THE UTILIZATION AND MANAGEMENT OF SOCKPUPPETS WITHIN ONLINE COMMUNITIES

by

Melissa Morris

A Capstone Project Submitted to the Faculty of

Utica College

May 2014

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

The Internet is the principle arena for online communication. Within the online community, individuals can choose who they are. If a member chooses an online identity that is something other than who they are in real life, then the identity created is a sockpuppet. The purpose of this research was to examine the utilization and management of sockpuppets within online communities. What are the ethical and legal boundaries in the use of sockpuppets within civilian online communities? What is the role of sockpuppets in the intelligence community? The intent behind sockpuppet use determines the ethical and legal boundaries within civilian online communities. If the intent is for entertainment and communication, online communities exhibit various levels of tolerance for ethical versus unethical choices of sockpuppets. However, legal boundaries are crossed if the intent is to do harm. The United States is not consistent with legislation involving sockpuppets. The intelligence community uses sockpuppets to assist in maintaining national security. A sockpuppet allows an analyst to infiltrate targeted online communities, and once inside to gather information about the group. Sockpuppets are accepted within the communities and gain a perspective similar to an offline undercover agent. It takes great effort and skill to create long lasting and believable identities that effectively collect actionable intelligence. Conclusions generated based on a review of the current research include; federal legislation and management defining and clarifying criminal use of a sockpuppet, the creation of a best practices manual for the intelligence community to standardize training and utilization of sockpuppets, as well as continued study of the evolution of the sockpuppet.

Keywords: Cybersecurity, Professor Christopher Riddell, Mr. Jeffrey Bardin, sockpuppets, online, communities, ethics, legal, intelligence, identity.

Acknowledgements

Foremost, I would like to thank my capstone committee chair, Professor Christopher Riddell for his extreme patience in the face of numerous obstacles. Your words of encouragement and firm expectations helped me forge ahead during tumultuous times. I would like to thank my second reader, Mr. Jeffrey Bardin, for the inspiration to take on the topic of sockpuppets. Your classes and our conversations instilled priceless insight, passion, and laughter into all of my research. To Mr. Joe Giordano, thank you for the constructive comments and warm encouragement throughout my academic program, it always made everything seem possible. To Mr. Chet Hosmer, Dr. Leonard Popyack, Jr., and Mr. Vernon McCandlish, thank you for exciting my passion through your coursework and the personal example you set through your careers. I would like to thank my friends for knowing that I am insane and sticking by my side anyhow. I am deeply grateful for the love and support from my family. My three children have sacrificed time that I will forever attempt to repay, thank you Serenity, Brady, and Jillian. Finally, I would like to thank my husband, Nathan Morris. He has always been there reassuring me, pushing me, and above all supporting me through the good times and bad. I could not have completed this without him.

Table of Contents

List of Illustrative Materials

The Utilization and Management of Sockpuppets within Online Communities

The Intelligence and National Security Alliance Cyber Intelligence Task Force stated, "All operations in cyberspace begin with a human being" (*Operational Levels of Cyber intelligence*, 2013, p.1). In order to interact online, humans create an identity. Nomenclature used for the identities people create include Internet persona, social identity, virtual persona, and avatar. For the purposes of this research, the term sockpuppet will be defined as, an online identity used for purposes of deception within an online community (IT Law Wiki, 2014).

Most commonly, these identities communicate with family, friends, business associates, and potential corporate partners. A sockpuppet can carry out a multitude of tasks, for example, debating, sharing information, collaborating, and entertaining. However, the sockpuppets that people shape on the Internet are not always reliable. The purpose of this research was to examine the utilization and management of sockpuppets within online communities. What are the ethical and legal boundaries in the use of sockpuppets within civilian online communities? What is the role of sockpuppets in the Intelligence community?

Initially, a sockpuppet was "a false identity through which a member of an Internet community speaks with or about oneself, pretending to be a different person, like a ventriloquist manipulating a hand puppet." (Malone, 2013, para.2). The earliest use of the term sockpuppet was by Dana Rollins in a 1993 listserv conversation (McFedries, 2006) and again in 2006 involving people using sockpuppets to boost their own works. This led to Paul McFedries (2006) definition in WordSpy, "a fake persona used to discuss or comment on oneself or one's work, particularly in an online discussion group or the comments section of a blog" (para. 1). "Facebook estimates that roughly 7 percent of accounts – some 76 million – are phony. Twitter guesses 5 percent of its 200-million [plus] active users are bogus" (Tynan, 2013, para. 1). These

fabricated identities are often created for the purpose of boosting a point of view, praising a product, backing another person, or supporting a cause. In a New York Times article by Stone & Richtel (2007), they defined sockpuppeting as, "the act of creating a fake online identity to praise, defend or create the illusion of support for one's self, allies or company" (p.1). Today the reach of the term sockpuppet goes beyond alternate identities of people who post in an online environment, to include other uses of sockpuppets (Laden, 2009). For example, sexual predators, identity thieves, spies, hackers, intelligence agents, and opportunists all utilize sockpuppets.

The alternate uses of sockpuppets appeared in headlines around the world. On February 5, 2013, the United States Attorney's Office published a press release with the headline, "Eighteen People Charged in International $200 million Credit Card Fraud Scam, Crime Ring Invented 7,000 Fake Identities to Obtain Tens of Thousands of Credit Cards" (States News Service, 2013, p. 1). In an article entitled, Cyber-Spying for Dummies (2008), Mark Hosenball discussed the plight of counterterrorism officials. The officials considered using fake identities to login to suspected terroristic websites. However, the idea was abandoned because a mandate stated they must use government computers to access the Internet. The identification of the computer systems as government run would be a simple task for the terrorists. In December 2013, many news outlets recounted a story in which the National Security Agency (NSA) used fake identities to infiltrate and spy on people in the game, World of Warcraft.

Exactly one year after the United States Attorney's office uncovered a sockpuppet crime ring, on February 5, 2014, PC Tech magazine reported that NSA and Federal Bureau of Investigation (FBI) agents contacted Jacob Allred. Mr. Allred is the creator of fakenamegenerator.com, a website that auto generates an identity with a name, date of birth, address, mother's maiden name, and a social security number. Additionally, the identities created

on the website offer credit card numbers that will pass an initial validation test. Online community members across the globe use fakenamegenerator.com for a multitude of legal purposes; including, network penetration testers, fiction authors, and law enforcement. However, the temptation within online communities to use a sockpuppet for personal gain is powerful. In October 2013, a report indicated that Fox News employed fake commentator accounts to counter negative feedback aimed at them on blogs in various online communities (Dimiero, 2013). The fabricated pro-Fox arguments boosted the network's position throughout online communities.

Sockpuppets are not a new phenomenon; some would like to label them a warped extension of overactive social media, but it has a profound past. Benjamin Franklin authored letters and other works as Mrs. Silence Dogood, Alice Addertongue. Infamously, Benjamin Franklin posed as Richard Saunders and wrote, "Poor Richard's Almanack" (Dwyer, 2012). Mr. Franklin posed as upwards of eleven pseudonyms (PBS, 2002). Would our culture today vilify or criticize Benjamin Franklin's sockpuppetry? Most people in the United States see his actions as necessary and heroic (PBS, 2002). Jim Dwyer (2012) reported in the New York Times,

> Fernando Pessoa, a Portuguese poet and man of letters in the early 20th century, who created 72 imaginary names to cover his various writing moods and modes; he staged debates among them and had one announcing the death of another, to much grief. Pessoa called these "heteronyms," a term that lacks the faintly musty notes of sockpuppet. (para.7)

The ability to enlist technology and social media to travel thousands of miles with a sockpuppet in seconds, while at the same time talking to millions of people, is new. The speed at which technology transports our information causes complicated split second decisions about our online identity.

Ethics are, “the rules or standards that govern conduct. How I live my life and make my decisions” (Lohrmann, 2012, para. 24). Moreover, Raphael Golb developed sockpuppets to defend and promote his father’s theories on the Dead Sea Scrolls. In total, he created 80 plus identities that interacted and referred to one another to foster his arguments about his father’s findings and subsequent mistreatment in his opinion (Leland, 2013). Mr. Golb sent hundreds of emails meant to harass, and at least one of the sockpuppets impersonated a real professor that was the main academic rival to his father’s research (Leland, 2013). Harassment and impersonation are criminal acts, but the sockpuppets by themselves are a murky field in terms of legal debate. Ethically, the sockpuppet tests a person in different ways. There are many among the population that offer guidance or ask questions about the ethical and legal considerations in terms of sockpuppets, but nothing is clear. Staff Sergeant Dale Sweetnam, the noncommissioned officer in charge of the Online and Social Media Division in the Office of the Chief of Public Affairs states, “You have to stay vigilant, protect your information and always be on the lookout for social media scams” (Social Media Division, U.S. Army Office of the Chief of Public Affairs, 2011, para. 3).

The Telstra Foundations authored information about fake profiles and identity theft on a page called Lawstuff (2013). However, every detail referred to using someone else’s information to make a fake profile or account. It did not address legalities of a profile that is created from fake information. Some literature indicated that the actions of the identity, and not the actual identity itself, cause the legal and ethical issues. In 2008, Lori Drew from Missouri created a MySpace sockpuppet of a 16-year-old boy that she named Josh Evans. She utilized the sockpuppet to befriend and create a relationship with Megan Meier (Meredith, 2010). Megan was a 13-year-old girl that Lori Drew’s daughter disliked. Lori Drew maintained the relationship

and then ended it abruptly. Megan committed suicide over the loss of the relationship (Schwartz, 2009). Lori Drew was convicted for misrepresenting her identity, in violation of the MySpace terms of service (Meredith, 2010). The Los Angeles United States Attorney successfully claimed that it was addressed through federal computer fraud legislation against accessing a computer without authorization via interstate commerce (Meredith, 2010). The grand jury charged Drew with conspiracy and three counts of accessing protected computers without authorization in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 (Digital Media Law Project, 2010). The indictment charges that

> On or about the following dates, defendant Drew, using a computer in O'Fallon, Missouri, intentionally accessed and caused to be accessed a computer used in interstate commerce, namely, the MySpace servers located in Los Angeles County, California, within the Central District of California, without authorization and in excess of authorized access, and, by means of interstate commerce obtained and caused to be obtained information from that computer to further tortious acts, namely intentional infliction of emotional distress on [Meier]. (Digital Media Law Project, 2010, p.1)

Drew appealed the verdict, arguing that her use of a false identity did not constitute unauthorized access to MySpace, based on a 1973 breach of contract dispute where a court of appeals ruled that fraudulently induced consent is consent nonetheless (Meredith, 2010). Her attorneys additionally argued that she did not have a fair trial because the jury was unfairly prejudiced, and on grounds of failure to state an offense, vagueness, and unconstitutional delegation of prosecutorial power. In 2009, the court heard Drew's motion for acquittal, eventually granted the motion, and dismissed all charges (Digital Media Law Project, 2010).

