. However, the norms for this type of cyber operation against IT systems have not been established. If the United States had used its cyber offenses in addition to financial aid to increase citizens' knowledge of events inside the country, it would have revealed that it has the capability to do so; computer forensics after the fact may also have revealed the US sources and methods for conducting such an attack and thereby reveal new knowledge to adversaries. However, the United States may occasionally have to demonstrate its capability in an overt way to deter its adversaries.

[62] Blowback refers to unintended consequences of a military or intelligence operation suffered by assets of the aggressor. Blowback can cross domains (i.e., aggressive action in the conventional military domain can result in cyber attack against the aggressor's associated cyber assets). This definition is adapted from Chalmers Johnson, "Blowback," *The Nation*, October 15, 2001.

[63] Franz-Stefan Gady, "Syria: Preparing for the Cyber Threat," *National Interest*, September 5, 2013.

[64] This would be difficult to sustain without physical presence because Syrian officials could disconnect the coaxial cables and network links that connect Syria to the Internet.

There are other possibilities for cyber operations in Syria as well. Recently, David Sanger and Eric Schmitt wrote in the *New York Times* that the United States has been planning cyber operations against the Assad regime since the beginning of the conflict there. In particular, there has been discussion at the highest levels of government concerning a possible humanitarian mission that could be conducted via cyber attack. The details of that humanitarian role are not disclosed, but there is possibility that acknowledged US responsibility for that role could change the worldview of US cyber operations, which has recently been portrayed in an unflattering light after leaks by Edward Snowden.[65]

Many cyber vulnerabilities inside Syria are best left alone. According to Franz-Stefan Gady, "Syria is connected to the World Wide Web via three undersea cables and a terrestrial line via Turkey; however, the digital gateway to the country is centrally controlled by the state-owned Syrian Telecommunications Establishment (STE), which makes it much easier to cut off connectivity. Consequently, the impact of a cyber-weapon launched against the STE with the aim of knocking Syria offline will proportionally have bigger net effects on Syria than similar attacks on a country with a more decentralized critical information infrastructure."[66] Gady continues, "The same is true for the Syrian power grid. According to Jeffrey Carr, it is a small grid with only about 14 power-generating stations, all of which use foreign vendors, providing easy access points for foreign cyber warriors. Syria also receives most of its electricity from a single source—Iran. Both factors combined make the successful targeting of a select number of industrial control systems to cut off electricity simpler."[67]

These two items represent severe vulnerabilities to the Syrian nation that would have debilitating effects on not only the government but also the population. The United States must weigh proportionality and the military necessity of any action it would take in cyberspace, in addition to collateral damage. Using cyber effects to cause power outages or communication losses will hurt the regime but will also have potentially unacceptable effects on noncombatants.

When the United States deploys military forces to a conflict, it must be able to defend its networks and critical infrastructure from the opposing side and its supporters. If the United States conducts kinetic action against the Assad regime, the real possibility exists that the SEA, or other cyber actors sympathetic to the regime, could retaliate against the United States, Israel, or Western interests.[68] The questions remain: who would respond in cyberspace to US kinetic attack in Syria and what kinds of capabilities, cyber and otherwise, does that group possess? The SEA likely does not possess capability against US critical infrastructure, but that is not to say that the Iranians or Russians do not. We cannot rule out the possibility that Russia or Iran would use their cyber capabilities to attack the United States for deploying forces in the Syrian civil war. The cyber domain offers opportunity for proxy warfare but likely with more blowback than is worth the risk. The nuclear capability of an adversary routinely is a factor in US political and military decisions; cyber capability of an adversary will also have to be a consideration in future conflicts.

The most destructive cyber capabilities (those with significant collateral effects on civilian populations) are likely to be used only when the existence of the actor is at stake. The United States, Iran, and Russia are indirectly participating in the Syrian civil war. None

[65] David Sanger and Eric Schmitt, "Syria War Stirs New U.S. Debate on Cyberattacks," *New York Times*, February 24, 2014.

[66] Franz-Stefan Gady, "What Would Cyber-War with Syria Look Like?" *World Report* (blog), *U.S. News and World Report*, September 13, 2013.

[67] Ibid.

