The Middle East's Cyber Power: How Syria's cyber war asphyxiated Civil Society Organizations' efforts against the Assad regime

Vinicius Gorczeski

Centre for Social Sciences, email: vinicius.gorczeski@tk.mta.hu: +36.1.2246700/5213

Abstract This paper analyzes the Syrian government's cyber strategy to crack down on activists that have started operating in cyberspace since the civil war broke out in 2011. The analytical exercise is done though the lenses of the geopolitics of the Internet and international relations. Focus is placed on Iran and Russia's participation in aiding the Syrian regime to control narratives of the conflict through disseminating fake news and propaganda. Such strategy has undermined global actors' understanding of the conflict. Grounded on the potential negative policy implications of that strategy, this paper proposes policy recommendations that think tanks, humanitarian organizations, and other international non-governmental actors and local grassroots can adopt together. The objective is to discuss tools that can bypass and overcome state control of cyberspace in closed regimes in order to ensure that accurate information flows among key actors involved in shedding light on, and responding to, an obscure conflict.

Keywords Syrian Civil War, Middle East, Iran, Russia, Cyberspace, Journalism, Social Media, Fake News, Disinformation Campaign, censorship, cyber crime

Date April 2018

Table of Contents

Introduction

At the early stage of the civil uprising against the regime of Bashar Al-Assad in Syria, in 2011, the activist Rami Jarrah joined the crowd and started filming the protests on the streets that soon faced the government's response: violence, killings, and detentions for those involved.[1] The Syrian Internet, previously quite slow and unstable, suddenly became faster and more reliable after the outbreak, Jarrah told Al Jazeera.[2] He said the regime learned the power offered by cyberspace as a counter-insurgency tool: he was detained for three days and tortured by government forces. The first question in the interrogation concerned his cyber activities: his contacts on Facebook were demanded, as well as the IPs from where his account on social media had been accessed. The strategy of using cyberspace to chase down activists against the regime became a mark of the Syrian war.[3]

This essay aims to explain how the Syrian government has used, directly or indirectly, cyberspace with the goal of remaining in power. Cyberspace here is understood as a domain consisting of the "interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] Assad's cyber strategy took advantage of hacktivist groups like the Syrian Electronic Army (SEA), with which the regime has a convenient, informal connection, to perpetrate cyber-attacks against his opponents.[5] Although there is no consensus on a definition,

[1] Ruhfus, Juliana. "Syria's Electronic Armies." Accessed April 11, 2018. https://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html.
[2] Ibid.
[3] Baiazy, Amjad. "Syria's Cyber Wars," January 6, 2012. http://www.academia.edu/3555530/Syria_Cyber_Wars.
[4] JP 1-02, 141, **quoted in** Schott W. Beidleman, "Defining and Deterring Cyber War" (U.S. Army War College, 2009), http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf.
[5] Stewart Bertram, "'Close Enough' – The Link between the Syrian Electronic Army and the Bashar Al-Assad Regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies," Contemporary Voices: St Andrews Journal of International Relations 8, no. 1 (February 8, 2017), https://doi.org/10.15664/jtr.1294.

cyber-attacks here are understood as attempts "to use the internet or advanced computer technology to harm the fundamental interests of a political community substantially".[6] Ultimately, the Syrian regime's strategy hampered international efforts to support grassroots organizations working to build up a stronger civil society. What's worse, the cyber strategy helped asphyxiate Civil Society Organizations (CSOs) and other activists, preventing them from better coordinating opposition efforts.[7]

Later, this essay hints upon Assad's cyber strategy as being supported by and similar to his international allies in the conflict. First, Iran is known for having trained cyber activists in Syria, although no proof has been collected since the nature of cyber conflict allows for protecting perpetrators' identities and the way they coordinate.[8] Second, Syria's cyber strategy resembles Russia's policy of shaping regional political events by favoring cyber hacktivists with whom it has mutual interests, examples of victims being Georgia, Ukraine, and Estonia.[9]

The Assad regime emits signals that it has learned from Russia on how to do the same, with nefarious implications for future conflicts that spill into the cyber realm. The misuse of cyberspace in the current Syrian war can become a blueprint for future conflicts — especially authoritarian regimes backed up by cyber powers that may eventually face a democratic uprising.

