Exploring OSINT for

Master of Science

Information & Communications Technology

Adrienne Lawson

University of Denver University College

November 8th, 2019

Faculty: Gary Reeves

Director: Mike Batty, PhD

Dean: Michael J. McGuire, MLS

Executive Summary

Despite what a few dystopian thinkers espouse on the news every night the old adage "knowledge is power" still applies to today's world yet it is one with a twist. Anyone from anywhere can learn anything and that includes useful, sensitive information. For example, when you receive an unknown phone call from a strange number you might Google the number, find a reverse phone lookup website and seek out who actually called your phone (so that you know whether to blacklist the number or not). The information you find may include phone service provider, location, name, address and even a map of their closest location. Without knowing it you're utilizing Open Source Intelligence or OSINT.

In this essay, OSINT will be examined further beyond the confines of "people snooping on their exes" and reverse phone lookups. Open Source Intelligence is much more in depth than people realize. The method of OSINT gathering is utilized in many fields and greatly impacts high profile and highly classified areas such as government information security & cybersecurity, counterterrorism, national security, and law enforcement/legal proceedings. On the flipside, OSINT can be used by hackers, various other criminal types and anyone with a little persistence, patience and self-training. Again, OSINT can be gathered by anyone from anywhere at any time. See, there's that twist. Anyone can have the power.

OSINT is More Than Snooping on Your Exes

Open Source Intelligence or OSINT is defined by Michael Bazzell as, "…any intelligence produced from publicly available information that is collected, exploited and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Bazzell 2018)." What is so crucial to understand about this definition and OSINT in general is that it is just as important who is collecting, exploiting & disseminating the information as the information itself. A Midwest soccer mom, divorced, two kids, sipping wine on a Friday night while trawling Tinder for potential dates while simultaneously Googling and social media searching them is OSINT small potatoes, yet it is still important all the same. The example of the winemom on Tinder is the quintessential example of passive collection. It is merely collecting information about a target or subject via publicly available sources (Hassan 2018). Passive collection is the most common type of OSINT gathering and is known as "click-button" gathering. It is done by people everywhere 24/7. This research paper wouldn't exist without passive collection! That's right. The research that has gone into this paper was collected via passive collection i.e. web searches, books, journal articles and pamphlets.

On the opposite side of OSINT are semi-passive and active collection which are less known to the regular person and are usually not conducted by the general public. Semi-passive collection entails technical expertise by querying published name servers and looking at metadata from published documents and files (Hassan 2018). Active collection is a very technical collection method. It involves mapping the target's network infrastructure, scans for open services, vulnerabilities, and unpublished directories (Hassan 2018). With this type of OSINT gathering it is possible for the target to figure out they are being searched. Semi-passive

and Active collection are usually utilized by government agencies, hackers, pentesters and private companies. The average person can utilize these methods, yet it takes a higher degree of technical ability and knowhow. Despite the method used to obtain meaningful intelligence, the process is still the same for everyone. As shown below in Figure 1, the process is straightforward (Shakeel 2016).

1. Identify the source – where is the source of the information?
2. Harvest the information – take what you need from the sources and leave.
3. Process the data – hash out what is useful from the harvest
4. Analysis – join the data with other pieces of data pulled from other sources
5. Report – create a final report logging all findings