[68] Shaun Waterman, "Obama Hit Pause on U.S. Action in Face of Crippling Cyber Strikes from Syria, Iran," *Washington Times*, August 28, 2013.

of the three have reached a threshold that requires the full spectrum of their cyber operations capability. Why not? Cyber attack against Syrian infrastructure would have devastating impacts on both the civilian population as well as the government and would likely result in international condemnation and possible retaliation.

For destructive cyber capabilities to be displayed, the practitioner would have to be able to defend or absorb a destructive cyber counterattack (blowback) as well as defend a coincident attack in other warfare domains, specifically the conventional domain. If the practitioner is willing to accept those risks, then evidence of destructive cyber capabilities is likely to be observed, which is likely to happen only when the existence of a state is at risk.

Preemptive or reactive targeting of cyber operators in the physical world may become the next step in the evolution of cyber operations. News agencies such as The Telegraph (United Kingdom) reported that members of the Iranian Cyber War Headquarters, the cyber element of the Iranian Revolutionary Guard Corps, assisted the SEA with some of its attacks. In an interesting development, the Israeli Mossad was accused of assassinating Mojtaba Ahmadi, commander of the Iranian Cyber War Headquarters, in October 2013.[69] If true, this targeted killing of an Iranian official would be the latest in a series of Mossad-sponsored assassinations conducted in Iran. Five scientists tied to the Iranian nuclear enrichment program have been killed in Iran since 2007. Those assassinations were likely an overt attempt to slow the pace of the Iranian nuclear program. There are some differences in the circumstances surrounding the killings, however. The nuclear scientists were killed by explosive devices magnetically attached to vehicles they occupied.[70] Mojtaba Ahmadi was killed by gunshots to the chest from two individuals on motorbikes.[71] The fact that an accused cyberwarrior would have the same gravitas as a nuclear scientist and therefore warrant assassination for his actions in the cyber domain represents an unprecedented next step in the advancement of cybersecurity.

The potential unintended consequences of using assassination as a response to cyber attack are significant. Assassination is not proportional to any observed offensive cyber actions that have originated from Syria, even with alleged Iranian support. Assassination as a result of cyber action or to prevent future cyber attack can lead to dangerous retaliation. Can a nation assassinate a cyber actor because of his or her network activities with respect to espionage, or is it merely a threat to critical infrastructure that warrants death? Clearly, there is much left to interpretation on the part of the aggressor who chooses assassination to deter or retaliate against a cyber threat.

Conclusion

The cyber element of the Syrian civil war has had a more important role than one might have expected. Those who study cyber operations and their role in conflict, like any other aspect of the use of power, are bound to learn from their studies; those who choose to ignore the lessons learned are likely to suffer the consequences.

While international norms are still being established for the applicability of cyber operations as an element of national power, a state may choose to limit its use to those actions that are defensible in the court of world opinion. Despite the secrecy and ambiguity associated with the domain, one must act with the

[69] Damien McElroy and Ahmad Vahdat, "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination," *Telegraph*, October 2, 2013.

[70] Patrick Cockburn, "Just Who Has Been Killing Iran's Nuclear Scientists?" *Independent*, October 6, 2013.

[71] McElroy and Vahdat, "Iranian Cyber Warfare Commander Shot Dead."

assumption that operations will be exposed, and involvement in those operations may be proven.

One should consider potential proportional retaliation in any domain a possible consequence of cyber operations. On one extreme, the Israelis seem to have taken to preemptive action in the physical domain to prevent future cyber attacks. On the other extreme, absorbing nuisance attacks and building better defenses is the norm for the United States. The United States has yet to set precedent for a response to a more significant cyber attack. It is unlikely that the world will observe the most destructive capabilities of cyber attack unless the existence of that nation-state is at stake. In the meantime, the world will observe a constant cyber "arms race" in which nation-states try to increase their capabilities of cyber attack, exploitation, and espionage, as well as their cybersecurity capability to defend against those very same operations. If a country with limited cyber capabilities such as Syria is in this arms race, expectations will grow that anyone can, and will, be involved in the future.

Bibliography

AhlulBayt News Agency (ABNA). "Syrian Electronic Army Hacks Israel's Main Infrastructure Control System (SCADA)," May 8, 2013. Available at *Pakistan Defence*, http://defence.pk/threads/syrian-electronic-army-hacks-israels-main-infrastructure-control-system.251234/.