A legal framework defining cyberwar, cyber-attacks, and cyberspace under international law would help counter issues deriving from any sort of cyber-conflict (such as enabling international actors to hold states accountable for cyber-attacks, which includes the

[6] Orend, B. (2014). Fog in the Fifth Dimension: The Ethics of Cyber-War. In L. Floridi, & M. Taddeo (Eds.), The Ethics of Information Warfare (pp. 3-24). New York: Springer International Publishing Switzerland, **quoted in** Deegan, Arthur, Yasir Kalid, Michelle Kingue, and Aldo Taboada. "Cyber-Ia: The Ethical Considerations Behind Syria's Cyber-War | Small Wars Journal," 2017, http://smallwarsjournal.com/jrnl/art/cyber-ia-the-ethical-considerations-behind-syria%E2%80%99s-cyber-war.
[7] Ahmed K. Al-Rawi, "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army," Public Relations Review 40, no. 3 (September 1, 2014): 420–28, https://doi.org/10.1016/j.pubrev.2014.04.005.
[8] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," Comparative Strategy 34, no. 2 (March 15, 2015): 133–48, https://doi.org/10.1080/01495933.2015.1017342.
[9] Jeffrey Carr, "The Role of Cyber in Military Doctrine," in Inside Cyber Warfare (O'Reilly Media, Inc., 2009).

current conflict in Syria), but efforts toward that goal seem to be distant.[10] However, even if that occurs, the granular and convenient relationship between states and cyber hacktivists would render the challenges of identifying perpetrators that could respond to their acts almost impenetrable.

In light of such issues, policy recommendations will be given to international organizations. They should focus on cyber protection regardless of their field of activity, in Syria or elsewhere. The use of cyberspace as a warfare tool can become a trend in future conflicts, especially those where societies stand against authoritarian regimes.

The Syrian cyber strategy and its victims

The Internet and social media were largely used as a platform for activists in Tunisia and Egypt to organize protests against their governments.[11] Both countries shut down the Internet to contain such oppositions, but that did not impede both uprisings from overthrowing the respective regimes.[12] In Syria, the opposite happened. Facebook, prohibited in the country until shortly before the revolution, remained opened.[13] The Syrian move was soon understood by activists as a part of a broader political objective — by allowing activists to keep accessing the Internet, the regime could use cyberspace as a way of cracking down on opponents, as previously mentioned. Internet in Syria was already under surveillance by the regime when the

[10] Beidleman, Schott W. "Defining and Deterring Cyber War." U.S. Army War College, 2009. http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf.
[11] Shehabat, Ahmad. "The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 201," n.d., 9.
[12] Ibid.
[13] Ibid.

uprising broke out, through filtering techniques to block users from accessing content related to politics, security, or social issues.[14] The country has twelve Internet providers, controlled by the Syrian Telecommunications Establishment (STE), a state-owned company, according to a study.[15] It became easy for the government to use the Internet for its own purposes, with the deployment of a system to control and monitor communications between activities through exchanged messages.[16]

A great part of this strategy was conducted not directly by the government, but by a third-party to the conflict, the pro-regime hacktivist group SEA. Four other main groups joined the pro-government efforts against the opposition since then, but what distinguishes the SEA from the others is the level of sophistication adopted in their acts: from 2011 and 2015, hundreds of distributed denial of service attacks (DDoS), malware, and spear phishing emails were systematically used to crack down on anyone against the Syrian government.[17] The group's most notable international attack was the defacement of the Associated Press Twitter account, in which a tweet stated that bombs at the White House had injured then-president Barack Obama, leaving the Dow Jones with a loss of USD 136 billion in minutes.[18] The American Federal Bureau of Investigation (FBI) has added two hackers from the group to its list of most wanted, for having provided "support to the Assad regime" and, therefore, for damaging the American "national security".[19]

Because of their pro-government efforts on cyberspace, suspicion was raised that the SEA was connected to Assad, especially when the latter thanked the role of cyber counter-