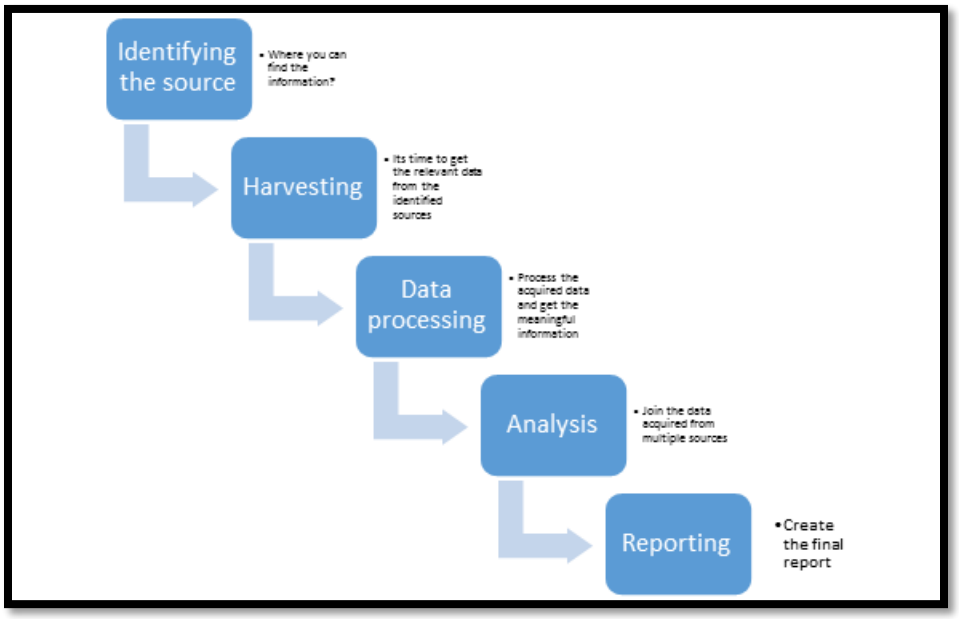

Figure 1: 5 step process of OSINT gathering. (Shakeel 2016)

This process has not changed for years. Seriously, this process has not changed for centuries. OSINT is that old though it only began to be called open source intelligence and OSINT in the 20th and 21st centuries. Gathering intelligence from public sources is much older than that and has a way deeper significance than people realize.

Historically, OSINT has been used for millennia or even more. Wherever there has ever been war, conflict or a need to secure vital information the gathering of openly available sources has always been vital. During the Revolutionary War George Washington had spies gather newspapers, pamphlets and other documents pertaining to the movements and troop strength of the British (Norton 2011). During WW2, open source intelligence offices were set up to track the activity of the Axis powers. Branches like the OSS and the Foreign Broadcast Intelligence Service were set up to monitor foreign media and information (Rawnsley 2015). Even England's BBC helped the war effort by monitoring and recording foreign radio broadcasts and shared this intelligence with the U.S. government and military forces (Colquhoun 2016). The people of today, especially this author's generation, owe a huge debt of gratitude to those who served in WW2 especially the unspoken heroes in intelligence and cryptography. These unspoken heroes used their skills, expertise and open source intelligence to end WW2. Without people like William Donovan, Sherman Kent, Alan Turing, Mavis Batey, Jane Fawcett, Julia Child (yes, that Julia Child), Moe Berg, and Joan Clarke the war would have gone on longer, with higher casualties and who knows what would have actually happened back then. The world we know today could be completely different had OSINT not been utilized.

After WW2, governments around the world began to reinvent and reshape their departments around intelligence and this would occur until well into the Cold War (Rawnsley 2015). As technological advancement changed the cultural landscape worldwide, OSINT changed as well. Decades went by and the methods and world changed around it to the point where it was no longer just about paper documents, TV, photographs, video and radio broadcasts. With the widespread use of the computer and the internet that meant and still means new avenues to gather intelligence. It is now quicker and more efficient for OSINT analysts in

all levels of government to search, find and vet sources via widely available search engines, software and social media sites. Though it must be said that it's not just governments that are utilizing OSINT and it's not just for war and peace. The expanse is wide, wild and each field must be touched upon to understand the full reach of the term.

Fields: National/Government

Examining U.S. intelligence's role, impact on & use of OSINT is indeed an arduous one yet not impossible. Openly available information is at the heart of every single U.S. government department & a multitude of positions scattered around the globe. The term given to the U.S. intelligence network is actually the United States Intelligence Community and it is made up of seventeen Federal departments under the supervision of the Office of the Director of National Intelligence (ODNI - of which it is also included in the total) (Members 2019).