Albanesius, Chloe. "Tango Messaging App Targeted by Syrian Electronic Army." *PCMag*, July 23, 2013. http://www.pcmag.com/article2/0,2817,2422129,00.asp.

Al Jazeera and Agencies. "Obama Delays Military Action against Syria." September 1, 2013. http://www.aljazeera.com/news/middleeast/2013/08/2013831163130308715.html.

Alterman, Jon B. *New Media New Politics? From Satellite Television to the Internet in the Arab World*. Washington, DC: The Washington Institute for Near East Policy, 1998. http://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyPaper48.pdf.

Article 34, Statute of the International Court of Justice. http://www.icj-cij.org/documents/?p1=4&p2=2.

Ashford, Warwick. "Syrian Hacktivists Hit Second Mobile App in a Week." *Computer Weekly*, July 24, 2013. http://www.computerweekly.com/news/2240201656/Syrian-hacktvists-hit-second-mobile-app-in-a-week.

Associated Press. "Syria Admits to Shooting Down Turkish Fighter Jet." *CBC News*, June 22, 2012. http://www.cbc.ca/news/world/syria-admits-to-shooting-down-turkish-fighter-jet-1.1168588.

Bacon, John. "Pro-Syrian Group Hacks U.S. Marine Corps Website." *Marine Corps Times*, September 2, 2013. http://www.marinecorpstimes.com/article/20130902/NEWS08/309020019/Pro-Syrian-group-hacks-U-S-Marine-Corps-website.

BBC News. "Syria Crisis: Guide to Armed and Political Opposition." December 13, 2013. http://www.bbc.com/news/world-middle-east-24403003.

Bennett, Cory. "Syrian Electronic Army Comes after U.S. Military." *FedScoop*, September 3, 2013. http://fedscoop.com/syrian-electronic-army-comes-after-us-military/.

Ben Zion, Ilan. "Hacking Assad…as Easy as 1,2,3,4." *Times of Israel*, September 6, 2012. http://www.timesofisrael.com/hackers-thought-like-idiots-and-broke-into-assads-email/.

Berki, Eleni, and Mikko Jäkälä. "Cyber-Identities and Social Life in Cyberspace." In *Social Computing: Concepts, Methodologies, Tools, and Applications*, edited by Subhasish Dasgupta, 92–104. Hershey, PA: IGI Global, 2010.

Blanchard, Christopher, Carla Humud, and Mary Beth Nikitin. "Armed Conflict in Syria: Overview and U.S. Response." Washington, DC: Congressional Research Service, January 14, 2014. https://www.fas.org/sgp/crs/mideast/RL33487.pdf.

Booth, Robert, Mona Mahmood, and Luke Harding. "Exclusive: Secret Assad Emails Lift Lid on Life of Leader's Inner Circle." *Guardian*, March 14, 2013. http://www.theguardian.com/world/2012/mar/14/assad-emails-lift-lid-inner-circle/print.

Bratu, Becky. "UN Confirms Chemical Weapons Were Used in Syria, Repeatedly." *NBC News*, December 12, 2013. http://worldnews.nbcnews.com/_news/2013/12/12/21881407-un-confirms-chemical-weapons-were-used-in-syria-repeatedly.

Brumfield, Ben. "U.S. Troops Arrive in Turkey; Rebels Battle for Airport in Syria." *CNN*, January 4, 2013. http://www.cnn.com/2013/01/04/world/meast/syria-civil-war/.

Carroll, Ward. "Israel's Cyber Shot at Syria." *Defense Tech*, November 26, 2007. http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria/.

CBC News. "Syria's Civil War: Key Facts, Important Players." April 3, 2014. http://www.cbc.ca/news2/interactives/syria-dashboard/.

Chatriwala, Omar. "Updated: Syrian Electronic Army Takes Down Most Major Qatar Websites." *Doha News*, October 19, 2013. http://dohanews.co/syrian-electronic-army-takes-down-most-major-qatar-websites/.

Cockburn, Patrick. "Just Who Has Been Killing Iran's Nuclear Scientists?" *Independent*, October 6, 2013. http://www.independent.co.uk/voices/comment/just-who-has-been-killing-irans-nuclear-scientists-8861232.html.

Coker, Margaret, and Valentino-Devries Jennifer. "U.S. Firm's Monitoring Gear Seen Aiding Syria." *Wall Street Journal*, May 24, 2013. http://online.wsj.com/article/SB10001424127887323336104578503292583322474.html#mjDropdown.