Literature Review

Historical Perspective of Anonymity

Throughout history anonymity has been a constant practice of stimulating unencumbered ideas and thoughts (Solove, 2002). In 1590, John Udall was convicted for using a pen name for his writings. In 1637, a law stated that all books would be regulated and that they must indicate a publisher and author. In 1694, many of these laws expired which allowed pen names to flourish, and the writings of political and religious debate did as well ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961). In 1789, Congress passed the first amendment which states:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. (Independence Hall Association, 2014, para. 1)

In the United States between 1789 and 1809, six presidents, fifteen cabinet members, twenty senators, and thirty-four congressional representatives published anonymously or under a pen name ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961).

In the 19th century, anonymity continued to cause debate and legal battles throughout the United States and Europe. In 1850, France passed a law that newspaper articles that were political, philosophical, or religious in nature had to be signed. In 1912, the United States Post Office Appropriations Act required people that used second class mail, used by newspapers, magazines, and periodicals, to reveal the names of officers and owners ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961). In 1923, New York State enacted a statute that forbid all oath based corporations and associations with more than twenty

members, excluding labor unions and some benevolent orders, from delivering any anonymous writings to non-members ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961). These entities had to file copies of their constitution, bylaws, membership rosters, officers, and political resolutions. Another part of the statute made it punishable to be a member of such an organization if they were knowingly violating the statute. This was appealed in Bryant v. Zimmerman in 1923. However, the New York State Supreme Court upheld the statute saying it did not violate the fourteenth amendment ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961).

In the 1950s and 1960s, suspected communist action groups had to provide the names of members, and the government required the registration of people and purpose when a person requested public space for a parade or meeting. In 1970, Title V of the Organized Crime Control Act of 1970, identified that the United States Attorney General may support the relocation and protection of a witness, or potential witness, of the federal or state government in an official proceeding concerning organized crime or other serious offenses.18 U.S.C.A 3521, et. seq ("18 U.S. Code Â§ 3521 - Witness Relocation and Protection," 1984). This program definitively sponsored the creation of new identities for witnesses along with complete relocation.

United States law literature points to solid constitutional protection for anonymous speech for approved groups and individuals. Federal and state constitutional statutes, legislation, and court decisions resolve public and private lawful regulation of anonymity. However, the research does not indicate a clear-cut consistent view of right and wrong, which is evidenced by current events in both sectors. Online Communities are a new realm for this type of constitutional argument.

Sockpuppets within Online Communities

A famous New Yorker cartoon by Peter Steiner deals specifically with anonymous identity in an online environment. It depicts a dog sitting at a computer terminal, saying to another dog, “On the Internet, nobody knows you’re a dog” (Steiner, 1993, p.61). Sockpuppets infiltrate all online communities. Some computer users see anonymity as entertainment, and other users feel being anonymous eliminates the necessity for civilized conduct. Those users think they can skirt responsibility for rude and sometimes illegal activities. Some instances support the idea of anonymity, but others indicate the negative aspects.

Academia and business. Research and learning can be a solitary life. An academic may spend years on a thesis, book, or research study, and sit and watch for years before the conversation begins about their work. As an alternative, they may instead use a sockpuppet to begin the debate themselves, hoping to stir the pot. That may lead to developing a pseudonym’s reputation, so they are taken seriously. However, pretending to be another person in a peer review situation is disrespectful, and it is a desecration to the trust that is a consistent theme among scholars (Naiman, 2013).

Benjamin Franklin wrote on a variety of topics under pseudonyms such as, Mrs. Silence Dogood, Richard Saunder, and Alice Addertongue ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961). He desired the ability to write from different viewpoints without concern of his own reputation getting in the way. However, the desire for success and wealth in academics and business motivated the birth of many sockpuppets. An American lawyer used online aliases to harass people in an academic dispute about the Dead Sea Scrolls. His father spent his life’s work on researching and theorizing about the Dead Sea Scrolls (Associated Press, 2010). Raphael Golb conviction included identity theft and other charges

related to Internet impersonation. Golb said free speech protected the writings. Carol Berkman, the judge in the case, said his conviction was about actions, not ideas. "It's not his words, but his conduct, it is still a crime to imitate people in the manner that [Golb] did . . . The victims felt invaded and hurt by this" (Associated Press, 2010, para. 8). The District Attorney stated that Golb was not simply commenting; instead, he spent, "thousands of hours of malicious harassment and impersonation" (Associated Press, 2010, para. 13). Golb went to prison stating, "Before this case, I did not know that satirical hoaxes of the sort were treated as crimes in the United States of America" (Associated Press, 2010, para.4). Golb's motivation was that of retribution for his father's rejection in his life's work. His rationalization was the first amendment, but he crossed the line when he used the actual names of other real people to discredit his father's opponents.

Novelists are subject to similar disgrace. However, unlike Benjamin Franklin using a pen name such as Richard Saunder to further his cause, in online communities they are boosting sales. An author reviewing their own work under another name started before online communities. "Walt Whitman and Anthony Burgess were both famous for having reviewed their books under pseudonyms" (Lindsey, 2013, p.1). Online communities make it easier for people to hide their identity for their own benefit. Glen Fleishmann, Amazon's catalog manager, was the first to use the term "customer review" to distinguish consumer-written book reviews from professionally written book reviews posted on Amazon (Dohse, 2013). Amazon developed the consumer review in 1995 for all of its products, and the temptation for self-serving praise began with it. Novelist R.J. Ellory publically apologized after the discovery that he was posting positive reviews of his own work as a sockpuppet on Amazon (Brooke, 2012). He used two sockpuppets to admire his own works, while he attacked other author's books. Mr. Ellory unknowingly did

not hide his connection to the sockpuppets. He offered his name and website to contact him, even though the post listed the sockpuppet names as the author of the comments. He said that he was responsible for a lapse in judgment (Brooke, 2012). Similarly, author Stephen Leather admitted to using sockpuppets to bolster his works popularity on Amazon. He stated,

> As soon as my book is out, I'm on Facebook and Twitter several times a day talking about it. I'll go on to forums and post there under my name and under various other names. You build up this network of characters who talk about your books and sometimes have conversations with yourself…everyone does [it]. (Brooke, 2012, p.2)

Some authors remain respectful of the consequences of such actions. They steer clear and reiterate that it can destroy a reputation and potentially an entire career. After several similar incidents, the British Crime Writers' Association condemned the practice and stated it was going to institute a code of ethics (Brooke, 2012). Using a sockpuppet for this type of false praise is called, "Astroturfing". A Forrester Research study found that half of the users who visit a retail site with consumer postings say that the consumer reviews are important or extremely important in their purchase decisions (Chen, Fay & Wang, 2003). There is a direct correlation in profit increase and star increase in reviews (Brooke, 2012). Profit increase or direct income, or greed, becomes motivation for the use of a sockpuppet in this context.

Websites like freelancer.com and fiverr.com allow companies to purchase or bid on phony reviews. These reviews can cost anywhere from five dollars each to five hundred dollars (Brooke, 2012). Authors started a petition called, "No Sockpuppets Here Please" to try to manage sockpuppets within their own community (Brooke, 2012). The petition is designed to be a voluntary pact of sorts between professionals. The under signers agreed not to utilize

sockpuppets for fake review and be alert and censure sockpuppets they discover. The debate remains whether this petition is something that works, or keeps the honest truthful.

Criminal. Commenting on a criminal case, Forbes' Kashmir Hill said, "The unmasking that law enforcement did highlights the fact that our online activity is not as anonymous as we may think when we're online under assumed names and on other people's networks" (2012, para. 6). Criminals that hide online behind sockpuppets are more sophisticated because law enforcement technologies are growing, and sockpuppet detection is on the rise. Digital rights proponents may not like the idea, but for victims of sockpuppets it is a relief.

Sockpuppet management among convicted sex offenders requires them to register any online identities they utilize with the state. Sockpuppets provide anonymity, and with a bit of technological knowledge they become difficult to detect. A sexual predator that wants to remain a sexual predator despite legal rules could employ this strategy. James R. Brisson Jr. went before the court in Winchester, New Hampshire, on charges of violating the sex offender registration law, indecent exposure, lewdness, and harassing communication and common law criminal contempt (Farrar, 2012). Mr. Brisson utilized a sockpuppet on a dating website, met a woman online and then off, and refused to let her leave his apartment. When she attempted to escape, he jumped on the hood of her car and exposed himself (Farrar, 2012). This was Mr. Bisson's third related conviction. His original sentence of two to five years now had an additional three to seven years for the sockpuppet crime.

Shawn Sayer stalked and harassed his ex-girlfriend using sockpuppets to create several fake emails and Internet profiles with her name and image. In 2006, he was convicted of stalking. Instead of heeding the conviction, he took his actions online (Morris, 2012). From 2008 to 2010, Mr. Sayer set up dozens of fake social media sockpuppets with his ex-girlfriend's

information. He used sexually explicit photos and videos obtained during their relationship to create ads for sexual services (Morris, 2012). Part of the sockpuppet profile included her address and telephone number. In 2008, men showed up at her doorstep expecting what was advertised. The men had no idea that the instructions on the sockpuppet profile pages were bogus. The victim moved to Louisiana and changed her name. However, Mr. Sayer located her and changed his sockpuppets to reflect her new identity and home. In August of 2009, men arrived at her home and knocked on the windows as instructed by the sockpuppet. The police at the time did not feel it warranted investigation. She wrote to the Attorney General, and it was sent to the Computer Crimes Unit (Morris, 2012). In order to catch Mr. Sayer's sockpuppets, the Computer Crimes Unit needed to be very thorough. Kevin Morris (2012) reported the several actions that took place:

- Subpoenas to Yahoo, Myspace, Facebook, and PayPal for the IP and login information used on the fake accounts. This information, used as a cross-referencing tool, would form the backbone of much of their detective work.
- A GPS device on Sayer's truck. Detectives later matched Sayer's geographic location with unsecured Wi-Fi networks that had been used to access the account.
- A (fully legal) stop in Sayer's driveway. Pretending to be lost, detectives pulled in and quickly scanned for any available unsecured wireless networks. They found one, which was owned by Sayer's neighbors across the street. That neighbors' IP address had been used to access one of the Facebook accounts.
- Hidden cameras. At a pizza shop in Saco, Maine, the cameras showed a green pickup truck remarkably similar to Sayer's pull up and sit idle for more than 20 minutes. IP logs show the fake MySpace account being accessed at the exact same time.

- Bearing a warrant, the detectives searched Sayer's home twice. The second time they seized a laptop, where they found proof Sayer had created 49 Yahoo accounts that he tied to fake social media accounts. (para. 11-15)

Shawn Sayer pled guilty to cyberstalking as part of a plea agreement with the state of Maine. His twenty-two month sentence included jail time for bail and protective order violations. However, because his actions crossed state lines, Judge D. Brock Hornby of the United States District Court in Portland, Maine, sentenced Mr. Sayer to the maximum five years in federal prison and three subsequent years of supervised release.