[14] Deibert, Ronald J. "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace," n.d. http://www.handbook-of-internet-politics.com/pdfs/chapter_23.pdf.
[15] Patrice Robin and Marie Baezner, "The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict" (ETH Zurich, 2017), https://doi.org/10.3929/ethz-b-000200662.
[16] Ibid.
[17] Ibid.
[18] Gross, Michael Joseph. "Silent War." Vanity Fair, 2013. https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business.
[19] "Two From 'Syrian Electronic Army' Added to Cyber's Most Wanted," Story, Federal Bureau of Investigation, accessed April 12, 2018, https://www.fbi.gov/news/stories/two-from-syrian-electronic-army-added-to-cybers-most-wanted.

revolutionaries publicly.[20] The relationship between the group and the government is still dubious. A study in which the author interviewed members of the group found that Damascus had given money to SEA hacktivists.[21] In another study, Bertram analyzed data related to the SEA's activities and found that the SEA was conveniently close to the government.[22] According to him, the SEA was distant from Assad to the point that the latter could avoid responsibility of cyber-attacks coming from the group; but it was close enough that the regime enjoyed the benefits of having a cyber army fighting for its political stability. The advantage from the nature of this relationship comes from the almost impossibility to identify the perpetrators of cyberattacks.[23]

The government simply turned a blind eye to the SEA's activities while it persecuted opponents in cyberspace.[24] The SEA's websites were hosted under the Syrian Computer Society — a pro-Assad branch, which provides, among others, access to the Internet to the SEA.[25] Bertram raised the fact that the regime could block contents on YouTube and Facebook, but SEA's content remained untouched, which leaves the suspicion that the regime was aware of the group's activities but did nothing to block them. The regime's silence, says Bertram, "speaks volumes" in this case.

The author also analyzed emails leaked by the WikiLeaks under the Syria files in 2012, and found that members of the SEA were directly connected to key governmental media

[20] Ruhfus, Juliana. "Syria's Electronic Armies." Accessed April 11, 2018. https://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html.
[21] Amjad Baiazy, "Syria's Cyber Wars," January 6, 2012, http://www.academia.edu/3555530/Syria_Cyber_Wars.
[22] Stewart Bertram, "'Close Enough' – The Link between the Syrian Electronic Army and the Bashar Al-Assad Regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies," Contemporary Voices: St Andrews Journal of International Relations 8, no. 1 (February 8, 2017), https://doi.org/10.15664/jtr.1294.
[23] Schott W. Beidleman, "Defining and Deterring Cyber War" (U.S. Army War College, 2009), http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf.
[24] Stewart Bertram, "'Close Enough' – The Link between the Syrian Electronic Army and the Bashar Al-Assad Regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies," Contemporary Voices: St Andrews Journal of International Relations 8, no. 1 (February 8, 2017), https://doi.org/10.15664/jtr.1294.
[25] Ibid.

interlocutors, three degrees below the regime's chief in hierarchy. 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.[26] Despite the impossibility to affirm whether this relationship is deliberate, the SEA has given Assad benefits — a supporter in cyberspace, and the possibility that this support promotes illegal activities that the state itself wouldn't be able to do openly.

The Syrian cyber strategy has effectively hampered civil society organizations' ability to coordinate with each other. Dayoub, an interviewee from a Syrian grassroots organization operating in Istanbul, said that at the beginning of the revolution the task of coordinating and mapping potential allies via the Internet was almost impossible: it took him more than three years to learn how to codify messages and use alternative Internet providers for those purposes.[27] "We finally professionalized the way of communicating on Facebook", Dayoub said about those strategies that happened to be studied by other authors.[28] Cyber-surveillance was one among other relevant reasons why activists moved to Turkey in 2015 — four years after the uprising, enough time for the government to establish a strong anti-opposition campaign with the help of cyber warfare.