Cullinane, Susannah. "OPCW Approves Road Map for Syria Chemical Weapons Destruction." *CNN*, November 16, 2013. http://www.cnn.com/2013/11/16/world/meast/syria-opcw-roadmap/.

Cybersecurity: The Digital Arms Trade." *Economist*, March 30, 2013. http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade.

Department of Defense, Defense Science Board. *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

Department of State, Office of the Spokesperson. "U.S. Government Assistance to Syria—Fact Sheet." September 7, 2013. http://www.state.gov/r/pa/prs/ps/2013/09/213927.htm.

Department of Treasury. "Frequently Asked Questions and Answers." http://www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx.

Department of Treasury, Office of Foreign Asset Control (OFAC). "Syria Sanctions Program." Washington, DC: Office of Foreign Asset Control (OFAC), August 2, 2013. http://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria.pdf.

Dwyer, Mimi. "Think Bashar al Assad Is Brutal? Meet His Family." *New Republic*, September 8, 2013. http://www.newrepublic.com/article/114630/bashar-al-assad-syria-family-guide.

Evans, Dominic, and Oliver Holmes. "Israel Strikes Syria, Says Targeting Hezbollah Arms." *Reuters*, May 5, 2013. http://www.reuters.com/article/2013/05/05/us-syria-crisis-blasts-idUSBRE94400020130505.

Fox, Zoe. "Anonymous Hacks Syrian President's Email. The Password: 12345" *Mashable*, February 7, 2012. http://mashable.com/2012/02/07/anonymous-assad-email-password/.

Fulghum, David. "Why Syria's Air Defenses Failed to Detect Israelis." Originally posted on *Ares*, an *Aviation Week* blog, October 3, 2007. Available at *Strategy Page*, http://www.strategypage.com/militaryforums/512-40367.aspx#startofcomments.

Gady, Franz-Stefan. "Syria: Preparing for the Cyber Threat." *National Interest*, September 5, 2013. http://nationalinterest.org/commentary/syria-preparing-the-cyber-threat-8997.

———. "What Would Cyber-War with Syria Look Like?" *World Report* (blog), *U.S. News and World Report*, September 13, 2013. http://www.usnews.com/opinion/blogs/world-report/2013/09/13/what-the-spanish-civil-war-tells-us-about-syria-and-cyber-attacks.

Gasparre, Richard B. "The Israeli 'E-tack' on Syria – Part II." *AirForce-Technology*, March 11, 2008. http://www.airforce-technology.com/features/feature1669.

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks*. Milpitas, CA: FireEye, 2014. http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

Goodarzi, Jubin. "Iran and Syria." *The Iran Primer*. United States Institute of Peace website. Accessed February 6, 2014. http://iranprimer.usip.org/resource/iran-and-syria.

Harding, Luke, and Charles Arthur. "Syrian Electronic Army: Assad's Cyber Warriors." *Guardian*, April 29, 2013. http://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background.

Holland, Steve. "U.S. to Keep 1,500 Troops in Jordan for Time Being." *Reuters*, December 13, 2013. http://www.reuters.com/article/2013/12/13/us-usa-troops-jordan-idUSBRE9BC0XX20131213.

Howell, Martin. "Reuters Twitter Account Hacked, False Tweets about Syria Sent." *Reuters*, August 5, 2012. http://www.reuters.com/article/2012/08/06/net-us-reuters-syria-hacking-idUSBRE8721B420120806.

IHS Jane's Defence Weekly. "Islamic Front Gains Reduce U.S. Options in Syria, Further Undermine Prospects for Upcoming Geneva II Summit." December 12, 2013. http://www.ihs.com/products/Global-Insight/industry-economic-report.aspx?ID=1065984918.

Information Warfare Monitor. "Syrian Electronic Army: Disruptive Attacks and Hyped Targets." June 25, 2011. http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/.

———. "Syrian Electronic Army Defaces 41 Web Sites, One UK Government Web Site." June 29, 2011. http://www.infowar-monitor.net/2011/06/syrian-electronic-army-defaces-41-web-sites-one-uk-government-web-site/.

International Committee of the Red Cross. "Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction Geneva, Paris 13 January 1993." https://www.icrc.org/ihl/INTRO/553?OpenDocument.