Throughout his federal trial, Shawn Sayer contested that the cyberstalking statute violated his constitutional rights, including the right to free speech (Gitomer, 2013). The District Court determined that the First Amendment did not protect Mr. Sayer's actions. Judge D. Brock Hornby stated, "Identity theft and threats also involve communication, and speech in that sense, and yet they are crimes not protected by the First Amendment" (Gitomer, 2013, para.9). The applicable federal precedence states when criminal law is broken, and the actions or communications do not contain political or religious context, the First Amendment is not involved. "The District Court concluded that all the elements of the interstate stalking offense under 18 U.S.C. § 2261A (2) (A) were satisfied" (Gitomer, 2013, para. 11).

These cases are looked at on a case-by-case basis and compared to identity theft, fraud, and cyberstalking laws that are currently in place. Currently, thirty-eight states have cyberstalking laws and forty states have cyberharassment laws (National Conference of State Legislatures, 2013). "Cyberharassment differs from cyberstalking in that it may generally be defined as not involving a credible threat" (National Conference of State Legislatures, 2013,

para. 3). Sockpuppets are not specifically mentioned within these laws, but many include anonymity in part of the description.

Other legal considerations. Anonymity's history includes both good and bad purposes, therefore, various countries have laws that protect and forbid anonymity. Several countries have laws protecting the anonymity of the person giving tips to newspapers, and laws protecting the anonymity in communication with priests and doctors. On October 26, 2001, six weeks after September 11, 2001, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the USA PATRIOT Act). The Act contains, "ten titles, and addresses myriad issues; including terrorism investigation funding, immigration requirements, the enhancement of federal authorities, assistance for terrorism victims, sharing of information among law enforcement agencies, bioterrorism prevention, and enhanced surveillance activities" (Harrison, 2004, p.177).

As more computer users live and work in cyberspace, they bring expectations that the legal norms of the real world will apply. Lawyers, judges, and juries, often without any real understanding or skill with electronic networks, are asked to prosecute, defend, or decide disputes within online communities. The following is the White House stance on the idea of trusted identity:

> Just as there is a need for methods to reliably authenticate individuals, there are many Internet transactions for which identification and authentication is not needed, or the information needed is limited. It is vital to maintain the capacity for anonymity and pseudonymity in Internet transactions in order to enhance individuals' privacy and otherwise support civil liberties. Nonetheless, individuals and businesses need to be able to check each other's identity for certain types of sensitive transactions, such as online

> banking or accessing electronic health records. The *National Strategy for Trusted Identities in Cyberspace* (NSTIC or Strategy) charts a course for the public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions. (*National Strategy for Trusted Identities in Cyberspace Enhancing Online Choice, Efficiency, Security, and Privacy*, 2011, p.1)

Laws that pertain to online anonymity or sockpuppets include those related to identity theft, fraud, cyberbullying, and defamation. Cyber stalking garners attention globally, however, judges have interpreted it differently depending on the case that was in front of them. In 2006, an amended law received mixed reviews. 47 U.S. Code § 223 states:

> Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications amendments seemingly include specific definitions to address online anonymity, "Whoever...utilizes any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet... without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person...who receives the communications...shall be fined under title 18 or imprisoned not more than two years, or both. (2006, section b)

In a defamation lawsuit involving Yahoo! and Dendrite International, Inc., the court developed a test that would decide if a plaintiff could attempt to identify an unknown online defendant. This test allows the court some objectivity in determining whether anonymity should be protected or rejected. It is not foolproof and it is still subjective to some extent. The test has four parts:

> Plaintiffs are required to 1) attempt to notify the anonymous posters of the pending subpoena; 2) specify exactly the alleged defamatory speech at issue; and 3) satisfy the elements of a prima facie defamation case in the jurisdiction. Provided these standards are met, a court then is to balance the defendant's First Amendment interest in anonymous speech against the strength of the plaintiff's prima facie case and the necessity for disclosure. (Massoglia, 2013, p.20)

The Dendrite test attempts to maintain the integrity of the online community member's First Amendment rights. Several courts have utilized the test to determine if a plaintiff could hunt a sockpuppet. The Cahill test alters the Dendrite test by removing the second and fourth part (Massoglia, 2013). The Cahill test assuming that these parts are included in the prima facie summary judgment standard (Massoglia, 2013).

According to the Pew Research Center, 59% of people surveyed say that people should have the ability to use the Internet completely anonymously (Rainie, Kiesler, Kang, & Madden, 2013). When Internet users are directly asked, 18% say they use the Internet in a way that hides or masks their identity. Pew's national survey revealed 86% of Internet users have tried to be anonymous online, or have taken one-step to try to mask their behavior to avoid being tracked (Rainie, Kiesler, Kang, & Madden, 2013).

Sockpuppets in the Intelligence Community

China has been using an army of two million sockpuppets called the 50 Cent Party to manipulate Internet users. This practice is an official occupation, Internet opinion analyst, paid by the government to push propaganda on message boards, blogs, and social media (Elsner, 2013). In 2007, a Chinese leader, Hu Jintao, created the 50 Cent Party to cultivate public opinion through social media (Elsner, 2013). In Iran, intelligence agents directed attacks towards the

Green Revolution protestors within the country in order to shut them down (Fitsanakis & Bolden, 2012). The Russian version of China's 50-cent party is called the 30-Ruble Army. The task is the same; leave tens of comments each day under tens of different sockpuppets (Khazan, 2013). Twenty-two out of sixty countries have paid pro-government commentators (Freedom House, 2013). The citizens (See table 1) of Russia rank the third highest in terms of social media use.

Table 1

Hours of Social Media Utilization

Countries in order of Social Media Engagement	**Average Hours Per Month**
Israel	11.1
Argentina	10.7
Russia	10.4

Note. Source, (Freedom House, 2013).

The United States is preparing a persona management system to counteract this rhetoric. The United States Central Command awarded a contract to Centcom, a California company, to create software that allows a single person to control multiple sockpuppets online. It is an online persona management service that allows a service member to control identities based all over the world (Cobain &Fielding, 2011). Each sockpuppet is required to have a backstory to secure plausible deniability. The intent of the program according to General David Petraeus is to counteract terrorist groups and the propaganda they post on blogs and social networking sites. Opponents are concerned that other governments will follow suit or United States citizens will be among the targets (Cobain & Fielding, 2011). This asymmetric warfare is found in other countries like Iran (Bardin, 2012).

In December 2008, Israel began attacking the Gaza strip, Israel enlisted Jewish volunteers around the world to flood counter-propaganda in blogs and social networking sites (Hulaimi,

2011). The strategy used sockpuppets to add credibility to the disinformation. During asymmetric warfare, the victim rarely is aware of the identity of the attacker. The United States government's strategic use and management of sockpuppets is a way to control the situation. Freedom House measured the level of Internet and digital media freedom (Freedom House, 2013). The definition Freedom House (2013) used came from the Universal Declaration of Human Rights, Article 19:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers. (p. 28)

Out of the sixty countries studied, only seventeen or 28% have freedom on the Internet, and 72% have partial or no freedom (See Appendix A - Internet Freedom in 60 Countries) (Freedom House, 2013). Another statistic discovered by Freedom House indicated that thirty-four of the sixty countries have declined in characteristics of freedom, including the United States (See figure 1).

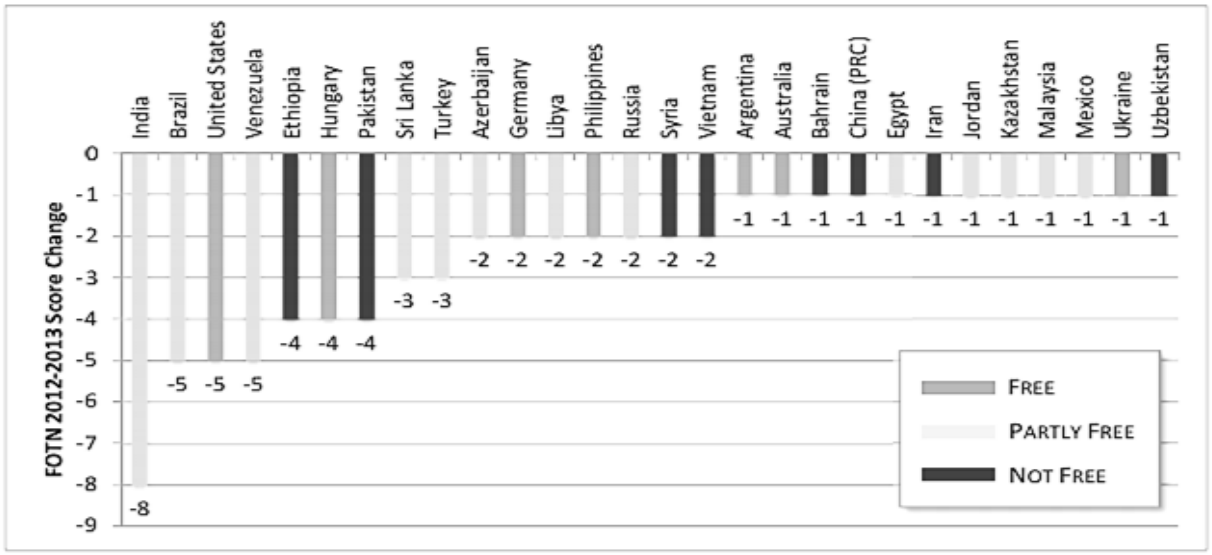


Figure 1. Loss of Internet Freedom, Freedom House, Freedom on the Net 2013: A Global Assessment of Internet and Digital Media, 2013, p.25

Jeffrey Bardin, Chief Intelligence Officer of Treadstone 71, presented at the International Conference on Cyber Conflict (CyCon) in Estonia (2012). He explained that the Iranian Republic Guard Corps (IRGC) is paying members of their group called the Basij to take down any anti-Iranian online presence. At the same time, they create pro-Iranian blogs, social network posts, and other propaganda. Bardin points out that these workers are paid $4.30 an hour to maintain the posts, which is higher than the minimum wage (Bardin, 2012). Iran wants Syria, Bahrain, Lebanon, and Palestine, including Hezbollah and Hamas, to hear the Islamic Revolution from their point of view. Bardin continued with, "[the] IRGC is very capable and the West shouldn't underestimate its adversary" (Bardin, 2012). From 2005 to 2012, a federal officer confirmed that Jeffrey Bardin located and shared contact numbers and other information gathered as a sockpuppet on Jihadist websites (Bennett, 2012). The FBI and United States military benefit from experienced sockpuppet users.

The government utilization of sockpuppets is a controversial topic. It may not have come to the forefront for the American public if not for the actions of a Hacktivist group called Anonymous. Anonymous exposed 70,000 emails from HBGary Federal. The emails contained information about a state-sponsored sockpuppet propaganda program (Ludlow, 2013). Furthering the controversy, Endgame Systems, offered services to other customers outside the United States (Ludlow, 2013). Russian and China have consistently denied allegations of using cyber-espionage and sockpuppets to gather information (Poduval, 2012).