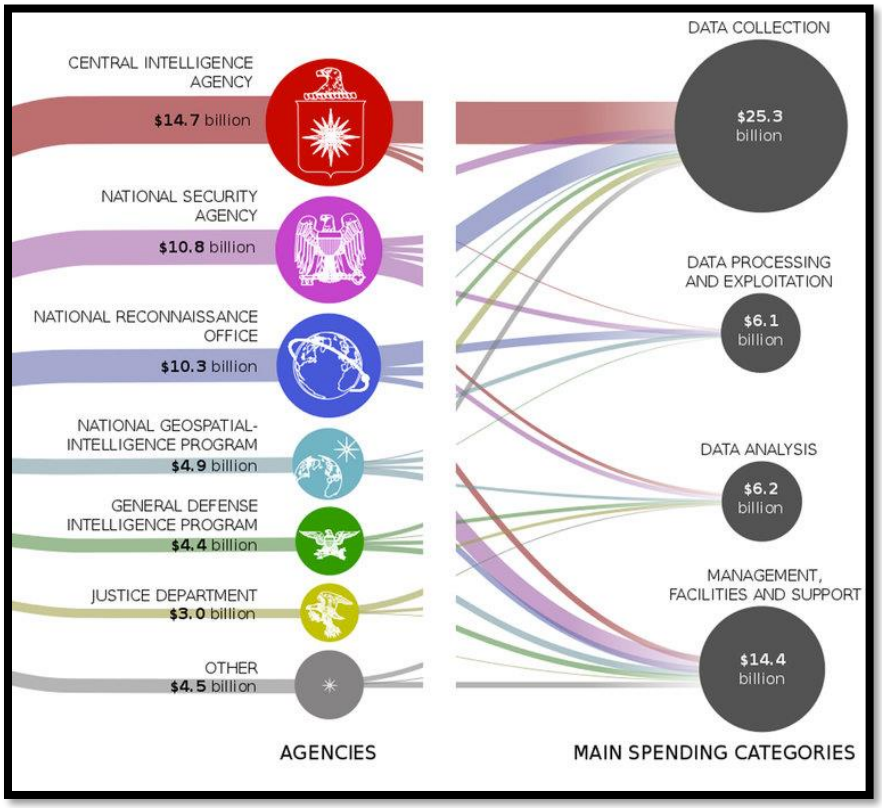

Figure 2: Illustration of the U.S. National Intelligence Funding. (Kelley 2013)

The two most well-known and well-traveled departments within this tight knit community are the Central Intelligence Agency (CIA) and the National Security Agency (NSA). Both of these agencies are the most heavily funded departments in the Community and in the government's "Black Budget" aka the U.S. National Intelligence Funding. *Figure 2* above illustrates the funding for each agency and when combined their funding total is half the entire budget rounding out at 25.5 billion U.S. dollars (Kelley 2013). This has likely to have jumped higher in recent memory owing much to changes in technology and the climate of the world we live in. All of this is mentioned – the departments, the funding, etc. – because it shows the seriousness and focus of the U.S. Government's attention and dedication to intelligence gathering.

The CIA, being the most well-known agency of the community, coupled in the mind with the Great and Powerful FBI, is an OSINT powerhouse. It has been in the OSINT business since its creation by the National Security Act of 1947 ("The Office..." 2013). Upon its inception as a government entity, the CIA absorbed the Foreign Broadcast Information Service (Rawnsley 2015). Today, this organization, now known as the Open Source Enterprise, is under both the jurisdiction of CIA and the ODNI. Now, one might ask, "what does of any of this have to do with OSINT?", "Why mention all this history?" and "How does the CIA gather it?" The answer is quite simple. Importance. It cannot be stressed enough that OSINT has always been around. It has been here as long as we have been at odds with each other on this planet and has evolved drastically in recent years. OSINT has evolved with the times and become a billion-dollar government investment within the field of all source intelligence analysis. Agencies and organizations utilize OSINT alongside other types of intelligence sources to protect and defend assets at home and abroad. The CIA utilizes the Open Source Enterprise (located in the U.S. and around the world) to source openly accessible information of all kinds that benefits and protects

U.S. interests, assets and infrastructure (Aftergood 2015). This means everything from foreign news broadcasts, Twitter accounts of locally elected leaders, newspapers, online forums, magazines, networks – if it's openly available and can be used by the U.S. then best believe the CIA already knows and is making it available to the Intelligence Community. Yes, the OSE makes all its intelligence data available to the entirety of the Intelligence Community and many other departments of the U.S. government (Central 2017). This is because information gathered could greatly impact national security.

By making the data available to the entirety of the Intelligence Community, the CIA, ODNI and OSE not only protect themselves by following protocols they are also giving other agencies like the NSA much needed information that could hinder or stop a national security incident. That doesn't mean that the other agencies do not do their own OSINT gathering – which they do – it means that if they receive matching data then that is another layer they do not have to vet as harshly. This does not mean less work. All of the agencies do their own intelligence gathering yet it is the top 2 big guns of the Community, the two with the highest investments, that tend to gather the most and see the most throughput. Having a higher throughput of actionable intel means there's a better chance of going forward and stopping terrorist attacks, shootings, bombings and other crimes including cyber attacks.

Military

Not to sound cheesy or dated yet I must say – "If there's something strange on your government network packet who you gonna call? NOT FEMA!" Seriously though, don't call FEMA. They have their own issues they're dealing with. In the United States, the department leading the charge in protecting the U.S. information and cyber infrastructure is the Department of Defense (DoD or sometimes referred to just as "The Pentagon"). This department is

"responsible for providing the military forces needed to deter war and protect the security of our country" (Agencies). Under its auspicious eye there are 3 military departments and 11 unified command units which includes U.S. Cyber Command (USCYBERCOM) (Agencies). Within the unit are sub-units for each branch of the military. This command unit is responsible for the operations and defense of DoD networks, for conducting cyber operations in defense of U.S. assets and to "strengthen the nation's ability to withstand and respond to cyber attack" (U.S. 2014). To this end, OSINT is highly valuable because, as it was stated before, everyone can use OSINT including hackers and social engineers. Units like USCYBERCOM must use what is available and essentially "think like an attacker" in order to both red team (offense) and blue team (defense) on behalf of the United States Government. Example: What would an attacker do to gain information about a specific location? They would look for literature and maps and if maps were not available, they would find other means to learn about the location. That could mean surveilling the site, using online mapping tools, live camera feeds yet it could also mean social engineering. A hacker could go into the real world by either calling, texting or emailing someone who works at the location or even going so far as to befriend someone in public in order to gain information. The DoD and USCYBERCOM is taking initiative in related ways and more to protect us and we, the general public, have noticed very little in the way of media coverage.

Last year, USCYBERCOM deployed personnel to Ukraine, North Macedonia, and Montenegro to help defend those countries' networks during the U.S. Midterm Election and help train officials in those countries on cybersecurity for their upcoming elections this year (Lyngaas 2019). This mission, called "Synthetic Theology", was also a mission of intelligence gathering to further investigate cyber attacks on U.S. voting systems (Vavra 2019). This was the first time

that the U.S. had worked in collaboration with those countries regarding cybersecurity and defense (Vavra). The need for the mission stems from the Russian election hacking of the 2016 presidential election and the presumption that Russian agents will double up their efforts to infiltrate voting registration and election systems during the 2020 presidential election (Parks 2019). By collaborating with neighboring countries on cybersecurity, USCYBERCOM can both investigate sources for election hacking in Russia, Ukraine, etc. as well as receive intelligence from government officials in collaborating countries. Having U.S. elections and the infrastructure behind them hacked by foreign countries is frightening and undermines the entire process. What is worse than that is not knowing if your government and your states are doing enough to protect a right you have as a citizen. Will the DoD and its entities be ready by 2020? Will OSINT be utilized correctly, enough or too much? These are all questions that segue into the good, the bad and the ugly of OSINT.

Good, Bad, Ugly: Disadvantages/Advantages

The biggest fear that a private citizen familiar with cybersecurity and intelligence might have is that OSINT (and other intelligence methods) is either not being utilized or it is being utilized to the point where intel is being overlooked, thrown away or never gathered at all. Overutilization can lead to "overload" ("What…"). "Overload" is when you get too much information to process and analyze so errors become prominent, yet no one notices because there's too much information to notice. This is a huge disadvantage of OSINT if not the biggest disadvantage besides time consumption (which can be remedied by using automated software). Not utilizing OSINT means missing out on information that is publicly available and that other people and organizations are most definitely getting their hands on. If hackers are utilizing

OSINT then why not utilize it in a defense and prevention capacity? Ignoring an entire field and collection method is foolhardy, dense and in the end undermines risk management.

If the world woke up one morning and the internet was gone or had never been invented there would still be newspapers, magazines, pamphlets, documents, books and so much more. OSINT would still exist like it has existed for centuries upon centuries. This is its biggest advantage – adaptability. A person doesn't have to have an internet connection to gather the information. They might need a library card, transportation and small bit of financing for travel & snacks yet even that is minimal. In whatever way a person chooses to collect information there are public sources available. The second biggest advantage, possibly tied with its adaptability, is its cost. OSINT costs considerably less than other intelligence gathering methods ("Advantages…" 2017). There are many free or open source software (FOSS) programs available that are running entire collections as well as FOSS automation tools (DMitry, Spiderfoot, DataSploit) (Passi 2019). On top of this, some of the best investigation tools are Linux-based which cuts down on operation costs (theHarvester, Recon-Ng) (Passi). The options are unlimited with how a person, private corporation, government organization or agency can set up and operate an OSINT investigation.

With all of this said and now knowing what OSINT is and how it can be utilized by everyone this author hopes that more people realize its worth. Open source intelligence impacts our daily lives without 99.9% of us even realizing such a thing exists. Hackers and social engineers use OSINT to gather information in their attacks on electrical grids and power stations of entire countries. Without government agencies utilizing intelligence collection who knows what the United States and the rest of the world would look like. If the national power grids can be hacked in other countries, then it can happen in the U.S. at any time and has happened quite

recently. Now is the time for OSINT to be at the forefront of intelligence gathering for the sake of its own evolution and for the sake of those that depend on security, cyberspace and freedom of information.

Works Cited

"Advantages and Disadvantages of Open Source Intelligence." 2017. *Expert System*. February 24. https://expertsystem.com/advantages-disadvantages-open-source-intelligence/.

Aftergood, Steven. 2012. "An Army Introduction to Open Source Intelligence." Federation Of American Scientists. September 13. https://fas.org/blogs/secrecy/2012/09/army_osint/.

Aftergood, Steven. 2015. "Open Source Center (OSC) Becomes Open Source Enterprise (OSE)." *Federation Of American Scientists*. October 28. https://fas.org/blogs/secrecy/2015/10/osc-ose/.

"Agencies - Defense Department." 2019. *Federal Register*. Federal Register. Accessed November 10. https://www.federalregister.gov/agencies/defense-department.

Bazzell, Michael. 2018. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. Charleston, SC: IntelTechniques.com.

Calkins, Laura M. 2011. "Patrolling the Ether: US–UK Open Source Intelligence Cooperation and the BBCs Emergence as an Intelligence Agency, 1939–1948." *Intelligence and National Security* 26 (1): 1–22. doi:10.1080/02684527.2011.556355.

"Center for the Study of Intelligence." 2019. *Central Intelligence Agency*. Central Intelligence Agency. October 1. https://www.cia.gov/library/center-for-the-study-of-intelligence.

Central Intelligence Agency. 2017. *III. How Intelligence-Sharing Works at Present*. Central Intelligence Agency. April 4. https://www.cia.gov/library/center-for-the-study-of-

intelligence/csi-publications/books-and-monographs/sharing-secrets-with-lawmakers-congress-as-a-user-of-intelligence/3.htm.

Colquhoun, Cameron. 2016. “A Brief History of Open Source Intelligence.” *Bellingcat*. July 14. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

“Cybersecurity.” 2019. *Department of Homeland Security*. October 23. https://www.dhs.gov/topic/cybersecurity.

Eccleston, Sally. 2018. “Open Source Intelligence: Automatically Finding New Cybersecurity Threats.” *Open Access Government*. December 12. https://www.openaccessgovernment.org/finding-cybersecurity-threats-with-open-source-intelligence/55608/.

Hassan, Nihad. 2018. “An Introduction To Open Source Intelligence (OSINT) Gathering.” *Secjuice*. Secjuice. August 22. https://www.secjuice.com/introduction-to-open-source-intelligence-osint/.

Kelley, Michael B. 2013. “Here's A Fantastic Data Visualization Of The US Intelligence Community's 'Black Budget' Spending.” *Business Insider*. Business Insider. September 3. https://www.businessinsider.com/data-visualization-of-the-black-budget-2013-9.

Karmanau, Yuras. 2019. “Ukrainian Official: Hacking Intensifies as Election Nears.” *AP NEWS*. Associated Press. February 13. https://apnews.com/5b22d3cf90b24a19ba03d82fe91329e0.

Lyngaas, Sean. 2019. “Cyber Command's Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia.” *CyberScoop*. CyberScoop. March 14. https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.

Mazzetti, Mark, and David E. Sanger. 2013. “Security Leader Says U.S. Would Retaliate Against Cyberattacks.” *The New York Times*. The New York Times. March 12. https://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html.

“Members of the IC.” 2019. *Members of the IC*. Office of the Director of National Intelligence. Accessed November 10. https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

Mercado, Stephen C. 2004. “Sailing the Sea of OSINT in the Information Age.” *PsycEXTRA Dataset*. doi:10.1037/e741272011-005.

Mueller, Robert S. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. U.S. Department of Justice. https://www.justice.gov/storage/report.pdf.

Naylor, Brian. 2018. “Russia Hacked U.S. Power Grid - So What Will The Trump Administration Do About It?” *NPR*. NPR. March 23. https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it.

Norton, R.A. 2011. “Guide to Open Source Intelligence A Growing Window into the World.” *The Intelligencer: Journal of U.S. Intelligence Studies* 18 (2): 65–67. https://www.afio.com/publications/Norton_Open_Source_in_AFIO_INTEL_WinterSpring2011.pdf.

NSA/CSS. 2019. “Oversight.” *Frequently Asked Questions Oversight*. NSA/CSS. Accessed November 10. https://www.nsa.gov/about/faqs/oversight-faqs/.

Parks, Miles. 2019. “Florida Governor Says Russian Hackers Breached 2 Counties In 2016.” *NPR*. NPR. May 14. https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.

Passi, Harpreet. 2019. “Top 10 Popular Open Source Intelligence (OSINT) Tools.” *Top Open Source Intelligence Tools*. September 26. https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools.

Pomerleau, Mark. 2019. “What the Future Holds for Cyber Command.” *What the Future Holds for Cyber Command*. Fifth Domain. July 25. https://www.fifthdomain.com/dod/cybercom/2019/07/25/what-the-future-holds-for-cyber-command/.

Rawnsley, Adam. 2015. “The Open-Source Spies of World War II.” *Medium*. War Is Boring. March 3. https://medium.com/war-is-boring/the-open-source-spies-of-world-war-ii-7943bd5b663c.

"Section 2 INTELLIGENCE COLLECTION ACTIVITIES AND DISCIPLINES." 2019. *Section 2 - INTELLIGENCE COLLECTION ACTIVITIES AND DISCIPLINES - Operations Security - INTELLIGENCE THREAT HANDBOOK*. Federation of American Scientists. Accessed November 10. https://fas.org/irp/nsa/ioss/threat96/part02.htm.

Shakeel, Irfan. 2016. "The Art of Searching for Open Source Intelligence." *Infosec Resources*. Infosec Institute. May 9. https://resources.infosecinstitute.com/the-art-of-searching-for-open-source-intelligence/#gref.

Tabatabaei, Fahimeh, and Douglas Wells. 2016. "OSINT in the Context of Cyber-Security." *Open Source Intelligence Investigation Advanced Sciences and Technologies for Security Applications*, 213–31. doi:10.1007/978-3-319-47671-1_14.

Team, SecurityTrails. 2018. "SecurityTrails: What Is OSINT? How Can I Make Use of It?" *The World's Largest Repository of Historical DNS Data*. SecurityTrails. September 6. https://securitytrails.com/blog/what-is-osint-how-can-i-make-use-of-it.

"The Office of Strategic Services: Research and Analysis Branch." 2013. *Central Intelligence Agency*. Central Intelligence Agency. April 30. https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/oss-research-and-analysis.html.

The PTES Team. 2016. "Intelligence Gathering." *Intelligence Gathering - Pentest Standard 1.1 Documentation*. The PTES Team. https://pentest-standard.readthedocs.io/en/latest/intelligence_gathering.html.

U.S. Cyber Command. 2018. “Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command.” *USCYBERCOM Vision April 2018*. April. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM Vision April 2018.pdf?ver=2018-06-14-152556-010&source=post_page----------.

U.S. Cyber Command Public Affairs. 2014. “U.S. Cyber Command.” *U.S. Cyber Command - U.S. Strategic Command*. April 16. https://web.archive.org/web/20140416192156/http://www.stratcom.mil/factsheets/2/Cyber_Command/.

Vaas, Lisa. 2019. “350 Hackers Hunt down Missing People in First Such Hackathon.” *Naked Security*. October 15. https://nakedsecurity.sophos.com/2019/10/15/350-hackers-hunt-down-missing-people-in-first-such-hackathon/.

Vavra, Shannon. 2019. “Cyber Command Has Redeployed Overseas in Effort to Protect 2020 Elections.” *CyberScoop*. May 8. https://www.cyberscoop.com/cyber-command-redeployed-overseas-effort-protect-2020-elections/.

Vavra, Shannon. 2019. “U.S. Ramping up Offensive Cyber Measures to Stop Economic Attacks, Bolton Says.” *CyberScoop*. CyberScoop. June 11. https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/.

“What Is Open Source Intelligence and How Is It Used?” 2019. *Recorded Future*. Recorded Future Team. February 19. https://www.recordedfuture.com/open-source-intelligence-definition/.