———. "Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. Geneva, 17 June 1925." https://www.icrc.org/ihl/INTRO/280?OpenDocument.

Internet World Stats. "Internet Usage Population and Telecom Reports for the Americas." http://www.internetworldstats.com/stats2.htm.

———. "Syria Internet Usage, Broadband and Telecommunications Report." http://internetworldstats.com/me/sy.htm.

Isaacson, Betsy. "Hackers Reveal How They Accessed Syrian President Bashar Assad's Emails Using World's Worst Password." *Huffington Post*, September 7, 2012. http://www.huffingtonpost.com/2012/09/07/assad-syria-worlds-worst-password-anonymous-hack_n_1863462.html?view=print&comm_ref=false.

Johnson, Chalmers. "Blowback." *The Nation*, October 15, 2001. http://www.thenation.com/article/blowback#.

Joubert, Vincent. *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?* NDC Research Paper 76. NATO Defense College Research Division, May 2012. http://www.ndc.nato.int/news/current_news.php?icode=394.

Karam, Zeina. "Syria's Civil War Plays Out on Social Media." *Denver Post*, October 20, 2013. http://www.denverpost.com/nationworld/ci_24347121/syrias-civil-war-plays-out-social-media.

Keys, Matthew. "Syrian Electronic Army Denies Cyber Attack on Hockey Forum." *The Desk*, September 9, 2013. http://thedesk.matthewkeys.net/2013/09/09/syrian-electronic-army-denies-attack-on-hockey-forum/.

Khare, Anupika. "Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts." *iDigital Times*, July 19, 2013. http://www.idigitaltimes.co.uk/articles/492337/20130719/syrian-electronic-army-hacks-truecaller-database-gains.htm.

Krebs, Brian. "Trade Sanctions Cited in Hundreds of Syrian Domain Name Seizures." *Krebs on Security*, May 8, 2013. http://krebsonsecurity.com/2013/05/trade-sanctions-cited-in-hundreds-of-syrian-domain-seizures/.

Libicki, Martin. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

———. *Managing September 12th in Cyberspace*. Santa Monica: RAND Corporation, March 21, 2013. http://www.rand.org/pubs/testimonies/CT384.html.

Lynch, Marc. "How Syria Ruined the Arab Spring." *Foreign Policy*, May 2, 2013. http://www.foreignpolicy.com/articles/2013/05/03/how_syria_ruined_the_arab_spring?print=yes&hidecomments=yes&page=full.

McElroy, Damien. "Saudi Arabia Warns It Will Act against West's Policy in Middle East." *Telegraph*, December 18, 2013. http://www.telegraph.co.uk/news/worldnews/middleeast/saudiarabia/10524721/Saudi-Arabia-warns-it-will-act-against-Wests-policy-in-Middle-East.html.

McElroy, Damien, and Ahmad Vahdat. "Iranian Cyber Warfare Commander Shot Dead in Suspected Assassination." *Telegraph*, October 2, 2013. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/10350285/Iranian-cyber-warfare-commander-shot-dead-in-suspected-assassination.html.

Merrigan, Tara. "Harvard's Website Hacked by 'Syrian Electronic Army.'" *Harvard Crimson*, September 26, 2011. http://www.thecrimson.com/article/2011/9/26/syrian-group-syria-video/.

Messieh, Nancy. "Hackers Take Down Official LinkedIn Blog for 'Spreading Lies About Syria.'" *The Next Web*, April 26, 2012. http://thenextweb.com/me/2012/04/26/hackers-take-down-official-linkedin-blog-for-spreading-lies-about-syria/#!qcK4S.

Microsoft Developer Network. "Public Key Infrastructure." Accessed January 27, 2014. http://msdn.microsoft.com/en-us/library/windows/desktop/bb427432(v=vs.85).aspx.

Mims, Christopher. "How The Syrian Electronic Army Hacked the AP—And Who Are These Guys Anyway?" *Quartz*, April 23, 2013. http://qz.com/77464/how-the-syrian-electronic-army-hacked-the-ap-and-who-are-these-guys-anyway/.

Moussa, Ihsan, interviewed by Jihad Yazigi. "The Syrian Computer Society at the Heart of Syria's IT Sector." *The Syria Report*, April 2002. http://www.mafhoum.com/press3/98T44.htm.