Following the terrorist attacks directed toward the United States on September 11, 2001, social media spaces, blogs, and discussion groups became the ideal place to strengthen the terrorist message (Soriano, 2012). Many sockpuppet names appeared to join a psychological war on the United States. The best-known example is the Abu Hafs Al Masri Brigades, a fictitious

organization that claimed responsibility for various actions (Soriano, 2012). Government use of sockpuppets offers surveillance of these organizations. However, instances of Americans using sockpuppets can risk national security if they are exposed. According to judiciary subcommittee, there are reports that a sockpuppet revealed a picture from a soldier taken on patrol in Afghanistan that contained embedded data identifying his exact location (Subcommittee, 2010).

The United States Military legally can utilize and manage sockpuppets as long as it is directed towards foreign soil. The Smith-Mundt Act of 1948 "prohibits domestic dissemination of information designed for foreign consumption, as a way to ban domestic propaganda. By policy and practice, the [Department of Defense] DoD adheres to Smith-Mundt restrictions on domestic propaganda" (Duncan, 2013, p.131). Operation Earnest Voice (OEV) is a campaign by the United States Government. The purpose of the campaign is to utilize sockpuppets to maintain social media profiles that can spread positive messages about the United States. Ntrepid, the security company, created special software to create and manage multiple sockpuppets. The job of these sockpuppets is to post propaganda aimed at boosting the United States position around the world. The citizens of the United States, according to the security company, will not be targeted (Cobain & Fielding, 2011). The specifications required for the program are listed below:

- Fifty users simultaneously - 10 sockpuppets per user
- Appear to originate anywhere in the world
- Thorough background for each profile to support full identity
- Secure Virtual Private Network (VPN) to hide the operation
- Fifty static Internet Protocol (IP) addresses to enable agencies to manage the sockpuppets
- Nine private servers that use commercial hosting centers
- Data deletion after each session

Centcom spokesperson Commander Bill Speaks said, "The technology supports classified blogging activities on foreign-language websites to enable Centcom to counter violent extremist and enemy propaganda outside the US" (Cobain & Fielding, 2011, para. 6). General James Mattis, the 11th commander of Centcom, added, "OEV seeks to disrupt recruitment and training of suicide bombers; deny safe havens for our adversaries; and counter extremist ideology and propaganda" (Cobain & Fielding, 2011, para. 16). The OEV sockpuppet program offers unique counter-terrorism and intelligence capabilities to the United States.

There are different kinds of intelligence practices that are connected to sockpuppets. Open Source Intelligence (OSINT) collects information from open public systems. According to the US Army Field Manual 2.0, OSINT is "the discipline that pertains to 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" (*Open Source Intelligence*, 2012, p. 135). Open source refers to information that is given without the expectation of privacy. Types of OSINT include security feeds, public intelligence feeds, and public comments in blogs, social media, or Internet Relay Chat (IRC) channels (Miller, 2014). Human Intelligence (HUMINT) collects information from another human, either in person or through some means of communication. According to the US Army Field Manual 2.0, HUMINT is "the collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities" (*Open Source Intelligence*, 2012, p. 109).

Sockpuppets utilize a combination of these two systems. The creation of the false identity online and building a reputation for that sockpuppet in order to gain access to communities and

forums used by closed groups (Miller, 2014). Creating an online community account using the sockpuppet profile allows an intelligence analyst to create friendships and collect information. According to Jennifer Bosson and Johnathon Weaver's research, "Shared negative attitudes heighten people's feelings of "knowing" the attitude sharer" (Weaver & Bosson, 2011, p. 490). This targets specific groups for specific information, and necessitates a larger investment in time due to the obstacles that must be dealt with to gain trust and leverage (Miller, 2014). Jeffrey Bardin at Hacktivity (2012) put it this way,

> It's how you get into somebody's site, or someone's forum, or Facebook sites, and become a resident, a friend to them, and stay there for years to access their sites, and actually become one of them for quite a period of time. Clandestine Cyber Human Intelligence. That's where we're taking traditional spy tradecraft from the physical world, and, we're applying it to the cyber world. (2012, para.2)

A new study by the Mediterranean Council for Intelligence Studies' (MCIS) 2012 Intelligence Studies Yearbook points to the use of social media as "the new cutting edge in open-source tactical intelligence collection" (Fitsanakis & Bolden, 2012, para. 1). IntelNews.org's Joseph Fitsanakis, who co-authored the study, reports:

> We explain that Facebook, Twitter, YouTube, and a host of other social networking platforms are increasingly viewed by intelligence agencies as invaluable channels of information acquisition. We base our findings on three recent case studies, which we believe highlight the intelligence function of social networking. (Fitsanakis & Bolden, 2012, p.28)

Esti Peshin, Director of Cyber Services for Israeli Aerospace Industries, believes it is not difficult. "We want to create a comprehensive intelligence picture, rather than producing just one

single item of information, since that single item can be faked" (Novitski, 2014, para. 2). Peshin went on, "Israeli Aerospace Industries experiments have shown that it takes only 48 hours to create a believable and complex fake identity, with no less than a hundred Facebook friends who believe it is a real person. All it takes is opening an e-mail account" (Novitski, 2014, para. 2).

Jeffrey Bardin agrees that it starts with creating an email address, however, he feels strongly that it takes time to create viable and believable sockpuppets, "the main thing when you do this is actually patience; it takes a long time. There are sockpuppets I've had out there for many years, and these sockpuppets are still active today…" (2012, p. 1). He offers this example:

> At one time, I [Jeffrey Bardin] had multiple different sockpuppets on a cyber-Jihadist site; one of them had a lot of experience on this site and was well respected. And I had another junior member on this site, and I wanted to get another layer into this site with my senior member, so what I did is I set up my junior member, my other personality, and I made him make some things that were contrary to bin Laden. He said it online. And over here at my senior sockpuppet, I called him out, got him kicked off this site, and because of that I got better street credentials on this site. So, it's a way that you can use tools and techniques to get in and penetrate further into these different sites. (Bardin, 2012, p. 3)

Rick Holland, principal analyst at Forrester Research serving Security & Risk Professionals (2013), concurs with Mr. Bardin, "you will have to build knowledge, capabilities, and maturity over time" (p.9). He feels strongly that an intelligence analyst must have patience and work diligently to collect information from the target. He proposes steps that may take years to work through:

1) Lay a solid foundation of essential capabilities

2) Establish buy-in

3) Identify required staffing and skill levels

4) Establish intelligence sources

5) Derive actionable intelligence (p.9)

Initially, it is critical to understand the target that is under surveillance. Knowing the target is an important factor to an Intelligence agenda (Miller, 2014). It is critical to understand the complete picture of the target. Historical, cultural, linguistic, and political information are important in the development of a sockpuppet (Bardin, 2012). Background research is essential in order to have an intelligent conversation with the target. The tools that appeared in Jeffrey Bardin's Hacktivity presentation in 2012 are shown in Table 2.

Table 2

Sockpuppet Tools

Website	**Purpose**	**Details**
Fakenamegenerator.com	Identity creation	Complete identity creator with all details including country origin, language, and identification documents, offers adjustable parameters, .csv or SQL
Identitygenerator.com	Identity creation	
Crypto.cat	Encrypted chat	After chat the conversation disappears in 30 minutes
Touchgraph.com	Connectivity browser	Advanced cluster computation reveals inherent groupings
Paterva.com/web6/ products/maltego	Open Source Intelligence program	Determines the relationships and real world links between several entities
Httrack.com	Offline browser utility	Download a website from the Internet to a local directory
Topsy.com	Search engine	Tracks data on Twitter and makes it searchable
Twopcharts.com	Search engine	Tracks data on Twitter by city or language
TinEye.com	Image reverse search engine	Put in an image and it will locate it

Note. Source, (Bardin, 2012).

Sockpuppets require vigilance and patience, but research indicates competence and skill are of equal importance. Without these characteristics, detection of the false identity is likely. Detection studies include a variety of technical and logical processes to attempt to determine the legitimacy of an online persona. Common sense proponents remind the public that skepticism is positive (Koenigs, 2011). To identify a sockpuppet researchers point out that a little research can go a long way. Initially, complete a Google background check, look for inconsistencies, for example, the average Facebook user has 130 friends, if the number is not close to that, then suspicions begin to rise (Koenigs, 2011). More formal sockpuppet detection includes Clickstream analysis, SybilRank, Paired post examination, linguistic differences among users, and time profiling combined with stylometric analysis. Clickstream detection is an algorithm designed to monitor user's clicks (Wang et al., 2013). Most detection systems search predict patterns of typical use and therefore identify false identities. SybilRank is a system designed to rank an identity on a given number of factors to determine its viability (Yang, Cao, & Sirivianos, 2012).

One sockpuppet detection study combined time profile-based matching for matching based on the publishing time of posts and stylometric matching based on the written post itself (Johansson, Kaati, & Shrestha, 2013). One of the simplest techniques focused specifically on online communities. It looked for pairs of aliases with heightened similarities (Zheng, Lai, Chow, Hui, & Yiu, 2011). Lastly, Cornell researchers worked on an algorithm that proved to be effective ninety percent of the time (Ott, Cardie, & Hancock, 2012). It examined online reviews within travel websites. Only sixty percent of human detectors used in the study could identify the fake reviews. The research determined that sockpuppet reviews included more exaggeration, filler, and increased use of pronouns, verbs, and adverbs (Ott, Cardie, & Hancock, 2012).

Discussion of Findings

The purpose of this research was to examine the utilization and management of sockpuppets within online communities. What are the ethical and legal boundaries in the use of sockpuppets within civilian online communities? What is the role of sockpuppets in the intelligence community?

The term sockpuppet refers to the utilization of an online identity for deception. The boundaries of ethics and the law in sockpuppet use begin with the intent of the user. The sockpuppet itself is not good or evil. The human behind the sockpuppet chooses its path. Therefore, using a sockpuppet alone is not unethical or illegal, but the actions of the sockpuppet, which are controlled by the user, might be.

In 2010, an attorney named Raphael Golb was found guilty on thirty out of thirty-one charges including identity theft, aggravated harassment, and criminal impersonation (Associated Press, 2010). The conviction was unique because the charges were all related to using multiple sockpuppet accounts to harass and impersonate scholars he alleged discredited his father, Norman Golb. Mr. Golb defended his activities as "satirical hoaxes" that he claimed should be protected by free-speech rights (Associated Press, 2010, para. 4). He was disbarred and sentenced to six months in prison but remained free on appeal on $25,000 bail (Associated Press, 2010). Carol Berkman, the judge in the Raphael Golb case, said his conviction was about actions, not ideas. "It's not his words, but his conduct, it is still a crime to imitate people in the manner that [Golb] did . . . The victims felt invaded and hurt by this" (Associated Press, 2010, para. 8). Mr. Golb's intent began as an innocent son defending his father, however, he crossed the line from unethical to illegal when he impersonated others and attempted to destroy their careers.