That lagged the process of mapping allies doing similar jobs in Syria and of establishing networks with international organizations as well. The controlled cyberspace and the impossibility to coordinate on the ground with people living in regime-controlled areas in Syria made many organizations fail to know what other grassroots groups were doing, Dayoub said. Activists could only safely operate — both in the physical and in the digital realms — in opposition-held areas; as long as the regime regained access to those areas, activists had to

[26] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," Comparative Strategy 34, no. 2 (March 15, 2015): 133–48, https://doi.org/10.1080/01495933.2015.1017342.
[27] Interview with Dayoub, a Syrian activist working on civil society building, 13 February 2018.
[28] Faris, Rob, Hal Roberts, Rebekah Heacock, Ethan Zuckerman, and Urs Gasser. "Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice," n.d., 18.
[28] Interview with Dabbagh, a Syrian working with a think tank in Syria, 14 February 2018.

evacuate and terminate their operations, said another interviewee working with an international organization in Syria.[29] These accounts help show how the Syrian government used cyberspace to support its military strategies on the ground. The asphyxia imposed on activists and international organizations through cyberspace, with the support of SEA, gave the regime a strategic advantage in the civil war.

Iran's and Russia's influence on the Syrian strategy

The effectiveness of the Syrian cyber strategy against opponents has been partly attributed to neighboring allies, like Russia and Iran.[30] Since the outbreak of the conflict, Iran has helped pro-Assad groups and militias not only with equipment but also with training, and money.[31] As the SEA's strategy in cyberspace became more sophisticated over time, evidence suggested that the hacktivists in Syria have also been assisted by Iran, through the latter's Cyber Army.[32] As the documentary Zero Days showed, Iran has built its cyber capabilities in response to Stuxnet.[33] With powerful interviews and secret sources from the National Security Agency in the US, the movie shows how Stuxnet, a powerful computer worm, was developed in a joint and covert operation between the American and Israeli intelligence agencies with the intent of physically destroying Iran's nuclear centrifuges in 2008, lagging the country's nuclear plans and helping Western countries buy time to impose sanctions on Iran. It was the first time a virus

[30] Robin, Patrice, and Marie Baezner. "The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict." ETH Zurich, 2017. https://doi.org/10.3929/ethz-b-000200662.
[31] Bryan Lee, "The Impact of Cyber Capabilities in the Syrian Civil War | Small Wars Journal," accessed April 11, 2018, http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war.
[32] Gross, Michael Joseph. "Silent War." Vanity Fair, 2013. https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business.
[33] Gibney, Alex. *Zero Days*. Documentary. Magnolia Pictures, 2016.

had such an impact.

The strategy failed to block Iran from advancing its nuclear capabilities and only offered a small strategic advance, as Zero Days has shown. Worse than that, Iran, apparently in revenge for Stuxnet, built up a cyber army, financed with $20 million, that today is known for being the fourth largest in the world.[34] The lessons depicted in the movie are startling. By having helped deploy Stuxnet against Iran, the US has indirectly helped create a cyber power that allegedly backs up the Syrian regime.

The Syrian cyber strategy is also remarkably similar to the one Russia has developed over the past decades. In 2007, when the Estonian authorities decided to move a statue that served as a memorial to the Soviet Red Army, the act was responded to by a massive cyber-attack that paralyzed the country's banking system and governmental bodies.[35] After the attacks, which lasted for weeks, few doubted that the Russian authorities weren't involved, since instructions to attack the Estonian government were made available in Russian and came from Russian IP addresses.[36] The similarity to the Syrian case is that no proof could be found directly associating Moscow with the cyber intrusion.[37] In 2008, Georgia would fall victim to a similarly orchestrated and organized cyber-attack that took place almost at the same time that Russia invaded the country, and Ukraine was also a victim of such cyber-attacks.[38] These cases are examples of how Russia uses cyber-attacks to shape political events; it avoids attributability by not acting to hold pro-government hacktivist groups accountable — or maybe even covertly supports them with resources.[39]

[34] Insider, Paul Szoldra, Business. "Iran Now Has One of the Largest Armies of Hackers in the World — and the US Is Partly to Blame." Business Insider. Accessed April 13, 2018. http://www.businessinsider.com/us-hacker-army-stuxnet-2016-7.
[35] McGuinness, Damien. "How a Cyber Attack Transformed Estonia." BBC News, April 27, 2017, sec. Europe. http://www.bbc.com/news/39655415.
[36] Ibid.
[37] Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," n.d., 11.
[38] Ibid.
[39] Ibid.

Russia's cyber strategy teaches that states can take advantage of proxy, non-state actors, overtly or covertly, to perform attacks in cyberspace that would otherwise be deniable.[40] They are already a reality because conflicts taking advantage of cyberspace are taking place with Russia's support. Availing themselves of the same kind of covert operations used under Stuxnet, Western opponents operating in Syria's orbit have been enjoying the fact that forces like NATO cannot do anything to respond to cyber-attacks because no one can say for sure they are behind them.[41] Such attacks originating in the East not only shape political landscapes in Eastern Europe and the Middle East, but could be ultimately directed at the West in case the US — or even Israel — take the risk of deploying another cyber weapon like Stuxnet or even in case they deepen their kinetic participation in the Syrian war.[42] The SEA in Syria has no such resources to attack Western infrastructures like Stuxnet did, but Russia and Iran could — and both are on the Syrian side.[43]

Jame's and Rohozinski's predicted that cyber weapons would object the goal of constraining adversaries' capacity to coordinate, maneuver, or synchronize and from shifting adversaries' focus in a war in the context of international cyber conflicts.[44] But reality shows that the masters of cyber weapons today can not only aim their codes at international bodies, but can transfer their know-how to authoritarian regimes — and the latter can turn them against their own people.

[40] Klimburg, Alexander. "Mobilising Cyber Power." Survival 53, no. 1 (February 2011): 41–60. https://doi.org/10.1080/00396338.2011.555595; and Andrew, James. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine," n.d., 11.
[41] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," Comparative Strategy 34, no. 2 (March 15, 2015): 133–48, https://doi.org/10.1080/01495933.2015.1017342.
[42] Ibid.
[43] Edwin Grohe, "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict," Comparative Strategy 34, no. 2 (March 15, 2015): 133–48, https://doi.org/10.1080/01495933.2015.1017342.
[44] Farwell, James P., and Rafal Rohozinski. "The New Reality of Cyber War." Survival 54, no. 4 (September 2012): 107–20. https://doi.org/10.1080/00396338.2012.709391.

Policy recommendations

Overcoming the implications of cyberattacks at the international level is challenging, as the documentary Zero Days has explored. There is no legal framework defining it internationally as previously noted. Although efforts must be taken to overcome this legal vacuum, so countries can be held accountable for attacks committed through cyberspace, any solid framework remains far from being designed and adopted by the international community.[45] As discussed before, the fact that states are using non-state actors to perpetrate cyberattacks against their external and internal enemies would render legal frameworks worthless even if they already existed. Proposing definitive solutions at the international level could be naïve. It would be more feasible if international non-state actors — such as donors, think tanks, or humanitarian organizations—, surveyed the digital environment in which they are operating to render collaboration, democratization, and humanitarian efforts between them and grassroots organizations to be more efficient and effective.

Therefore, policy recommendations will focus on those actors. A survey conducted in Syria and other countries in the Middle East in the wake of the Arab Spring showed that few activists knew how to protect themselves in the digital realm, in a moment where a high number of respondents were facing cyber-attacks, threats, arrests, and detentions because of their online activism.[46] Policies involving technological responses in a cyber conflict cannot be rendered as a "one-size-fit-all" model, since states like Syria can shift, tweak, and adapt their digital tools to overcome activists' security measures.[47] But some feasible (and non-exhaustive list of) policy ideas for Syria and future cyber conflicts could help and are numbered below:

[45] Deegan, Arthur, Yasir Kalid, Michelle Kingue, and Aldo Taboada. "Cyber-Ia: The Ethical Considerations Behind Syria's Cyber-War | Small Wars Journal," 2017, http://smallwarsjournal.com/jrnl/art/cyber-ia-the-ethical-considerations-behind-syria%E2%80%99s-cyber-war.
[46] Faris, Rob, Hal Roberts, Rebekah Heacock, Ethan Zuckerman, and Urs Gasser. "Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice," n.d., 18.
[47] Hal Roberts et al., "The Evolving Landscape of Internet Control," n.d., 12.

1) Offering security protection techniques, combined with the tutoring of a team of digital experts could improve the cyberspace landscape in places like Syria. They should be part of the scope of policies that international organizations deploy in war zones regardless of their field of work: be they involved in humanitarian work or in empowering civil society. This is particularly relevant in civil wars that have their cyberspaces under surveillance and that are used as a tool for warfare like Syria's. Rendering the digital-scape a safer environment allows civil society to better collaborate and coordinate against states' cyber reactions to cyber insurgencies.

2) International organizations can learn from the Syrian experience of working with diaspora communities and help local organizations build their own protected channels of communications with the outside world. The availability of a team of digital experts is key to assisting local grassroots groups on how to do that. They can help set a protected channel of communication where locals can coordinate support with other relevant actors — activists or international organizations — through the support of diasporas living outside the country. That can help avoid the risks arising from Internet control and improve coordination. The exercise of mapping diaspora communities outside war zones is a necessary step to make this policy more effective.

3) International organizations should permanently monitor cyberspace when working in conflict zones like Syria. Technical experts can help trace DDoS attacks and techniques deployed by hacktivists[48] — whether they work directly with governments or not, like the SEA in Syria — and therefore be more prepared to adjust digital responses to such attacks.

4) As part of the previous digital strategy, international organizations may work more closely with think thanks, NGOs, or companies working on Internet-related issues, like the OpenNet Initiative.[49] This would likely improve advocacy efforts for both international

[48] Ibid.
[49] "About ONI | OpenNet Initiative." Accessed April 15, 2018. https://opennet.net/about-oni.

organizations and the local grassroots groups with whom the former ones establish partnerships, through a policy of name and shame, while building up a solid documentation of attacks deployed and used in cyberspace by relevant parties to the conflict. By releasing that type of information, other networks may be aware of other organizations working on similar issues — and they will also learn how to overcome digital barriers or how to respond to attacks deployed against them.

References

"About ONI | OpenNet Initiative." Accessed April 15, 2018. https://opennet.net/about-oni.

Al-Rawi, Ahmed K. "Cyber Warriors in the Middle East: The Case of the Syrian Electronic Army." *Public Relations Review* 40, no. 3 (September 1, 2014): 420–28. https://doi.org/10.1016/j.pubrev.2014.04.005.

Andrew, James. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine," n.d., 11.

Antolin-Jenkins, Vida M. "Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places Articles, Essays & Notes." *Naval Law Review* 51 (2005): 132–74.

Baiazy, Amjad. "Syria's Cyber Wars," January 6, 2012. http://www.academia.edu/3555530/Syria_Cyber_Wars.

Beidleman, Schott W. "Defining and Deterring Cyber War." U.S. Army War College, 2009. http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf.

Bertram, Stewart. "'Close Enough' – The Link between the Syrian Electronic Army and the Bashar Al-Assad Regime, and Implications for the Future Development of Nation-State Cyber Counter-Insurgency Strategies." *Contemporary Voices: St Andrews Journal of International Relations* 8, no. 1 (February 8, 2017). https://doi.org/10.15664/jtr.1294.

Carr, Jeffrey. "The Role of Cyber in Military Doctrine." In *Inside Cyber Warfare*. O'Reilly Media, Inc., 2009.

Clayton, Mark. "Syria's Cyberwars: Using Social Media against Dissent." *Christian Science Monitor*, July 25, 2012. https://www.csmonitor.com/USA/2012/0725/Syria-s-cyberwars-using-social-media-against-dissent.

Deegan, Arthur, Yasir Kalid, Michelle Kingue, and Aldo Taboada. "Cyber-Ia: The Ethical Considerations Behind Syria's Cyber-War | Small Wars Journal," 2017. http://smallwarsjournal.com/jrnl/art/cyber-ia-the-ethical-considerations-behind-syria%E2%80%99s-cyber-war.

Deibert, Ron. "The Geopolitics of Cyberspace After Snowden," 2015. http://www.currenthistory.com/Deibert_CurrentHistory.pdf.

Deibert, Ronald J. "The Geopolitics of Internet Control Censorship, Sovereignty, and Cyberspace," n.d. http://www.handbook-of-internet-politics.com/pdfs/chapter_23.pdf.

"Egypt Internet Users." Accessed April 12, 2018. http://www.internetlivestats.com/internet-users/egypt/.

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War Science & Technology." *Georgetown Journal of International Affairs* 9 (2008): 121–26.

Faris, Rob, Hal Roberts, Rebekah Heacock, Ethan Zuckerman, and Urs Gasser. "Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice," n.d., 18.

Farwell, James P., and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (February 2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

———. "The New Reality of Cyber War." *Survival* 54, no. 4 (September 2012): 107–20. https://doi.org/10.1080/00396338.2012.709391.

Gibney, Alex. *Zero Days*. Documentary. Magnolia Pictures, 2016.

Grohe, Edwin. "The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict." *Comparative Strategy* 34, no. 2 (March 15, 2015): 133–48. https://doi.org/10.1080/01495933.2015.1017342.

Gross, Michael Joseph. "Silent War." *Vanity Fair*, 2013. https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business.

Insider, Paul Szoldra, Business. "Iran Now Has One of the Largest Armies of Hackers in the World — and the US Is Partly to Blame." Business Insider. Accessed April 13, 2018. http://www.businessinsider.com/us-hacker-army-stuxnet-2016-7.

Keller, Max Fisher and Jared. "Syria's Digital Counter-Revolutionaries." *The Atlantic*, August 31, 2011. https://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (February 2011): 41–60. https://doi.org/10.1080/00396338.2011.555595.

Kopan, Tal. "McConnell Will Finesse CISA as NDAA Amendment — Privacy Folks Cry Foul — House Oversight Plans First OPM Hack Hearing - POLITICO." Accessed April 11, 2018. https://www.politico.com/tipsheets/morning-cybersecurity/2015/06/mcconnell-will-finesse-cisa-as-ndaa-amendment-privacy-folks-cry-foul-house-oversight-plans-first-opm-hack-hearing-212543.

Korns, Stephen W., and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (2008): 17.

Lee, Bryan. "The Impact of Cyber Capabilities in the Syrian Civil War | Small Wars Journal." Accessed April 11, 2018. http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*, April 27, 2017, sec. Europe. http://www.bbc.com/news/39655415.

"Middle East Internet Usage Stats and Facebook Statistics." Accessed April 11, 2018. https://www.internetworldstats.com/middle.htm.

Railton, J. S., D. Regalado, and N. Villeneuve. “Behind the Syrian Conflict’s Digital Front Lines.” *CA: FireEye*, 2015. https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-behind-the-syria-conflict.pdf.

Roberts, Hal, Ethan Zuckerman, Robert Faris, Jillian York, and John Palfrey. “The Evolving Landscape of Internet Control,” n.d., 12.

Robin, Patrice, and Marie Baezner. “The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict.” ETH Zurich, 2017. https://doi.org/10.3929/ethz-b-000200662.

Ruhfus, Juliana. “Syria’s Electronic Armies.” Accessed April 11, 2018. https://www.aljazeera.com/programmes/peopleandpower/2015/06/syria-electronic-armies-150617151503360.html.

Sanger, David E. “Syria War Stirs New U.S. Debate on Cyberattacks.” *The New York Times*, February 24, 2014, sec. Middle East. https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.

Shehabat, Ahmad. “The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 201,” n.d., 9.

“Syria.” Media Landscapes. Accessed April 11, 2018. https://medialandscapes.org/country/syria.

“Syria Internet Users.” Accessed April 12, 2018. http://www.internetlivestats.com/internet-users/syria/.

“Tunisia Internet Users.” Accessed April 12, 2018. http://www.internetlivestats.com/internet-users/tunisia/.

“Two From ‘Syrian Electronic Army’ Added to Cyber’s Most Wanted.” Story. Federal Bureau of Investigation. Accessed April 12, 2018. https://www.fbi.gov/news/stories/two-from-syrian-electronic-army-added-to-cybers-most-wanted.

Wentworth, Travis. “How Russia May Have Attacked Georgia’s Internet.” Accessed April 12, 2018. http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111.

Wirtz, James J. “Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy,” n.d., 11.