Obama, Barack. "President Obama Addresses the Nation on Syria." September 10, 2013. Video available at http://www.whitehouse.gov/issues/foreign-policy/syria?utm_m.

———. "President Obama Speaks on Syria." September 1, 2013. Video available at http://www.whitehouse.gov/issues/foreign-policy/syria?utm_m.

Oweis, Khaled Yacoub. "Syria Expands 'Iron Censorship' over Internet." *Reuters*, March 13, 2008. http://uk.reuters.com/article/internetNews/idUKL138353620080313?sp=true.

Perez, Evan. "U.S. Beefs Up Security Measures before Possible Military Strike on Syria." *CNN*, September 1, 2013. http://www.cnn.com/2013/08/31/us/us-syria-cyber-attacks/index.html.

Perlroth, Nicole. "Hunting for Syrian Hackers Chain of Command." *New York Times*, May 18, 2013. http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html?pagewanted%3Dall&_r=0.

Peterson, Andrea. "Here's How One Hacker Is Waging War on the Syrian Government." *The Switch* (blog), *Washington Post*, August 28, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/28/heres-how-one-hacker-is-waging-war-on-the-syrian-government//?print=1.

Rafizadeh, Majid. "Assad's Family: The Unrecognized Nuances and the Politics." *Huffington Post*, May 13, 2013. http://www.huffingtonpost.com/majid-rafizadeh/assads-family-the-unrecog_b_3152404.html?view=print&comm_ref=false.

Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst/Oxford University Press, 2013.

Salomons, Elad. "Did the Syrian Electronic Army Attack Haifa's Water Supply SCADA System?" *Water Simulation*, June 5, 2013. http://www.water-simulation.com/wsp/2013/06/05/did-the-syrian-electronic-army-attack-haifas-water-supply-scada-system/.

Sanger, David, and Eric Schmitt. "Syria War Stirs New U.S. Debate on Cyberattacks." *New York Times*, February 24, 2014. http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html?_r=0.

Scharr, Jillian. "What Is the Syrian Electronic Army?" *Tom's Guide*, August 29, 2013. http://www.tomsguide.com/us/what-is-syrian-electronic-army,news-17472.html#what-is-syrian-electronic-army%2Cnews-17472.html?&_suid=138444207537307304943396805894.

Schmitt, Michael N. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts." In *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, 151–178. Washington, DC: National Research Council, 2010.

Schwartz, Matthew. "FBI Warns of Syrian Electronic Army Hacking Threat." *Information Week*, September 6, 2013. http://www.informationweek.com/attacks/fbi-warns-of-syrian-electronic-army-hacking-threat/d/d-id/1111444?.

Sterling, Bruce. "Syrian Electronic Army Invades University of California Los Angeles." *Wired*, July 6, 2011. http://www.wired.com/beyond_the_beyond/2011/07/syrian-electronic-army-invades-university-of-california-los-angeles.

Stecklow, Steve. "Dubai Firm Agrees $2.8 Million Fine over Syria Sanctions-Busting." *Reuters*, April 25, 2013. http://www.reuters.com/article/2013/04/25/syria-sanctions-fine-idUSL6N0DC3PT20130425.

———. "Dubai Firm Fined $2.8 Million for Shipping Blue Coat Monitoring Gear to Syria." *Reuters*, April 25, 2013. http://www.reuters.com/article/2013/04/25/us-syria-sanctions-fine-idUSBRE93O11X20130425.

Stone, Michael. "Anonymous Hacks Syrian Electronic Army: Operation Syria Engaged." *Examiner.com*, September 2, 2013. http://www.examiner.com/article/anonymous-hacks-syrian-electronic-army-operation-syria-engaged.

TRADOC G-2 Intelligence Support Activity. *Syrian Electronic Army (SEA) Targets Qatar*. Published by Matthew Keys, November 26, 2013. http://www.scribd.com/doc/187378871/US-Army-Doc-on-Syrian-Electronic-Army.

United Nations. "Security Council Establishes UN Supervision Mission in Syria, with 300 Observers to Monitor Cessation of Violence, Implementation of Special Envoy's Plan." April 21, 2012. http://www.un.org/News/Press/docs/2012/sc10618.doc.htm.

———. "Security Council Requires Scheduled Destruction of Syria's Chemical Weapons, Unanimously Adopting Resolution 2118 (2013)." September 27, 2013. http://www.un.org/News/Press/docs/2013/sc11135.doc.htm.