On the other side of the spectrum, Ben Franklin utilized several sockpuppets to voice different opinions and views. He did not want his political reputation to influence how people viewed his pieces. Anonymity within online communities is a complex subject that elicits debate. The First Amendment guarantees freedom of speech, however, it does not guarantee how that communication will be viewed and criticized. The advent of sockpuppets can be linked to the desire to influence other people without the consequences associated with one's actual identity. Anonymity offers the ability to express an opinion without the fear of retribution or condemnation. Some would argue that this only shields criminals and the dishonest. However, anonymity online allows people to examine problems, take part in discussion, and look for advice privately. The most contentious characteristic of sockpuppets is the idea that it offers chances for people to push ethical and legal boundaries without accountability.

One of the first sockpuppet cases that gained public attention was the 2008 case involving Lori Drew and Megan Meier. Megan Meier interacted with a boy named Josh Evans who claimed to be a 16-year old boy being homeschooled in a nearby town (Schwartz, 2009). However, Josh was a sockpuppet. The intent was allegedly to gather information about Megan, and use it later to humiliate her in retaliation for alleged rumors that Megan spread about Lori Drew's daughter. However, that intent escalated throughout the sockpuppet relationship. Initially, it crossed an ethical boundary because the intent was to defame another person, but the intent moved into the legal realm when Ashley Gills, posing as Josh Evans, insinuated that Megan should do harm to herself (Schwartz, 2009). Lori Drew, the co-creator of the sockpuppet, referred to the actions as a joke. Ashley Gillis, an 18-year old accomplice, claimed that she sent the final message to stop communications. The final message read, "Everybody in O'Fallon knows how you are. You are a bad person, and everybody hates you. Have a shitty rest of your

life. The world would be a better place without you" (Schwartz, 2009, p. 407). Megan Meier killed herself hours later.

Attorneys tried the case under the Computer Fraud and Abuse Act (CFAA) that Congress passed in 1986, based on MySpace terms of service. However, the charges were not strong enough to stick. After this case, Missouri's law now specifies that cyber harassment, particularly adults over 21 harassing children under 18, is a felony punishable with up to four years in prison (Meredith, 2010). This criminal case addresses the boundary of ethics and the law. On one side, it appears that Lori Drew directly caused Megan's death using a sockpuppet to torment Megan. The sockpuppet befriended Megan, communicated and shared emotions online, and then turned on her. In the real world, unless in written letters, this would be a case of he said she said. There would be little proof that Josh said hurtful things to Megan. Even if he did, and he was real, would that be enough to hold him criminally accountable for her death? Megan chose to claim her own life. Lori Drew and her daughter, along with Ashley Gills, must live with that for the rest of their lives. Whether offline or within an online community these actions ethically crossed every line, but legally it was not enough to hold the sockpuppeteers accountable.

Ethics are a subjective discipline. Criminals, victims, and the legal system do not always have the same perspective. Shawn Sayer's ex-girlfriend was not taken seriously by authorities even with protection orders in place (Morris, 2012). James R. Brisson's victim was not protected from the sexual predator that failed to register his sockpuppets with the state (Farrar, 2012). Ethically, Shawn Sayer and James R. Brisson Jr. believed their behavior was warranted. Their own personal ethics allowed them to make the decisions that they did. However, the ethics of cyberspace and the societal standard would disagree. In cyberspace, ethics are critical to informing and transforming according to Lohrmann (2013), they assist the user in navigating

online communities. Mr. Sayer and Mr. Brisson ethically became lost. Criminally, cyberstalking and cyberharassment are punishable in forty states (National Conference of State Legislatures, 2013). The critical word in every law is the word "intent". These men were ethically and legally accountable for their actions within the online community and the real world results.

"While many states have taken steps to account for the increased dangers posed by Internet victimization, there is a need for more complete coverage in this area of law to account for the full spectrum of problematic behavior in the cyber context" (Schwartz, 2009, p. 409). The unethical use of a sockpuppet within online communities needs regulations. The intent to do harm goes beyond anonymity and free speech. Toleration for the use of a sockpuppet within an online community for fraud or victimization cannot stand. Civilian online communities look to the legal system for assistance in actions that are against the law. However, online communities do not have a consistent vocabulary, and laws regarding sockpuppets and other online issues awkwardly intersect and have vague language (Schwartz, 2009). Some state laws address anonymous communications, but other states have not included the use of a sockpuppet within their legislation. To create a safe atmosphere within the online communities, it is essential to have consistent standards of behavior. The behaviors are protected by the Constitution if revealing a true identity deters the expression of ideas because the person is afraid of retribution or does not want publicity ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961). However, the Constitution is support based on the deterrence and direct government action or a disclosure provision can supersede that protection ("The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil," 1961).

The United States Military has the authority to use Facebook, Twitter, and other social media outlets for intelligence operations as long as it is directed strictly at foreign targets

(Duncan, 2013). The United States population prolifically uses social media, but not as much as other countries. Statistics indicate that the United States is at the bottom of the top ten countries based on the number of hours engaged in social networking (See table 3).

Table 3

Top Ten Social Media Utilization Countries

Countries in order of Social Media Engagement	**Average Hours Per Month**
Israel	11.1
Argentina	10.7
Russia	10.4
Turkey	10.2
Chile	9.8
The Philippines	8.7
Colombia	8.5
Peru	8.3
Venezuela	7.9
Canada	7.7
United States	7.6

Note. Source, (Freedom House, 2013).

Laws, regulations, and restrictions throughout the world are censoring and punishing users that do not comply, and global Internet freedom continues to decline as a result of monitoring and censorship (Freedom House, 2013). Many countries will arrest citizens that post any political statements on social media, and sockpuppet use is difficult due to registration laws governing online communities. South Korea maintained a law that mandated its citizens register their real names when participating in online communities (Freedom House, 2013). This law was recently overturned, but the persecution continues in several places around the world. It is understandable why sockpuppet use is controversial. However, the intelligence community utilizing sockpuppets to maintain homeland security is warranted. The temptation of unethical behavior still exists even within government, but a knowledgeable watchdog for our safety may

be more important. Although the United States is not involved in the extensive censorship that happens around the globe, in recent years the United States has increased surveillance. Since September 11, 2001, national security is a high priority, and it has expanded to meet new demands. The passage of the USA PATRIOT Act boosted the expansion and growth of national security. The legislation provided allowances for prevalent surveillance, collaboration between the Pentagon and the private sector, and aggressive legal actions (Harrison, 2004). With it came new and changed trepidations for United States citizens trying to protect their privacy, safeguard their identity, and preserve their right to anonymity.

The government utilizes sockpuppets to assist in the protection of people in real and online communities. The intelligence community employs sockpuppets to gather intelligence, infiltrate hostile groups, and further the United States position in online communities. A sockpuppet fosters a relationship with potential threats and builds trust to facilitate open conversation. Jennifer Bosson and Johnathon Weaver's research in 2011 highlighted the connection between individuals that share negative attitudes and feelings toward the same target. This connection encourages a higher level of trust than an American with opposing viewpoints could create. It creates a relationship and opens the door to increased information flow. A sockpuppet account, or multiple sockpuppet accounts, interact and produce a level of intelligence artifacts that a basic open source intelligence search would leave undiscovered. It is social engineering within online communities.

In Jeffrey Bardin's courses at Utica College, students completed an assignment to create a sockpuppet using fakenamegenerator.com. This sockpuppet obtained Facebook friends and Twitter followers. The sockpuppet required a realistic resume posted on LinkedIn, and a background for a specific context of the student's choice. This assignment allowed students to

engage in practice, and research what an intelligence analyst experiences. Information gathered within the constraint of the course offered a powerful example of sockpuppet utilization. The management of such an entity appeared daunting to students within the course. It required nurturing rapport, building credibility, and managing various levels of creativity. The boundaries of sockpuppet use within this course compete against inexperienced users and the vast online communities. Utilizing a sockpuppet for intelligence gathering takes time and experience to master, but it produces vital and powerful information about a potential enemy.

Managing one or multiple sockpuppets is a time consuming and delicate task. Some feel it is a voluntary task to agree to. The British Crime Writers put together a petition that simply stated no more sockpuppets here and asked for signatures. All told, they received roughly 400 signatures. Ironically, it is possible that many of the signatures were sockpuppets. At the ground level, sockpuppets are complex to create, and painstaking to maintain and manage. Jeffrey Bardin teaches how to create a sockpuppet. The table below is a checklist of his basic recommendations for initial startup and management (See table 4).

Table 4

Checklist for Sockpuppet Creation

Items Necessary to Create Sockpuppets
□ Create email addresses
□ Document Sockpuppets
□ Maintain Anonymity
□ Virtual Machine per sockpuppet
□ Choose and learn your OSINT tools
□ Acquire pre-paid phones
□ Establish Twitter and Facebook accounts to match personas
□ Create a YouTube site tying to Twitter, and Facebook
□ Setup IRC accounts to match sockpuppets
□ Need to understand Open source and HUMINT
□ Need historical understanding
□ Need religious understanding

□ Need cultural understanding
□ Need linguistic skills
□ Maintain operational security (OPSEC)
□ Social Engineering skills
□ Validate sources
□ Learn intelligence analysis
□ Critical thinking
□ Cognitive bias
□ Taxonomy

Note. Source, (Bardin, 2012).

This list represents a checklist of the multitude of items necessary for an accurate depiction and safely anonymous sockpuppet. An experienced practitioner hones the tradecraft to assure consistency and security. Mr. Bardin uses dozens of sockpuppets to monitor and interact within various facets of online communities (Bennett, 2012). There are opposing viewpoints in the management aspect related to this clandestine intelligence. Major R. J. O'Conner, Army Special Forces, stated in 2012, "This is a domain of warfare where an individual can make a difference, personalities are acceptable in this domain" (Bennett, 2012, p. 1). However, the director of the Homeland Security Policy Institute at George Washington University, Frank Cilluffo, explained, "Someone needs to be the quarterback to coordinate these things, if it's not coordinated in any way, it can cause problems for the good guys" (Bennett, 2012, p.1). It appears that Washington agreed. The bid for an online persona management system went out before Mr. Cilluffo made the statement.

The civilian online communities impacted by malicious and criminal sockpuppets may heed the call for detection programs as a form of management. Current law is utilized to manage sockpuppets in these online communities. Identity theft, impersonation, cyberharassment, cyber stalking, and computer fraud have applied to sockpuppet cases in courts around the globe. Civilian online communities need specific laws to manage sockpuppets. Federal legislation with specific language may offer management and deterrence to criminals and those looking to

employ fraudulent behaviors. In some cases, a healthy dose of vigilance and skepticism are the only management necessary.

Detection programs may help civilian online communities police their own websites. Promising research in determining false reviews and fake comments offers businesses and academic institutions the ability to monitor and expunge suspicious content. Ott, Cardie, & Hancock (2012), determined that an algorithm for detecting fake travel reviews could identify false information in excess of ninety percent of the time. For larger corporate websites with business and financial loss at stake, a solution as simple as an algorithm could save the bottom line. However, if the algorithm drops in its accuracy, then the business would be back where they began. Who would maintain the algorithm and monitor its success? Other detection systems target personas themselves. Matching profile information or applying a complex set of mathematical rules to all online communities may not be efficient. Since it is in its infancy, and there are few options, detection in the form of awareness and prudence may be the best option.

The formal governmental management system created by Ntrepid is a different type of management. This management is for maintaining a database of sorts for purposefully created sockpuppets. The flexibility of this system may not offer the necessary tools, especially with detection programs on the rise. Each persona has many characteristics of a handcrafted sockpuppet, however; it cannot attain the level of personability that someone like Jeffrey Bardin strives for in his meticulous sockpuppet development. The Ntrepid sockpuppet can appear to originate anywhere. Each persona has a background and history supported by seemingly historical, technical, cultural, and geographic data that remains reliable (Cobain & Fielding, 2011). The concern is the believability and flow of the sockpuppets developed by Ntrepid. This contract may be the piece of data that caused our Internet freedom to decline slightly. Jeffrey

Bardin maintains Excel spreadsheets with detailed data of every sockpuppet he maintains. He updates the data after sessions to insure the accuracy before the next encounter. The comparison suggests that the management system is necessary; however, the type of management system is uncertain. It is unclear if a structured and machine-like system will collect the information desired by the government. It is less demanding in terms of man-hours and diligence, but intelligence at this level does not define itself by speed or ease.

Recommendations

Using and managing a sockpuppet is an endeavor that necessitates vigilance, training, and proficiency. The role of the sockpuppet is developing across the Internet, and as such, it is important to recognize the historical significance of pseudonyms and anonymous speech. Additionally, it is critical to remember the unique, predominantly autonomous nature of online communities, and the negative impact that mandated identification could have on free speech. The value of anonymity found in the use of a sockpuppet is profoundly linked to the establishment of the United States of America. Although John Hancock and several others signed the Declaration of Independence and the Constitution with their real names, pseudonyms forged the journey to the freedoms outlined in those documents.

These early examples of sockpuppets disseminated publications that united colonizers to fight for independence. The question of anonymity was not as important as working together to fight persecution. The Silence Dogood letters, Common Sense, The Federalist Papers, and other writings exemplify an author's purpose for anonymity. This initial use of sockpuppets during the American Revolution carved a precedent for the importance of anonymity and pseudonymity in the United States, and, therefore, led to the First Amendment of the Constitution.

As the world continues to struggle with the pressure to challenge authority anonymously, sockpuppets in online communities present a new playing field. Online communities are the most innovative forum for the expression of opinion since man could communicate, but many stakeholders feel they have reasons for the suppression of anonymity, and the subsequent hatred of sockpuppets. Nevertheless, others vehemently defend the critical necessity of sockpuppets in online communities.

Currently, online community networks such as Amazon, Facebook, Twitter, Yahoo, and Yelp do not have accountability for the content posted within their site. Terms of service, privacy notices, or conditions of use clauses for online communities state that they are not responsible for content published on their site by others. They do not have a vested interest in the content, therefore, they do not attempt to alter or enforce even the basic terms of service. The online community reserves the right, but not the obligation to edit content that violates the terms. The agreements additionally explain that false identities [sockpuppets] are not allowed.

If these online communities were required to begin policing themselves for these violations, then each entity would be held accountable for the perceived intent of its members. As a self-governing community, the enforcement of such policies might include charging a fee for each additional account name, and the gathering of more in depth identifying information from each member of the community. This policy change would be a radical new process. Moreover, the problem with a shift of this magnitude is that it would create an imbalance between the haves and have-nots. Those that could afford to create multiple sockpuppets would rule the Internet while those without the resources would not have their voice heard. Additionally, online communities within this system of accountability might ban membership to questionable users. Selective or segregated membership forms a rift in the connectivity of

cyberspace. The risks of online community direct accountability outweigh the benefits, and, therefore, are not recommended.

In the public sector, the intelligence community utilizes sockpuppets the same way as an undercover agent is used offline. Sockpuppets are the eyes and ears within a suspicious online community or near a particular community member. Sockpuppets become infiltrators, data-miners, and observers of potential national security risks within online communities. In the process, the intelligence community risks boundaries of ethics and legalities, not to mention concerns related to the balance of power. As a result, the areas requiring review are the inconsistencies in the development of sockpuppets, and the best techniques and methods related to their use.

Based on a review of available literature the current recommendations for sockpuppet use include; (1) federal legislation and management defining and clarifying criminal use of a sockpuppet, and (2) a best practices manual for the intelligence community to standardize development, training, and utilization of sockpuppets.

Federal legislation and management defining and clarifying criminal use of a sockpuppet. Without reliable self-governance, the legal system must address sockpuppet crime with cautious scrutiny. Legal management of sockpuppets in civilian online communities is unpredictable, dichotomous, and arbitrary. Using a sockpuppet has both positive and negative purposes, and prohibiting its use, sacrifices the good to punish the bad. Ethical and legal boundaries related to sockpuppets within online communities are unclear. When a member of an online community chooses to use a sockpuppet, it is an ethical decision how and what that sockpuppet will become. Ethical choices are subjective and personal, however, when the intent becomes to inflict harm, the sockpuppet crosses legal boundaries. Therefore, laws need to

address these possibilities and clarify definitions and consequences based on intent. Careful and focused work needs to occur within the Legislative Branch of government to clarify and define legal statutes related to actions and procedures when a sockpuppet crosses the line from unethical behavior and bad choices into illegal intent and harmful conduct.

Recent cases involving sockpuppets appear to believe that laws should apply the same way to conduct in online communities as they do to conduct in offline communities. Current federal laws do not specify online sockpuppet behaviors in separate legislation. There is a danger that an imbalance in legal consequences for offline versus online behaviors could result in criminals congregating more in one community than in the other. Criminals will naturally seek out the environment that affords the least consequences. Current federal guidelines should be reviewed carefully in order to enforce and protect all citizens throughout the vast reach of cyberspace.

There are a limited number of states with legislation that directly indicates electronic, online, or Internet identity crimes. If a state does not have specific wording attorneys attempt to get a case thrown out because an electronic, online, or Internet method is not mentioned in the law. The definitions are vague and interpretable. However, judges have ruled that the laws do not need to indicate the means by which the crime occurred. On the other hand, the possible outcomes of litigation in states that do not have specific language related to electronic, online, or Internet identity crimes will not be as clear. This lack of clarity may lead to a power struggle regarding this developing topic.

Therefore, while it may be true that the means of impersonation, fraud, stalking, or harassment is unimportant, what is at issue is where the crime takes place. It is difficult, if not impossible, to argue that online communities are anything but Federal jurisdiction. The act of

going on the Internet and interacting within an online community automatically creates a federal venue. Electronic, online, or Internet involvement is not simply a how; it is moreover a where in terms of legislation consideration.

On the other side of the spectrum, applying CFAA to an identity crime like Drew vs. Meier is similarly inappropriate. The verdict in this case epitomizes the inexplicable lack of federal law definitively dealing with the issue of the criminal use of sockpuppets. Current cyberstalking laws do appear to be effective once a victim is heard. These laws garner more attention due to the perceived violent potential. Increased analysis is critical to safeguard the reliability of current laws, and federal legislation is critical to ensure consistency and systemic application. A law that identifies the turning point of sockpuppet utilization focused on the intent of the user is necessary. A federal statute that would address the criminal use of sockpuppets should state: a person is guilty of identity fraud and/or criminal impersonation if he or she creates a fake profile unrelated to a specific person, impersonates another person by creating a fake profile of another person, or by wrongfully gaining access to the victims account through other electronic means; with the intent to harm, intimidate, or threaten subsequently causing the victim severe psychological, emotional, or financial harm. Electronic means includes, but is not limited to, Internet websites, social networking sites, email websites, dating websites, and other Internet websites requiring personal information to gain access.

Finally, the general public struggles to stay informed of technological changes. Therefore, the legalities related to online communities foster public suspicion and fear. It is a complicated area to sufficiently and respectfully delineate. However, it is clear that the critical determining factor in these cases is intent. Precise adjudication with a sharp eye towards the Constitution and Declaration of Independence is necessary for confidence within the populace.

Best practices manual for the intelligence community to standardize training and utilization of sockpuppets. Cyber intelligence is an analytic field that depends on information gathered from multiple sources within its community. The intention in this community is to inform decision makers on matters concerning operations and national security. When the data is analyzed and placed in context, the information becomes intelligence. Quality intelligence reduces uncertainty and allows more time for careful and economic choices. It is necessary for the intelligence community to gather information from a variety of sources. It is important for the decision makers to support action with a complete picture of what is occurring and why.

One way the intelligence community gathers this information within online communities is by utilizing sockpuppets to collect financial, legal, social, or technical facts about an adversary. This operational intelligence helps decision makers elect to take a particular approach based on the given information, therefore, not wasting time or money on alternative paths that will not lead to reaching the objective at hand. Utilizing a sockpuppet to reveal adversarial tactics, techniques, and procedures provides an unfettered view into their organization. It allows the decision makers the information they need to devise defenses and know who and what the threats are before they happen. In order for the intelligence community to successfully utilize and manage sockpuppets they need to identify best practices, recruit or train qualified analysts, maintain current and accurate data about official sockpuppet use, and devise an assessment of sockpuppet effectiveness. Research indicates that this cannot be completed with a mass sockpuppet management system. Best practices of sockpuppet use must include:

1.) Standardized training that focuses on the intelligence cycle as a framework

2.) Cyber street smarts - target area subject matter expertise

3.) Hands-on practice with tools that assist planning and gathering

4.) Clear and precise requirements for the purpose and data to be collected

5.) Thorough understanding of collection and analysis methods and tools

6.) Standards for maintenance, assessment, and continued sockpuppet utilization

The recommendations are directly correlated with the intensity and detail necessary to create and maintain a sockpuppet at this level. The intelligence cycle is a logical framework that feeds back on itself and responds to the current threats and needs. The planning and direction stage helps an analyst identify the adversary being examined. At this stage, the sockpuppet or sockpuppets must be developed and tailored to the online community being infiltrated. Critical to mission success are the characteristics selected for the sockpuppet including, name, nationality, age, and location. An understanding of the target's culture, religion, language, and history must play a part in the development of the sockpuppet. Ntrepid's specifications for an online persona management system that is standardized in number and output, may not work for this detailed and highly personalized purpose. It is important for this process to be custom-made, and it is unclear if a persona management system could accomplish the necessary level of intimacy.

Once the sockpuppet is complete and solid, then it is important to focus on the requirements of the task. The direction of the investigation and required depth of infiltration maintain focus for the analyst using the sockpuppet. What are the desired objectives and outcomes of the task? When is the intelligence needed? Who is the audience for the intelligence being gathered?

There are other tools for the development, collection, processing, and analysis stages of the intelligence cycle. Tools that maintain Internet address anonymity in addition to virtual machines allow the analyst work unobtrusively. Specific software or spreadsheet programs are helpful to keep accurate and complete records of all sockpuppet demographics and activities.

Collection and analysis methods include social media, keyword analyzers, link analysis tools, and website collectors. These methods and processes are fluid and change often, but there are some tools that have remained useful for several years. These tools help maintain the reliability, validity, and sensitively of the information. At this point, the sockpuppet user begins to make judgments and decisions about the target based on gathered information.

The analysis of the information is a process of developing inferences about the target based on the data collected and using that to create actionable intelligence. Interpreting conversations, actions, images, and other media pull the information together and create a larger picture. An analyst must evaluate the information to decide if further collection is warranted. The inferences must be credible and consistent; therefore, accurate records of sockpuppet details become crucial to the investigation. Software such as Analysis of Competing Hypothesis (ACH) would be helpful and should be included within best practices. Arranging and sorting these records begins to paint a picture while documenting intelligence activities at the same time.

Research and development should establish national best practices related to sockpuppet utilization within the intelligence community to facilitate connectivity across the information continuum. Technology continues its fast-paced evolution, and the lines between the public and private sectors become blurred. The United States must integrate government methods and techniques with private sector methods and techniques to create the necessary operational intelligence. Sockpuppets are a key tool for analysts to bridge that gap.

Future Research

Sockpuppets are an exponentially shifting component of online communities and the Internet in general. A vast amount of topics remain undiscovered. There are several studies discussing a real identity policy versus a detection algorithm application. Several pundits feel the

solution lies in limiting an individual online to their actual offline identity, without exception. Others feel that is an unconstitutional perspective, but profess that detection algorithms offer online communities the ability to root out harmful fake profiles.

Another potential area of research is the idea of online community accountability through self-governance. The above recommendations discounted it because of the potential segregation if fee based identities were the best way for communities to pass the accountability on to the user. There may be a way to make online community owners police their own site.

Continued examination of sockpuppet utilization and management is important to the field of intelligence because it provides an innovative tool within social networks to gather information. However, technology is changing so quickly that it is crucial to avoid stagnation in this area of research. Social media will continue to be a valued source of information in various situations. Sockpuppets within online communities are the counterparts of offline undercover agents. They are poised to be an eyewitness, as well as, the first to disseminate information about an emerging event.

Further research might look into forging a powerful collaboration construct to share the information available to an analyst in all phases of sockpuppet utilization and management. Informal and formal collaboration across agency, network, and classification level is an area that requires consistency. The more security agencies work together and share information about targets, the easier it will be to keep up with the changes and complex nature of those changes. Reforming the intelligence process to align with the information age is vital but it necessitates procedural changes. The intelligence community needs integration in all aspects of the intelligence cycle. The speed at which technology changes and travels necessitates the centralization of analysts and the process in general. In the past, it was possible to segregate

parts of intelligence gathering and piece things together. However, currently information travels and changes too fast for that type of process.

Another potential investigation involves a system designed to analyze social media. It is critical for intelligence analysts to comb social media for potential warnings of impending actions. Research and development of an automated system that could assist in the analysis of the dynamic environment of social networks could offer a significant advantage to our decision makers. Additionally it would offer analysts that utilize sockpuppets current information to aid in accurate interaction and strategic analysis. A strong open source platform that has the flexibility to change search parameters and geo-locate a search based on breaking events or emerging threats could make the difference in sockpuppet attainment. Research into the development of such a system would need to consider several factors. A system of would need, at the most basic level, to provide a warning. It would need to identify specific, credible threats and monitor adversarial conditions. This system would need to utilize ontology to create the ability to predict likely developments or future actions by conducting trend, pattern, association, and timeline analysis. It would be critical to research the advantages and disadvantages of allowing automation of geospatial location of adversaries, deception detection, and monitoring of target groups.

Lastly, the psychological impact of long-term sockpuppet use on the analyst may be an area to explore. Sockpuppets require significant effort to develop and maintain if they are to be believable and gather powerful, actionable intelligence. The depth that an analyst interacts may be an area of concern. How do analyst's function within two worlds at the same time? An undercover agent immerses himself or herself in one community or group. An intelligence analyst may manage several sockpuppets in various communities simultaneously. Multi-tasking

at this level is a new topic that online communities bring to the forefront. An experimental study of live sockpuppet interactions and reactions would provide insight into utilization and outcome. The researcher would create a group of sockpuppets populated with multiple perspectives, including positive and negative. The sockpuppets would interact to create a buzz, debate each other, and follow a storyline through to a planned end. The experiment would encompass how the interaction with outside members of online communities influences the pre-determined story and the analyst. Some questions the researcher might focus on include; can the original storyline be maintained to completion? How often do you have to tweet, post, blog, etc. to maintain or build a community? What tools can be used to automate sockpuppet activity? Could the characters/sockpuppets have pre-determined conversations? Could an autobot be created to engage the characters in a humanistic manner? How does the analyst psychologically handle multiple personalities and offline interactions?

References

Associated Press. (2010, November 18). NY lawyer gets jail in Dead Sea Scrolls case. Retrieved from http://www.foxnews.com/us/2010/11/18/ny-lawyer-faces-sentence-dead-sea-scrolls-case/

Bardin, J. (2012, November 21). So you want to be a cyber-spook open source intelligence. In *Hacktivity 2012*. Retrieved from http://www.youtube.com/watch?v=u5mSJidUH0Q

Bennett, B. (2012, September 17). Civilian 'hacktivists' fighting terrorists online. Retrieved from http://phys.org/news/2012-09-civilian-hacktivists-terrorists-online.html

Brooke, C. (2012, September 03). The author caught out praising his own books on Amazon... and writing disparaging reviews of his rivals' works. Retrieved from http://www.dailymail.co.uk/news/article-2197294/The-author-caught-praising-books-Amazon--writing-disparaging-reviews-rivals-works.html

Chen, Y., Fay, S., & Wang, Q. (2003, February). *Marketing implications of online consumer product reviews* [PDF].

Cobain, I., & Fielding, N. (2011, March 18). Revealed: US spy operation that manipulates social media. Retrieved from http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

The Constitutional right to anonymity: Free speech, disclosure and the devil. (1961). *The Yale Law Journal, 70*(7), 1084-1128. Retrieved from http://www.jstor.org/stable/10.2307/794351?ref=search-gateway:25503cf11024a2ca9e983e06af9b2dc9

Digital Media Law Project. (2010, March 23). United States v. Drew. Retrieved from http://www.dmlp.org/threats/united-states-v-drew#description

Dimiero, B. (2013, October 20). Fox news reportedly used fake commenter accounts to rebut critical blog posts. Retrieved from http://mediamatters.org/blog/2013/10/20/fox-news-reportedly-used-fake-commenter-account/196509

Dohse, K. A. (2003, Fall). *Fabricating feedback: Blurring the line between brand management and bogus reviews* [PDF]. Maryland Law Review.

Duncan, K. A., Major. (2013). *Assessing the use of social media in a revolutionary environment* (Master's thesis, Naval Postgraduate School, 2013) (pp. 1-153). Monterey, California: Naval Postgraduate School. Retrieved from https://calhoun.nps.edu/public/bitstream/handle/10945/34660/13Jun_Duncan_Kirk.pdf?sequence=1

Dwyer, J. (2012, September 25). The Internet: Puppet theater for a new age. Retrieved from http://www.nytimes.com/2012/09/26/nyregion/sock-puppetry-time-honored-tradition-thrives-online.html

18 U.S. Code Â§ 3521 - Witness relocation and protection. (1984, October 12). Retrieved from http://www.law.cornell.edu/uscode/text/18/3521

Elsner, K. (2013, November 27). China uses an army of sockpuppets to control public opinion – and the US will too. Retrieved from http://guardianlv.com/2013/11/china-uses-an- army-of-sockpuppets-to-control-public-opinion-and-the-us-will-too/

Farrar, C. (2012, April 2). Man coerced tenant to have sex, police say. Retrieved from http://www.sentinelsource.com/news/local/man-coerced-tenant-to-have-sex-police-say/article_00d54e19-ffdc-5181-a2be-7d96bf1e32da.html

Fitsanakis, J., & Bolden, M. (2012, February). Social Networking as a Paradigm shift in tactical intelligence collection. Retrieved from http://www.rieas.gr/images/mcis2012.pdf

47 U.S. Code Â§ 223 - obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications. (2012). Retrieved from http://www.law.cornell.edu/uscode/text/47/223

Freedom House. (2013, October 3). *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media* (Rep.). Retrieved http://www.freedomhouse.org/sites/default/files/resources/FOTN%202013%20Summary%20of%20Findings.pdf

Gitomer, S. R. (2013, April 15). Cyberstalking: A new phenomenon. Retrieved from http://www.tourolawreview.com/2013/04/cyberstalking-a-new-phenomenon/

Harrison, D. L. (2004). The USA PATRIOT Act: A new way of thinking, an old way of reacting, higher education responds. *North Carolina Journal of Law & Technology, 5*(2), spring, 177-212. Retrieved from http://www.ncjolt.org/sites/default/files/harrison.pdf

Hill, K. (2012, July 18). The dogged digital detective work that busted an online harasser. Retrieved from http://www.forbes.com/sites/kashmirhill/2012/07/18/ the-dogged-digital-detective-work-that-busted-an-online-harasser/

Holland, R. (2013, January 15). *Five Steps To Build An Effective Threat Intelligence Capability* [PDF]. Cambridge, MA: Forrester Research, Inc.

Hosenball, M. (2008, May 24). Intelligence: Cyber-spying for dummies. Retrieved from http://www.newsweek.com/intelligence-cyber-spying-dummies-89913

Hulaimi, W. A. (2011, March 20). Sockpuppets doing rub-a-dubs on the net. *New Strait Times Press,* p. 21.

Independence Hall Association. (2014). First Amendment rights. Retrieved from http://www.ushistory.org/gov/10b.asp

IT Law Wiki. (2014). Wikia-Sockpuppet. Retrieved from http://itlaw.wikia.com/wiki/Sockpuppet

Johansson, F., Kaati, L., & Shrestha, A. (2013, August 25). Detecting multiple aliases in social media. Retrieved from http://www.academia.edu/5117526/Detecting_Multiple_ Aliases_in_Social_Media

Khazan, O. (2013, October 09). Russia's online-comment propaganda army. Retrieved from http://www.theatlantic.com/international/archive/2013/10/russias-online-comment-propaganda-army/280432/

Koenigs, M. (2011, August 26). 9 tips for identifying fake online profiles. Retrieved from http://abcnews.go.com/Technology/tips-identifying-fake-facebook-profiles/story?id=14379498

Laden, G. (2009, March 6). Pseudoanonymoussockpuppetry on the intertubes. Retrieved from http://scienceblogs.com/gregladen/2009/03/06/pseudoanonymoussockpuppetry-on/

Leland, J. (2013, February 16). Online battle over sacred scrolls, real-world consequences. Retrieved from http://www.nytimes.com/2013/02/17/nyregion/ online-battle-over-ancient-scrolls-spawns-real-world-consequences.html

Lindsey, R. (2013, June 6). Sockpuppeting: The ethics and who does it harm? Retrieved from http://fordhamcyberculture.wordpress.com/2013/06/06/sockpuppeting-the-ethics-and-who-does-it-harm/

Lohrmann, D. (2012, September 29). Digging deeper into cyberspace: What are the ethical problems? Retrieved from http://www.govtech.com/blogs/lohrmann-on-cybersecurity/ Digging-Deeper-Into-Cyberspace-092912.html

Ludlow, P. (2013, June 18). The strange case of Barrett Brown. Retrieved from http://www.thenation.com/article/174851/strange-case-barrett-brown

Malone, E. (2013, September 26). Sock-Puppets. Retrieved from http://designingsocialinterfaces.com/patterns/Sock-Puppets

Massoglia, D. (2013, September). *Anonymity is the battlefield: Practical and legal considerations in the fight for free expression on the web* [Scholarly project]. Retrieved from http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=dan_massoglia

McFedries, P. (2006, September 25). Word Spy - Sock Puppet. Retrieved from http://www.wordspy.com/words/sockpuppet.asp

Meredith, J. P. (2010). Combating cyberbullying: Emphasizing education over criminalization. *Federal Communications Law Journal, 63*(1), 311-340. Retrieved from http://www.repository.law.indiana.edu/fclj/vol63/iss1/13

Miller, T. (2014). Threat intelligence and managed intelligence service. Retrieved from https://www.threatintelligence.com/module/threatintelligence/static/downloads/Threat%20Intelligence%20Managed%20Intelligence%20Service%20v1.0.pdf

Morris, K. (2012, July 18). There's no place to hide online-even for sophisticated stalkers. Retrieved from http://www.dailydot.com/news/shawn-sayer-cyber-harassment-arrest/

Naiman, E. (2013, April 10). When Dickens met Dostoevsky. Retrieved from http://www.the-tls.co.uk/tls/public/article1243205.ece

National Conference of State Legislatures. (2013, December 5). State cyberstalking and cyberharassment laws. Retrieved from http://www.ncsl.org/research/

telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx

Novitski, N. (2014, February 25). Cyber Expert: Open Source Intelligence Needs Improvement. Retrieved from http://i-hls.com/2014/02/cyber-expert-open-source-intelligence- needs-improvement/

Ott, M., Cardie, C., & Hancock, J. (2012, April 16). Estimating the prevalence of deception in online review communities. Retrieved from http://dl.acm.org/citation.cfm?id= 2187864&preflayout=flat

PBS. (2002). Wit and wisdom, name that Ben. Retrieved from http://www.pbs.org/benfranklin/ l3_wit_name.html

Poduval, S. (2012). Contours of security in cyberspace. *Maritime Affairs:Journal of the National Maritime Foundation of India, 8*(2), 73-94. doi: 10.1080/09733159.2012.742653

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013, September 5). Anonymity, Privacy, and Security Online. Retrieved from http://www.pewinternet.org/2013/09/05/ anonymity-privacy-and-security-online/

Schwartz, K. E. (2009). Criminal liability for Internet culprits: The need for updated state laws covering the full Spectrum of cyber victimization. *Washington University Law Review, 87*(2), 407-436. Retrieved from http://digitalcommons.law.wustl.edu/cgi/ viewcontent.cgi?article=1086&context=lawreview

Social Media Division, U.S. Army Office of the Chief of Public Affairs. (2011, July 11). Army stresses caution, education to combat social media scammers. Retrieved from http://www.army.mil/article/61432/

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review, 90*(4), 1087-1155. Retrieved from http://www.jstor.org/stable/10.2307/3481326?ref=search-gateway:7484ab9fd85ec1340beefc633909482f

Soriano, M. R. (2012). The vulnerabilities of online terrorism. *Studies in Conflict & Terrorism, 35*(4), 263-277. doi: 10.1080/1057610X.2012.656345

States News Service. (2013, February 5). Eighteen people charged in international $200 million credit card fraud scam crime ring invented 7,000 fake identities to obtain tens of thousands of credit cards. Retrieved from http://www.highbeam.com/doc/ 1G1-317596583.html

Steiner, P. (1993, July 5). On the Internet, nobody knows you're a dog [Cartoon]. *The New Yorker*, *69*(20), 61.

Stone, B., & Richtel, M. (2007, July 15). The hand that controls the sock puppet could get slapped. Retrieved from http://www.nytimes.com/2007/07/16/technology/16blog.html?pagewanted=all&_r=0

Subcommittee on Crime, Terrorism, and homeland Security. (2010, July 28). Online privacy, social networking, and crime victimization. Retrieved from http://judiciary.house.gov/index.cfm/hearings?ID=38763AB1-DFAB-547A-BA1A-1983C4535FF7

Telestra. (2013, November 15). Identity theft (fake profiles & hacking). Retrieved from http://www.lawstuff.org.au/nsw_law/topics/article7/article7

Tynan, D. (2013, November 5). Dear Internet bots and sockpuppets: Your days are numbered. Retrieved from http://www.itworld.com/it-management/381606/dear-internet-fakers-your-days-are-numbered

United States, Department of Homeland Security. (2011). *National strategy for trusted identities in cyberspace enhancing online choice, efficiency, security, and privacy*. Washington, D.C.: Dept. of Homeland Security, White House, Executive Office of the President.

United States, Department of the Army, Headquarters. (2012, July). *Open Source Intelligence*. Retrieved from http://www.fas.org/irp/doddir/army/atp2-22-9.pdf

United States, Intelligence and National Security Alliance, Cyberintelligence Task Force. (2013, September). *Operational Levels of Cyberintelligence*. Retrieved from http://www.insaonline.org/CMDownload.aspx?ContentKey=cfdfcf7c-02b4-4507-a054-2606d684ffb0&ContentItemKey=bc0f998f-85f7-4db6-9288-903f748e1de9

U.S. Army Intelligence Center of Excellence (USAICoE). (2010). *Intelligence - field manual no. 2-0* (United States, Department of the Army, Headquarters). Washington, DC. Retrieved from http://www.fas.org/irp/doddir/army/fm2-0.pdf

Wang, G., Konolige, T., Wilson, C., Wang, X., Zheng, H., & Zhao, B. Y. (2013, August 14). You are how you click: Clickstream analysis for sybil detection. Retrieved from http://www.cs.ucsb.edu/~ravenben/publications/abstracts/clickstream-usenixsec13.html

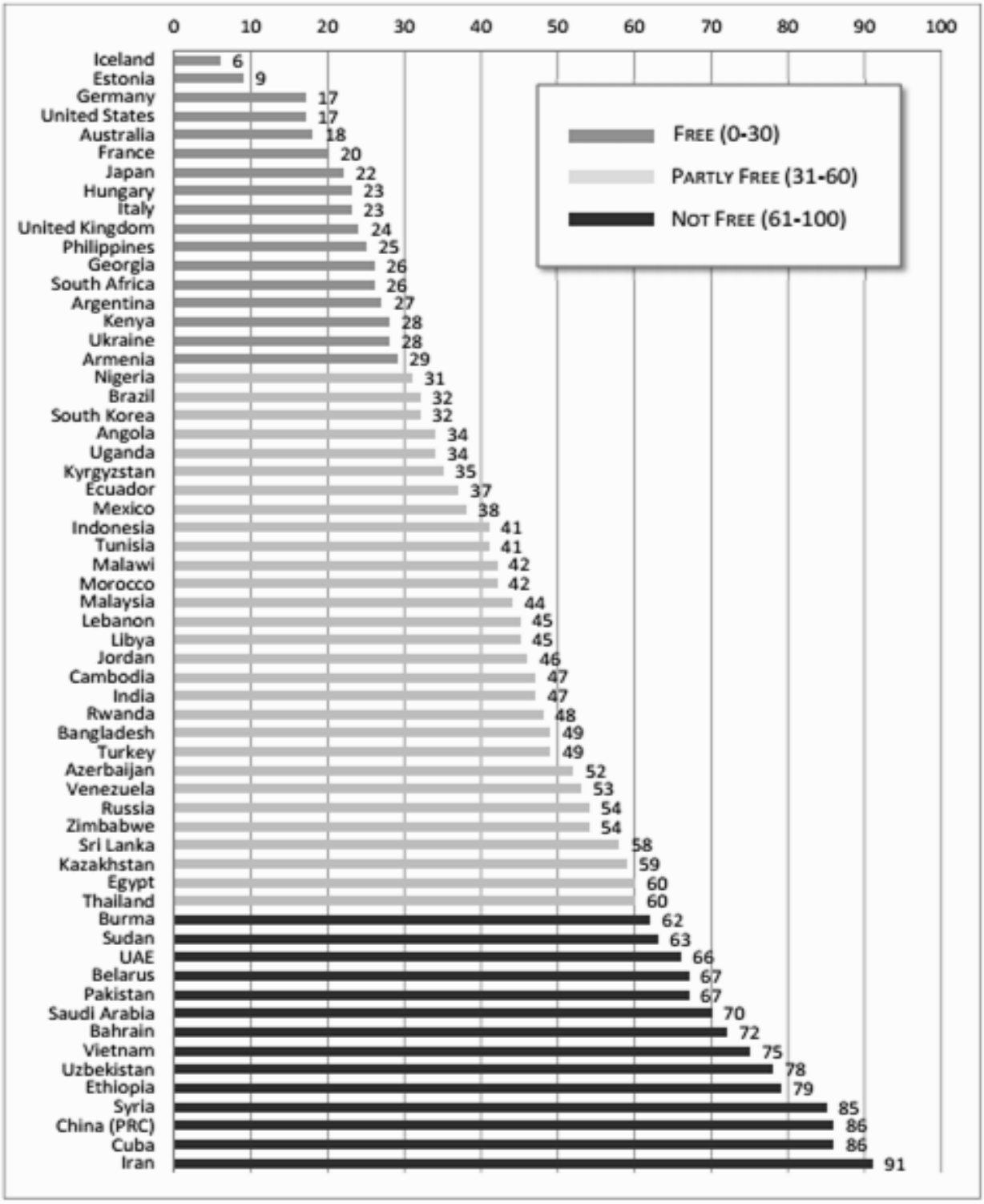
Weaver, J. R., & Bosson, J. K. (2011). I feel like I know you: Sharing negative attitudes of others promotes feelings of familiarity. *Personality and Social Psychology Bulletin, 37*(4), 481-491. doi: 10.1177/0146167211398364

Yang, X., Cao, Q., & Sirivianos, M. (2012, April 25). SybilRank: Aiding the detection of fake accounts in large scale social online services. Retrieved from https://www.cs.duke.edu/~qiangcao/sybilrank_project/index.html

Zheng, X., Lai, Y., Chow, K. P., Hui, L. C., & Yiu, S. M. (2011, October 14). Sockpuppet detection in online discussion forums. Retrieved from

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6079604&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6079604

Appendix A - Internet Freedom in 60 Countries



Note. Source, (Freedom House, 2013).