———. "Security Council Unanimously Adopts Resolution 2042 (2012), Authorizing Advance Team to Monitor Ceasefire in Syria." April 14, 2012. http://www.un.org/News/Press/docs/2012/sc10609.doc.htm.

———. *Action Group for Syria Final Communiqué*. Geneva: United Nations, June 30, 2013. http://www.un.org/News/dh/infocus/Syria/FinalCommuniqueActionGroupforSyria.pdf.

Valentino-DeVries, Jennifer, Paul Sonne, and Nour Malas. "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web." *Wall Street Journal*, October 29, 2011. http://online.wsj.com/news/articles/SB10001424052970203687504577001911398596328.

Valeriano, Brandon, and Ryan Maness. "The Fog of Cyberwar, Why the Threat Doesn't Live Up to the Hype." *Foreign Affairs*, November 21, 2012. http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar.

Vigna, Paul. "Stocks Plunge, Quickly Recover, on Fake Tweet." *MoneyBeat* (blog), *Wall Street Journal*, April 23, 2013. http://blogs.wsj.com/moneybeat/2013/04/23/stocks-plunge-quickly-recover-on-fake-tweet/.

Vinograd, Cassandra. "Syria Rebels: Islamic Militants Nabbed Our Weapons." *Associated Press*, December 13, 2013. http://bigstory.ap.org/article/syrian-rebels-islamists-welcome-peace-talks.

Wansink, Kylie. *Syria—Telecoms, Mobile, Broadband and Forecasts*. New South Wales, Australia: BuddeComm, 2014. http://www.budde.com.au/buddereports/1168/Syria_-_Telecoms_Market_Overview__Statistics.aspx?r=51.

Waterman, Shaun. "Obama Hits Pause on U.S. Action in Face of Crippling Cyber Strikes from Syria, Iran." *Washington Times*, August 28, 2013. http://www.washingtontimes.com/news/2013/aug/28/syria-iran-capable-of-launching-a-cyberwar/print/.

Windrem, Robert. "Syrian Electronic Army Seen as a 'Nuisance' Not a Serious Cyber Threat." *NBC News*, October 8, 2013. http://investigations.nbcnews.com/_news/2013/08/30/20250021-syrian-electronic-army-seen-as-nuisance-not-a-serious-cyberthreat?lite.

Acknowledgments

The writing of this paper would not have been possible without the help and guidance of James Scouras; he initially chose the topic and has guided writing efforts throughout the entire process. Several people have also taken the time to review the paper and provide significant feedback: Antonio DeSimone, Timothy Evans, Christine Fox, Susan Lee, Mark Lewellyn, Thomas Mahnken, Peter Nanos, and Edward Smyth.

About the Author

Captain Edwin J. Grohe, a native of Milford, Connecticut, graduated from the United States Naval Academy in 1993 with a bachelor of science in aerospace engineering. He was designated a naval aviator in November 1995 and joined the Electronic Attack community as an EA-6B pilot. As a junior officer, Captain Grohe completed operational tours assigned to VAQ-137, VAQ-135, and USS *Abraham Lincoln* (CVN-72), deploying multiple times in support of Operations Southern Watch, Iraqi Freedom, and Enduring Freedom. He also completed a tour as an instructor pilot at the Fleet Replacement Squadron (VAQ-129). Captain Grohe commanded VAQ-142 from 2012 to 2013. Under his leadership, the squadron earned the 2013 Battle Efficiency Award, the 2013 Arleigh Burke Trophy for Pacific Fleet, and the 2012 "Golden Wrench" for the best maintenance department in the Electronic Attack Wing. Captain Grohe also served as the deputy chief of future operations at US Cyber Command and led a joint-interagency operational planning team of consisting of twenty-seven US agencies and two key partner nations. In August 2013, Captain Grohe was selected as a federal executive fellow to the Johns Hopkins University Applied Physics Laboratory. He is currently assigned to the staff of the US 6th Fleet. His awards include the Defense Meritorious Service Medal, the Meritorious Service Medal, the Air Medal (four strike-flight awards), the Joint Service Commendation Medal, the Navy and Marine Corps Commendation Medal (three awards), the Navy and Marine Corps Achievement Medal (two awards), and various unit and campaign awards.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY